容器安全（TCSS）

产品文档

文档目录

- 产品简介-新
  - 产品介绍
- 产品架构-新
  - 产品架构
- 操作指南-新
  - 安全概览
  - 资产管理
    - 概述
    - 容器
    - 集群资产
    - 进程端口
    - 应用Web资产
  - 漏洞管理
    - 漏洞检测
  - 镜像风险管理
    - 概述
    - 本地镜像
    - 仓库镜像
    - 镜像拦截事件
  - 集群安全管理
    - 集群检查
    - 自建集群
    - 风险分析
  - 基线管理
    - 概述
    - 容器
    - 镜像
    - Docker主机
    - Kubernetes
  - 运行时安全
    - 概述
    - 容器逃逸
    - 反弹shell
      - 事件列表
      - 配置白名单
    - 文件查杀
    - 恶意外连
  - 高级防御
    - 概述
    - 异常进程
      - 事件列表
      - 规则配置
    - 文件篡改
      - 事件列表
      - 规则配置
    - 高危系统调用
      - 事件列表
      - 白名单管理

- K8s API异常请求
- 策略管理
  - 镜像拦截策略
- 告警设置
- 日志分析
  - 概述
  - 查询日志
  - 配置日志
- 混合云安装指引
  - 概述
  - 配置非腾讯云机器
  - 连接专线VPC
  - 热点问题
- 失陷容器隔离说明

最佳实践-新
- 容器安全等保测评解读
- 镜像漏洞扫描和漏洞管理

常见问题-新
- 常见问题

API文档
- 容器安全服务（tcss）
  - 版本（2020-11-01）
    - API概览
    - 调用方式
      - 接口签名v1
      - 接口签名v3
      - 请求结构
      - 返回结果
      - 公共参数
    - 告警设置相关接口
      - 添加编辑告警策略
      - 获取告警策略列表
    - 安全合规相关接口
      - 安全合规忽略资产+检测项列表
      - 安全合规忽略检测项+资产列表
      - 安全合规忽略检测项列表
      - 安全合规创建合规检查任务
      - 创建一个导出安全合规信息的任务
      - 删除安全合规忽略项， 资产+检测项列表
      - 删除检测项+资产列表的白名单策略
      - 安全合规取消忽略检测项列表
      - 安全合规查询某个资产的详情
      - 安全合规查询某类资产的列表
      - 安全合规查询某资产下的检测项列表
      - 安全合规查询定时任务列表
      - 安全合规查询检测项影响的资产列表
      - 安全合规查询某检测项影响的信息
      - 安全合规查询上次检测失败的资产的列表
      - 安全合规查询上次任务的资产通过率汇总信息
      - 安全合规查询上次任务的检测项的汇总信息列表

安全合规查询白名单列表
安全合规初始化用户的合规基线检测环境
安全合规编辑定时任务
安全合规重新检测选定的资产
安全合规用指定的检测项重新检测选定的资产
安全合规重新检测选定的检测项
安全合规重新检测上次检测失败的资产
安全运营-日志分析 相关接口
添加检索模板
删除检索模板
获取ES字段聚合结果
获取ES查询文档列表
获取索引列表
获取日志检索容量使用统计
获取公钥
导出ES查询文档列表
获取历史搜索记录
获取快速检索列表
查询安全日志告警信息
查询安全日志清理设置详情
查询安全日志投递cls可选项
查询安全日志投递Cls配置
查询安全日志投递kafka可选项
查询安全日志投递kafka配置
查询安全日志接入对象列表
查询安全日志接入列表
查询安全日志KafkaUIN
修改安全日志清理设置信息
更新安全日志-日志投递cls配置
更新安全日志投递kafka设置
修改安全日志接入对象
修改安全日志接入状态
修改安全日志kafkaUIN
重置安全日志主题设置
网络安全相关接口
容器网络创建网络策略添加并发布任务
容器网络创建Yaml网络策略并发布任务
容器网络创建网络策略添加任务
容器网络创建Yaml网络策略添加任务
容器网络创建检查Yaml网络策略任务
容器网络创建网络策略确认任务
容器网络集群下发刷新任务
容器网络集群网络策略创建自动发现任务
容器网络创建网络策略发布任务
容器网络创建网络策略撤销任务
容器网络创建网络策略删除任务
查询集群策略审计列表
查询集群策略列表
容器网络查询资产任务进度
查询集群网络空间标签列表

查询集群网络空间列表
查询集群网络pod标签
容器网络集群查看策略详情
容器网络查询网络策略自动发现任务进度
查询集群网络策略列表
容器网络查询网络策略策略执行状态
容器网络集群查看Yaml网络策略详情
容器网络创建网络策略更新并发布任务
容器网络更新Yaml网络策略并发布任务
容器网络创建网络策略更新任务
容器网络更新Yaml网络策略任务
计费相关接口
查询镜像授权信息
查询专业版需购买信息
查询容器安全服务已购买信息
查询安全日志商品信息
资产管理相关接口
添加容器安全镜像扫描设置
创建本地镜像木马列表导出任务
创建主机列表导出任务
卸载Agent客户端
获取用户当前灰度配置
查询平行容器安装命令
查询agent安装命令
查询资产同步最近时间
查询导出任务下载URL
查询导出任务管理列表
查询检查报告
查询促销活动
查询容器安全概览信息
查询当天未授权核数趋势
隔离容器网络状态
运行时安全-反弹Shell相关接口
添加编辑反弹shell白名单
删除运行时反弹shell事件
删除运行时反弹shell白名单
运行时反弹shell事件详细信息
运行时反弹shell列表
运行时反弹shell列表导出
运行时反弹shell白名单详细信息
运行时反弹shell白名单列表
修改反弹shell事件状态
运行时安全-容器逃逸相关接口
新增逃逸白名单
创建逃逸事件导出异步任务
创建逃逸白名单导出任务
删除逃逸白名单
查询容器逃逸事件详情
查询容器逃逸事件列表
查询待处理逃逸事件趋势

- 统计容器逃逸各事件类型和待处理事件数
- 查询容器逃逸事件列表导出
- 查询容器逃逸扫描规则信息
- 查询容器逃逸安全状态
- 查询逃逸白名单
- 修改容器逃逸扫描事件状态
- 修改容器逃逸扫描规则信息
- 修改逃逸白名单

运行时安全-木马调用相关接口
- 运行时文件查杀重新检测
- 运行时文件查杀一键扫描
- 查询导出任务的结果
- 查询木马自动隔离样本详情
- 查询木马自动隔离样本下载链接
- 查询木马自动隔离样本列表
- 查询木马自动隔离设置
- 运行时查询木马文件信息
- 查询木马事件趋势
- 查询运行时文件查杀事件列表
- 查询木马一键检测预估超时时间
- 运行时查询文件查杀实时监控设置
- 查询木马样本下载url
- 运行时查询文件查杀设置
- 运行时查询文件查杀任务状态
- 运行时文件扫描超时设置查询
- 运行时查询木马概览信息
- 运行时查询文件查杀任务列表
- 运行时文件查杀事件列表导出
- 修改木马自动隔离样本开关
- 修改木马自动隔离设置
- 运行时更新木马文件事件状态
- 运行时更新文件查杀实时监控设置
- 运行时更新文件查杀设置
- 运行时文件扫描超时设置
- 运行时停止木马查杀任务

运行时安全-高危系统调用相关接口
- 创建异常进程规则导出任务
- 删除运行时高危系统调用事件
- 删除运行时高危系统调用白名单
- 运行时高危系统调用列表
- 运行时高危系统调用列表导出
- 运行时高危系统调用系统名称列表
- 运行时高危系统调用白名单详细信息
- 运行时高危系统调用白名单列表
- 修改高危系统调用事件状态

运行时安全相关接口
- 添加编辑异常进程策略
- 添加编辑运行访问控制策略
- 添加编辑高危系统调用白名单
- 创建支持防御的漏洞导出任务

创建应急漏洞导出任务
创建异常进程事件导出异步任务
创建恶意请求事件导出任务
创建系统漏洞导出任务
创建受漏洞影响的容器导出任务
创建导出受漏洞影响的镜像任务
创建漏洞扫描任务
创建web漏洞导出任务
删除运行时异常进程策略
删除运行时访问控制策略
运行时异常进程事件详细信息
查询待处理异常进程事件趋势
运行时异常进程列表
运行时异常进程列表导出
统计异常进程各威胁等级待处理事件数
查询运行时异常进程策略详细信息
运行时异常进程策略列表
运行时异常进程策略列表导出
运行时访问控制事件详细信息
运行时访问控制事件列表
运行时访问控制事件列表导出
查询运行时访问控制策略详细信息
运行时访问控制策略列表
运行时访问控制策略列表导出
镜像绑定规则列表
查询应急漏洞列表
查询恶意请求事件详情
查询恶意请求事件列表
运行时高危系统调用事件详细信息
查询支持防御的漏洞列表
查询受漏洞的容器列表
查询漏洞详情
查询漏洞影响的镜像列表
查询漏洞扫描任务信息
查询漏洞扫描任务的本地镜像列表
查询web应用漏洞列表
修改运行时异常进程策略状态
修改异常进程事件状态
修改运行时访问控制策略状态
修改运行时访问控制事件状态
开通容器安全服务试用
停止漏洞扫描任务
镜像安全相关接口
新增单个镜像仓库详细信息
新增或编辑本地镜像自动授权规则
新增漏洞扫描忽略漏洞
检查单个镜像仓库名是否重复
镜像仓库创建镜像扫描任务
镜像仓库创建镜像一键扫描任务
创建镜像扫描任务

查询本地镜像组件列表导出
创建镜像导出任务
创建或者编辑弹性计费上限
创建漏洞防御导出任务
创建漏洞防御主机导出任务
查询本地镜像漏洞列表导出
取消漏洞扫描忽略漏洞
查询app服务列表
查询容器组件列表
查询容器信息
查询容器列表
查询db服务列表
查询主机信息
查询主机列表
查询镜像信息
查询镜像关联主机
查询镜像列表
查询镜像列表导出
查看镜像仓库资产更新进度状态
镜像仓库查询镜像仓库详情
镜像仓库查询镜像仓库列表
镜像仓库镜像列表导出
查看单个镜像仓库详细信息
镜像仓库仓库列表
镜像仓库查询镜像高危行为列表
镜像仓库敏感信息列表导出
镜像仓库查询一键镜像扫描状态
镜像仓库查询镜像统计信息
镜像仓库查询木马病毒列表
镜像仓库木马信息列表导出
镜像仓库查询镜像漏洞列表
镜像仓库漏洞列表导出
查询镜像风险列表
镜像风险列表导出
获取镜像扫描设置信息
查询镜像扫描状态
查询正在一键扫描的镜像扫描taskid
查询镜像简略信息列表
查询镜像病毒列表
镜像木马列表导出
查询镜像漏洞列表
镜像漏洞列表导出
查询端口占用列表
查询进程列表
查询账户容器、镜像等统计信息
查询web服务列表
查询自动授权规则授权范围主机信息
查询容器安全资产概览
查询容器安全未处理事件概览
查询镜像自动授权结果列表

查询本地镜像自动授权规则
查询镜像自动授权任务列表
查询本地镜像组件列表
查询用户镜像仓库下的命令空间列表
镜像仓库查看定时任务
查询本地镜像风险概览
查询容器安全本地镜像风险趋势
查询全部镜像列表
查询最新披露漏洞列表
查询后付费详情
查询扫描忽略的漏洞列表
查询容器运行时安全时间趋势
查询系统漏洞列表
查询增值服务需购买信息
查询漏洞防御事件列表
查询漏洞防御事件详情
查询漏洞防御攻击事件趋势
查询漏洞防御的主机列表
查询漏洞防御插件列表
查询漏洞防御设置信息
查询漏洞扫描忽略的本地镜像列表
查询漏洞扫描忽略的仓库镜像列表
查询漏洞镜像统计
查询应急漏洞各威胁等级统计镜像数
查询漏洞各威胁等级统计数
查询漏洞影响的仓库镜像列表
统计漏洞扫描页已授权和未扫描镜像数
查询漏洞风险统计概览
查询漏洞风险趋势
查询漏洞Top排名列表
主机资产刷新
镜像仓库停止镜像扫描任务
镜像仓库停止镜像一键扫描任务
停止镜像扫描
批量授权镜像扫描V2.0
修改漏洞防御事件状态
编辑漏洞防御设置
删除单个镜像仓库详细信息
授权镜像扫描
编辑本地镜像自动授权开关
镜像仓库资产刷新
更新单个镜像仓库详细信息
镜像仓库更新定时任务
集群安全相关接口
安装检查组件
创建集群检查任务
下发刷新任务
获取受影响的集群数量
查询节点类型的影响范围
查询workload类型的影响范围

查询所有检查项接口
查询单个集群的详细信息
查询用户集群资产总览
查询刷新任务
查询集群风险项列表
查询检查结果总览
查询未完成的刷新资产任务信息
用户集群资产查询
设置检测模式和自动检查
高级防御-k8sApi异常请求相关接口
创建文件篡改规则导出任务
创建k8s api异常事件导出任务
创建k8sApi异常规则导出任务
创建k8sapi异常事件规则
删除k8sapi异常事件规则
查询集群列表
查询k8s api 异常事件详情
查询k8s api异常事件列表
查询k8sapi异常请求规则详情
查询k8sapi异常请求规则列表
查询k8sapi 异常规则中范围列表
查询k8sapi异常事件统计
查询k8sapi异常事件趋势
修改k8sapi异常事件状态
修改k8sapi异常规则信息
修改k8sapi异常事件规则状态
数据结构
错误码

产品简介-新产品介绍

最近更新时间: 2024-08-23 15:08:00

概述

容器安全服务（Tencent Container Security Service, TCSS）提供容器资产管理、镜像安全、运行时入侵检测、安全基线等安全服务，保障容器从镜像生成、存储到运行时的全生命周期，帮助企业构建容器安全防护体系。 容器安全服务提供多项安全特性，包含：资产管理、镜像安全、运行时安全、基线合规、低资源占用特性。资产管理，提供自动化资产清点，包括容器、镜像、镜像仓库、主机等关键资产信息，帮助企业实现资产可视化。镜像安全，针对镜像、镜像仓库提供一键检测，支持漏洞、木马病毒、可信镜像等多维度安全扫描。运行时安全，自适应识别黑客攻击，实时监控和防护容器运行时安全，提供入侵检测、容器逃逸、进程黑白名单、文件访问控制等安全功能。基线合规，基于 CIS Benchmark 的 Docker、Kubernetes 最佳安全实践，提供一键检测和专业修复方案。低资源占用，一键部署轻量级 Agent，高性能，低占用 CPU/内存，兼容多个主流操作系统。

版本介绍

容器安全服务主要功能版本介绍：

分类	类别		详细描述
安全概览	安全概览		以可视化的图形、图表等方式展示资产信息（容器、镜像、主机）、漏洞风险、集群风险、待处理安全事件数量、运行时安全事件新增趋势、本地镜像新增风险趋势及详情
资产中心	资产管理		支持自动化统计容器、镜像、主机、进程端口、应用 Web 资产、运行应用、数据库应用等资产基本信息。
安全加固	漏洞管理		漏洞管理模块支持对容器环境中的镜像漏洞开展一键检测，为漏洞应急响应及漏洞运营场景提供更好体验。根据实际处理及漏洞响应类型，将漏洞划分为两类，分别是：应急漏洞、系统漏洞、Web应用漏洞。 （1）应急漏洞：支持按威胁等级、风险情况、是否可修复、风险标签、CVE编号、影响镜像名称/ID、漏洞组件名称和版本号筛选漏洞；扫描后，支持展示应急漏洞的披露时间、最新检测时间、影响本地镜像、影响仓库镜像和影响容器等。 （2）系统漏洞&Web应用漏洞：支持按影响资产紧急度和关注紧急度快速筛选漏洞，例如仅展示影响容器的漏洞、仅展示影响最新版本的镜像、重点关注、高危及严重、远程EXP等。同时关联漏洞影响的本地镜像、仓库镜像、容器等资产数据。
	镜像风险管理	本地镜像	支持定时扫描、一键扫描本地镜像获取镜像资产基本信息及镜像安全风险详情，并对业务环境存在风险的镜像总数、安全漏洞、木马病毒、敏感信息进行汇总
		仓库镜像	支持定时扫描、一键扫描仓库镜像获取镜像资产基本信息及镜像安全风险详情，并对业务环境存在风险的镜像仓库总数、安全漏洞、木马病毒、敏感信息进行汇总
		镜像拦截	用户可在“策略管理-镜像拦截策略”页面配置告警和拦截策略，如策略立即生效，则目标风险镜像启动容器时，将实时拦截镜像启动行为并上报事件记录；如策略配置了观察期，观察期仅告警不拦截，则目标风险镜像启动容器时，将实时上报镜像启动行为记录。两种情况均会产生事件记录
	集群风险管理	集群检查	支持自动检查、手动检查获取集群资产基本信息及其存在的配置和漏洞风险，并对业务环境中存在风险的集群及每个集群存在的风险数据进行汇总
		风险分析	支持按严重、高危、中危、低危对存在风险的集群节点进行统计，并按检查项对受影响的集群数、受影响的节点数进行统计

分类	类别		详细描述
	基线管理		支持CIS Benchmark基线检查标准，检测Docker及kubernetes安全基线，并对业务环境中合规容器占比、严重检查项、高危检查项、中危检查项、低危检查项进行统计； 基线检测结果包括基线检测项、类型、基线标准、威胁等级、检测结果、检测项详情等，检测对象包括容器、镜像、主机和kubernetes； 支持用户自定义安全基线检测周期和检测时间、配置基线忽略项
入侵防御	运行时安全	容器逃逸	支持实时检测容器内存在的敏感路径挂载、特权容器、提权事件、逃逸漏洞利用、访问Docker API接口逃逸、篡改敏感文件逃逸、利用cgroup机制逃逸等行为，并自定义开启/关闭检测规则； 支持按风险容器、程序提权、容器逃逸等对告警事件进行分类，明确区分存在风险的容器和容器逃逸行为； 告警信息包括：逃逸事件类型、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、节点名称、POD名称等，同时告警详情提供事件描述、解决方案、进程信息、父进程信息、祖先进程信息等详情
		反弹shell	支持实时检测容器内存在的反弹shell行为并产生告警，告警信息包括：进程名称、父进程名称、目标地址、进程路径、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID等，同时告警详情提供进程和父进程详细信息； 支持用户对告警事件加白处理，或按目标地址（IP、端口）、连接进程和生效镜像范围自定义新增白名单
		文件查杀	支持实时检测容器运行时存在的木马病毒并产生告警，告警信息包括文件名称、文件路径、病毒名称、首次生成时间、最近生成时间、容器名称/ID、镜像名称/ID、容器状态等，同时告警详情提供恶意文件详情、事件详情、解决方案、进程、父进程、祖先进程等详细信息； 支持实时监控、一键扫描和定时扫描容器内恶意文件；同时支持客户自定义开启自动隔离恶意文件开关
		恶意外连	支持实时检测容器外连恶意域名的行为并产生告警，告警信息包括事件类型、请求域名、容器名称/容器ID/运行状态/容器隔离状态、镜像名称/ID、主机名称/IP、首次生成时间、最近生成时间、请求次数等，同时告警详情提供恶意域名详情、事件详情、解决方案、进程、父进程、祖先进程等详细信息。当发现容器存在访问恶意域名/IP的行为时，您的容器可能已经失陷，因为恶意域名/IP可能是黑客的远控服务器、恶意软件下载源、矿池地址等，建议及时进行排查
	高级防御	异常进程	支持实时检测容器内存在的进程异常启动行为并告警通知或拦截异常进程。告警信息包括：进程路径、命中规则、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、动作执行结果等，同时告警详情提供进程和父进程详细信息； 异常进程系统策略至少包括代理软件、横向渗透、恶意命令、反弹shell、无文件程序执行、高危命令、敏感服务异常子进程启动等； 支持用户对告警事件加白处理，或按进程路径和生效镜像范围自定义新增进程放行规则； 支持用户自定义新增进程检测规则，配置内容包括规则名称、进程路径、执行动作（拦截、告警、放行）和生效镜像范围
		文件篡改	支持实时检测容器内存在的文件篡改行为并告警通知或拦截异常访问。告警信息包括：文件名称、进程路径、命中规则、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、动作执行结果等。同时告警详情提供进程和被篡改文件详细信息； 文件篡改系统策略至少包括篡改计划任务、篡改系统程序、篡改用户配置等规则； 支持用户对告警事件加白处理，或按进程路径、被访问文件路径和生效镜像范围自定义新增放行规则； 支持用户自定义新增访问控制规则，配置内容包括规则名称、进程路径、被访问文件路径、执行动作（拦截、告警、放行）和生效镜像范围
		高危系统调用	支持实时检测容器内存在的高危系统调用行为并产生告警，告警信息包括：进程路径、系统调用名称、首次生成时间、最近生成时间、事件数量、容器名称/ID、镜像名称/ID、节点名称、POD名称等，同时告警详情提供进程和父进程详细信息； 支持用户对告警事件加白处理，或按进程路径、系统调用名称和生效镜像范围自定义新增白名单
		K8s API异常请求	支持实时监控集群 API 异常请求行为，包括系统策略和用户自定义策略两部分。 系统规则：基于腾讯云安全技术及多维度多种手段，通过“匿名访问”“异常 UA 请求”“匿名用户权限变动”“凭据信息获取”“敏感路径挂载”“命令执行”“异常定时任务”“静态 pod 创建”“可疑容器创建”等共9个规则类型，对集群API异常请求行为进行全方位监测。 用户自定义规则：支持自定义 K8s API 异常请求字段，及具体生效范围，更加灵活贴近实际业务需求
策略配置	策略管理	镜像拦截策略	用户可在“策略管理-镜像拦截策略”页面配置告警和拦截策略。镜像拦截策略支持您对存在严重安全问题的镜像进行容器启动拦截，避免恶意镜像运行容器业务。支持拦截的镜像类型：存在严重&高危漏洞、木马病毒、敏感信息风险的镜像，特权模式启动镜像

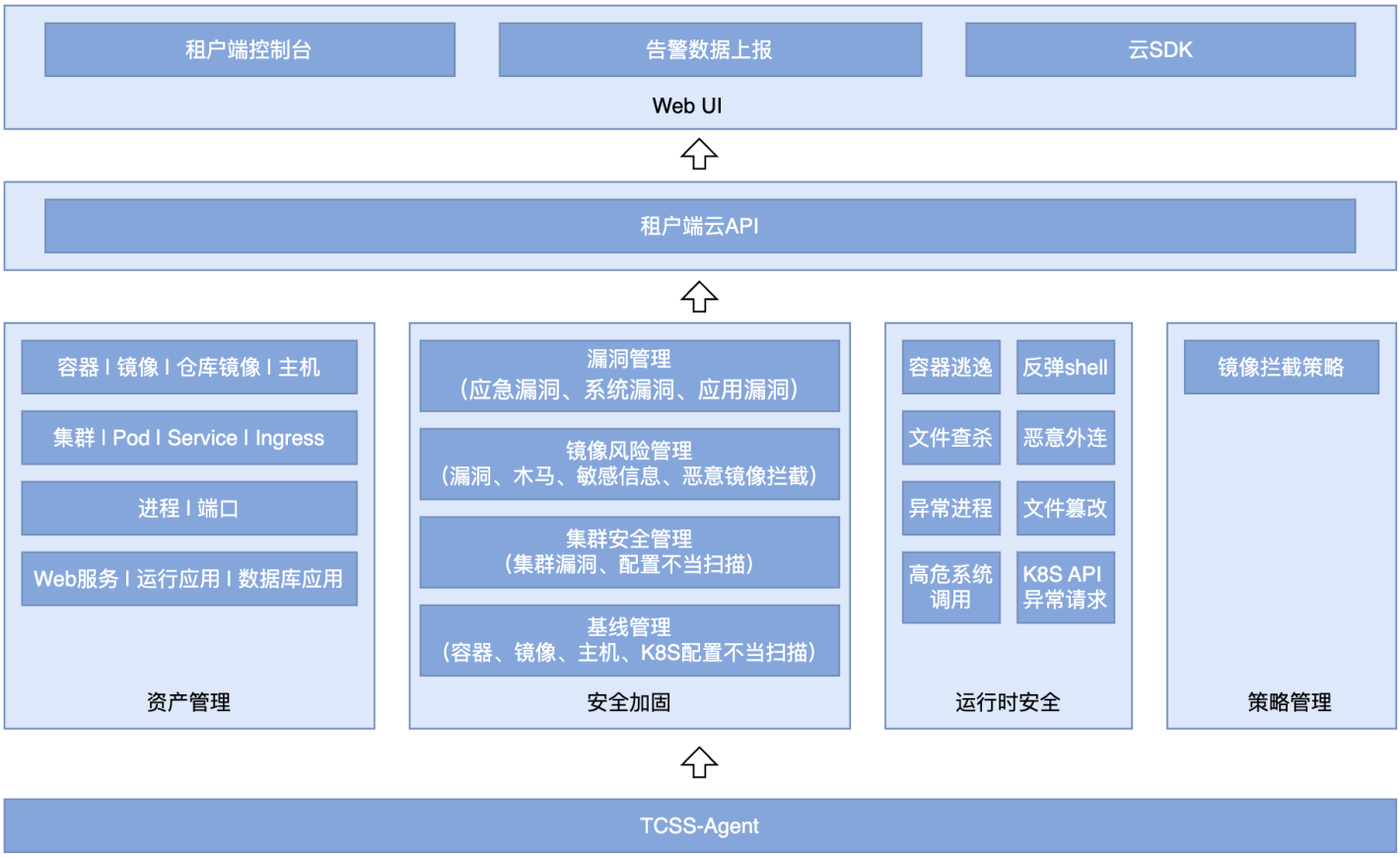
分类	类别		详细描述
安全运营	日志分析		支持按时间、日志类型、日志内容等自定义检索容器bash日志、容器启动审计日志、kubernetes API审计日志，并按检索结果展示日志趋势图； 支持自定义日志的展示字段和隐藏字段，查看json格式日志，并支持导出日志； 日志配置：支持自定义配置容器bash日志、容器启动审计日志和kubernetes API审计日志是否开启日志审计，以及按照日志类型自定义节点是否开启审计；支持按百分比和存储天数清理日志
设置中心	告警设置		可点击告警状态开关开启或关闭镜像安全事件和运行时安全事件告警，镜像安全事件包含本地镜像和仓库镜像的安全漏洞、木马病毒、敏感信息事件，运行时安全事件包括容器逃逸、异常进程、文件篡改等运行时事件

产品架构-新

产品架构

最近更新时间: 2024-08-23 15:08:00

下图是容器安全服务的产品架构示意图。



容器安全服务Agent

Agent是一个常驻在云主机操作系统中的轻量化进程，部署在需要保护的宿主机上，主要功能是根据用户配置的安全策略上报宿主机上容器运行时存在的安全风险数据和新增的安全事件数据、本地镜像扫描、资产识别、集群安全扫描和安全基线检查。同时响应用户和云端防护中心的指令，实现对容器上的安全威胁清除和恶意攻击拦截。

防护引擎

基于腾讯的大数据处理能力，云端防护中心接收全网Agent上报的安全事件和威胁数据，通过云端的多个威胁识别模型，对每一条上报的安全事件进行分析，根据分析结果给Agent下发相关拦截和处理指令，云端防护中心是容器安全服务的中枢神经系统，相关安全威胁的识别算法依赖于腾讯云安全团队的运营和智能调优，云端防护中心同时保存用户自己创建的相关安全策略配置，满足用户个性化的安全防护需求。

云API

提供给用户资产管理、漏洞管理、镜像安全管理、基线管理、运行时安全等相关云API服务。

租户端控制台

提供给用户使用的网页版本控制台，主要功能包括安全概览、资产管理（容器、集群、进程端口、应用Web资产）、漏洞管理、镜像风险管理（本地镜像、仓库镜像、镜像拦截事件）、集群安全管理、基线管理、运行时安全、高级防御、策略管理（镜像拦截策略）、日志分析、告警设置等供用户操作和查看的功能，以及对应的云SDK。

操作指南-新
安全概览

最近更新时间: 2024-08-23 15:08:00

本文档为您介绍容器安全服务各个安全模块的整体安全情况概览。

- 实时展示容器安全风险概览信息和容器安全事件新增趋势等信息。
- 容器安全服务的版本和使用情况，并提供升级、续费等功能。

主要功能

登录 容器安全服务控制台，在左侧导航中，单击**安全概览**，进入安全概览页面。

查看资产信息

1.在安全概览页面，资产信息模块展示容器、镜像、集群、主机节点的资产数量信息。

2.在安全概览页面，单击“模块总数”，可跳转到资产管理的对应模块列表。

查看版本和使用情况，升级、续费

在安全概览页面，版本信息窗口展示当前容器安全服务版本信息和版本到期时间，以专业版为例具体信息如下：

- 若当前版本即将到期将提醒用户进行续费，用户可单击**立即续费**，进入续费页面完成续费。

- 版本信息窗口同时展示当前用户的授权情况，包括总核数和授权核数、已购镜像授权。

- 总核数和授权核数：总核数是指用户业务节点的虚拟核数总和；授权核数是指用户开通专业版的核数。

> 说明：
>
> - 当授权核数小于总核数时，将提示用户需补充购买的核数，用户可单击升级，进入购买页面购买授权。
> - 当用户未补充购买所需授权核数时，将进入弹性计费模式，即超过授权核数将按1元/核/天进行弹性计费。

- 已购镜像授权：用户已购买的镜像安全扫描数量。

> 说明：
>
> - 当业务环境中存在未开启镜像安全扫描的本地镜像或仓库镜像时，将提示用户需补充购买的镜像授权数，用户可单击**选购**，进入购买页面购买授权。
> - 镜像授权购买后，还需用户进入**镜像安全>本地镜像/仓库镜像**页面对授权进行配置，用户可自定义配置需开启安全扫描的镜像。

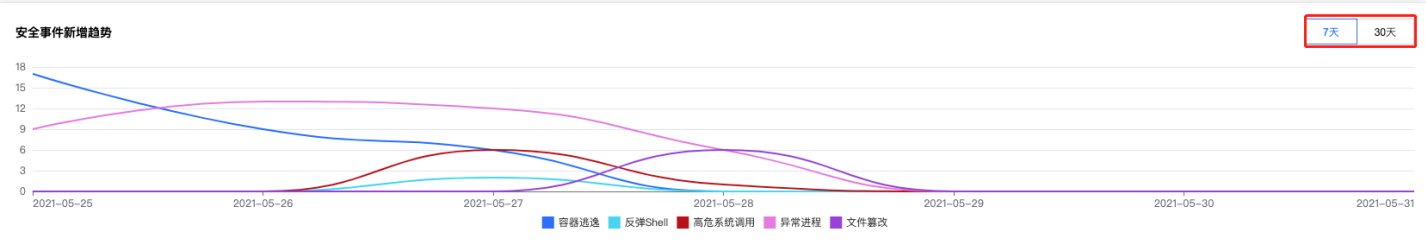
查看待处理安全事件

1.在安全概览页面，待处理安全事件模块展示当前待处理的安全事件的数量。

2.在安全概览页面，单击“模块总数”，可进入到相应的安全事件页面查看详情并进行处理。

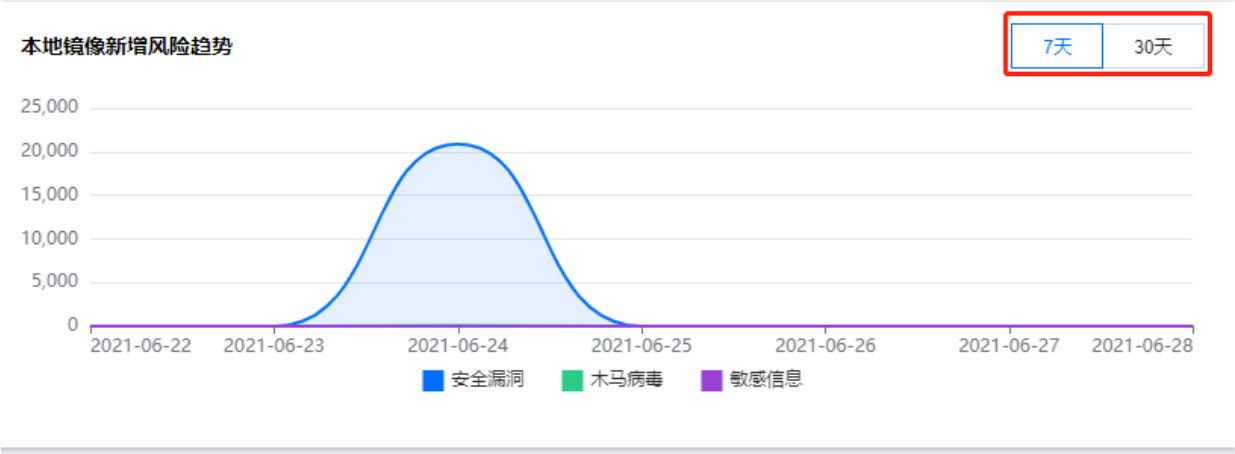
查看安全事件新增趋势

在安全概览页面，安全事件新增趋势模块展示7天或30天内运行时安全事件新增趋势。单击**7天**或**30天**可切换时间。



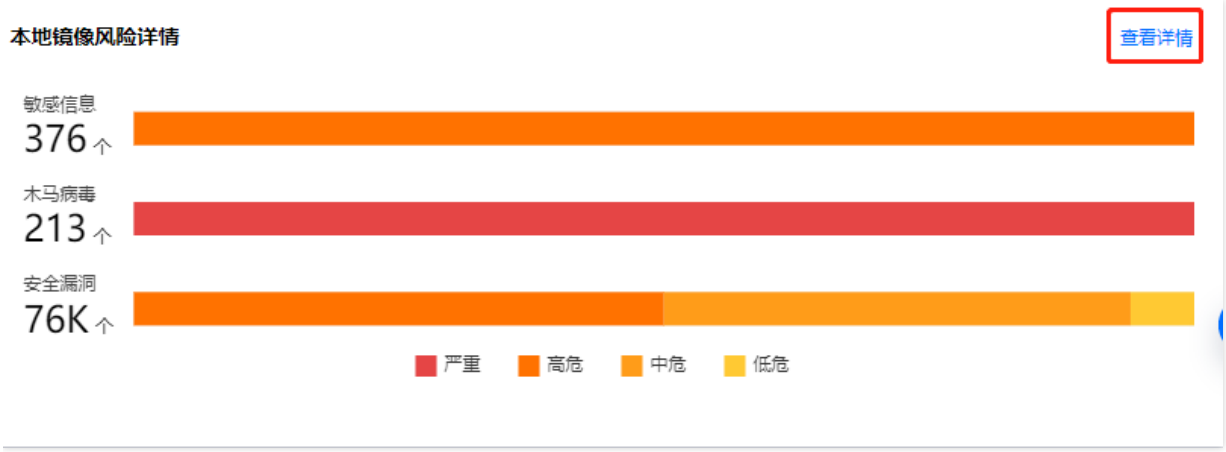
查看本地镜像新增风险趋势

在安全概览页面，展示7天或30天内本地镜像新增的安全漏洞、木马病毒、敏感信息数量趋势。单击**7天**或**30天**可切换时间。



查看本地镜像风险详情

在安全概览页面，本地镜像风险详情模块展示当前镜像存在的敏感信息、木马病毒、安全漏洞的风险总数和威胁等级分布。单击**查看详情**，可进入镜像安全模块查看详情并进行处理。



资产管理
概述

最近更新时间: 2024-08-23 15:08:00

本文档为您介绍资产管理所提供的自动化资产清点功能，支持清点容器、镜像和镜像仓库等关键资产信息，帮助企业实现资产可视化。

- 资产管理的数据每隔24小时自动同步一次，支持手动同步。
- 资产管理支持采集以下10种资产的信息：容器、本地镜像、仓库镜像、集群、主机节点、进程、端口、Web 服务、运行应用、数据库应用。
- 目前支持识别的资产有：

资产类型	资产信息
容器资产	容器、本地镜像、仓库镜像、集群、主机节点。
集群资产	集群、Pod、Service、Ingress。
进程端口	进程、端口。
应用web资产	Web 服务、运行应用、数据库应用。

容器

最近更新时间: 2024-08-23 15:08:00

本文档为您介绍容器模块功能，以及如何查看容器、镜像和主机等资产详情。

查看容器模块

容器展示模块中提供容器资产总数，以及正在运行、暂停运行和停止运行容器的数量。

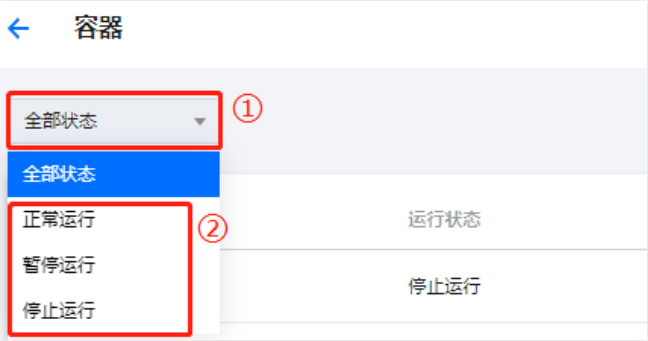
筛选容器列表

1. 登录[容器安全服务控制台，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击“容器总数”，进入到容器列表页面，可查看全部容器资产列表。

3. 在容器列表页面，可按运行状态对容器资产进行筛选，或搜索框通过“容器名称、容器ID、镜像名称、主机IP”等关键字对容器进行查找。

- 单击左上角的状态下拉框，按运行状态对容器资产进行筛选。



- 单击搜索框，通过“容器名称、容器ID、镜像名称、主机IP”等关键字对容器进行查找。

查看容器列表

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击"容器总数"，进入到容器列表页面，可查看全部容器资产列表。

3. 在容器列表页面，单击"容器名称"，右侧弹出抽屉展示该容器详情，页面可切换查看容器基本信息、进程和端口等信息。

4. 在资产管理页面，单击"主机 IP"，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

> **说明：**
>
> 在抽屉中，单击"数字"查看主机相关镜像数和相关容器数详情。

自定义列表管理

1.登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

2.在资产管理页面，单击"容器总数"，进入到容器列表页面，可查看全部容器资产列表。

3.在容器列表页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

4.在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 运行状态：包括正常运行、暂停运行和停止运行三种状态。

2. 镜像：关联镜像名称。

3. 所属 POD：容器所属 POD。

4. CPU|占用率：CPU 使用率。

5. 内存|占用：内存占用大小。

查看本地镜像模块

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，镜像模块展示了模块中镜像资产总数。单击"镜像总数"，可跳转**镜像安全**>**本地镜像**页面查看镜像详情。

查看镜像仓库模块

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，镜像仓库模块展示了镜像仓库资产总数。单击“镜像仓库总数”，可跳转**镜像安全**>**镜像仓库**页面查看镜像仓库详情。

查看主机模块

主机展示模块中提供主机资产总数，以及正在运行和已离线主机的数量。

筛选主机列表

1. 登录容器安全服务控制台，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击“主机总数”，可查看全部主机资产列表。

3. 在主机列表页面，可按主机状态对主机资产进行筛选，或搜索框通过“主机名、业务组、docker 版本、主机 IP”等关键字对主机进行查找。

- 单击左上角的状态下拉框，按主机状态对主机资产进行筛选。

- 单击搜索框，通过"主机名、业务组、Docker 版本 、主机 IP"等关键字对主机进行查找。

查看容器列表

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

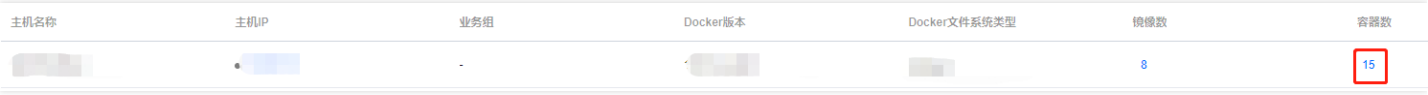
2. 在资产管理页面，单击"主机总数"，可查看全部主机资产列表。

3. 在主机列表页面，单击"主机 IP"，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

> **说明：**
>
> 在抽屉中，单击"数字"查看主机相关镜像数和相关容器数详情。

4. 在主机列表页面，单击"镜像数"，可查看关联镜像详情。

5. 在主机列表页面，单击“容器数”，可查看关联容器详情。



自定义列表管理

1.登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

2.在资产管理页面，单击“主机总数”，可查看全部主机资产列表。

3.在主机列表页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

4.在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表字段说明

1. 主机名称：主机名称。

2. 主机 IP：单击“主机 IP”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

3. 业务组：主机所属业务组名称。

4. Docker 版本：展示 Docker 版本号，如未安装，则显示“未安装”。

5. Docker 文件系统类型：Docker 文件系统类型。

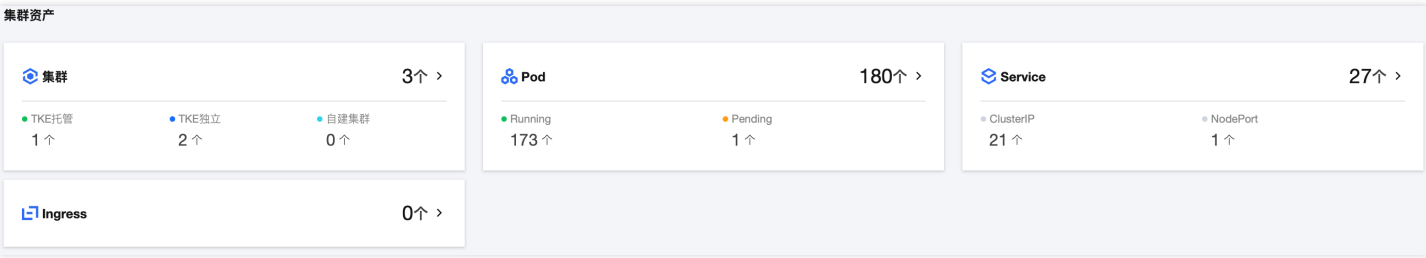
6. 镜像数：主机关联镜像数。单击“数字”可查看关联镜像详情。

7. 容器数：主机关联容器数。单击“数字”可查看关联容器详情。

集群资产

最近更新时间: 2024-08-23 15:08:00

本文档为您介绍集群资产功能，以及如何查看集群、Pod、Service、Ingress 资产详情。



查看集群模块

集群模块展示了集群总数以及每种集群类型的数量。

查看集群列表

1. 登录容器安全服务控制台，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击**"集群总数"**，进入集群检查页面，可查看全部集群资产。

3. 在集群检查页面，单击**搜索框**，通过"集群名称、集群 ID、集群类型、所属地域"等关键字可对集群进行查找。

自定义列表管理

1. 在集群检查页面，单击设置图标，弹出自定义列表管理对话框。

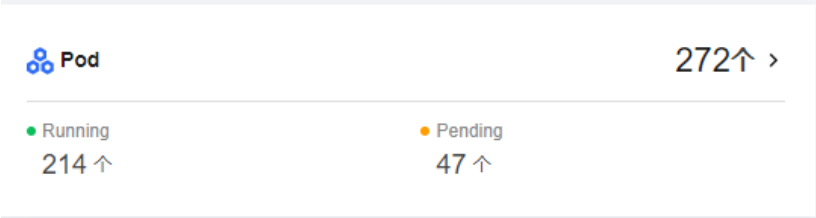
2. 在自定义列表管理对话框，选择所需的类型后，单击**确定**，即可完成设置自定义列表。

查看 Pod 模块

Pod 模块展示了集群 Pod 总数，以及 Running、Pending 状态的 Pod 数量。

查看 Pod 列表

1. 在资产管理页面，单击**"Pod 总数"**，进入 Pod 列表页面，可查看全部 Pod 资产。



2. 在 Pod 列表页面，可按"集群名称、命名空间、地域"对 Pod 资产进行筛选；单击**更多筛选**可按"Pod 状态、工作负载类型、工作负载名称、集群 ID、Pod IP、所在节点 IP、容器名称、容器 ID、镜像名称"对 Pod 资产进行筛选；或单击**搜索框**通过"Pod 名称"关键字可对 Pod 资产进行查找。

3. 找到目标 Pod，单击 **Pod 名称**，右侧弹出抽屉展示该 Pod 详情，页面可切换查看 Pod 基本信息、Service 和容器等信息。

自定义列表管理

1. 在 Pod 列表页面，单击设置图标，弹出自定义列表管理对话框。

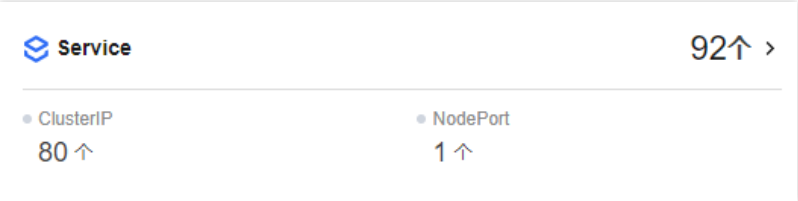
2. 在自定义列表管理对话框，选择所需的类型后，单击**确定**，即可完成设置自定义列表。

查看 Service 模块

Service 模块展示了集群 Service 总数，以及 ClusterIP、NodePort 类型的 Service 数量。

查看 Service 列表

1. 在资产管理页面，单击**"Service 总数"**，进入 Service 列表页面，可查看全部 Service 资产。



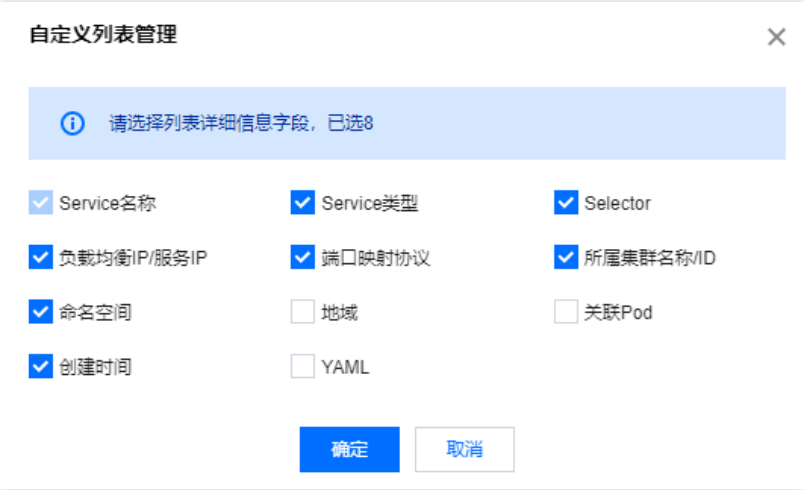
2. 在 Service 列表页面，可按"集群名称、命名空间、地域"对 Service 资产进行筛选，单击**更多筛选**可按"集群 ID、Service 类型、负载均衡 IP、服务 IP、Labels、端口"对 Service 资产进行筛选。或单击**搜索框**通过"Service 名称"关键字可对 Service 资产进行查找。

3. 找到目标 Service，单击**"Service 名称"**，右侧弹出抽屉展示该 Service 详情，页面可切换查看 Service 基本信息、Pod、YAML 和端口映射规则等信息。

自定义列表管理

1. 在 Service 列表页面，单击设置图标，弹出自定义列表管理对话框。

2. 在自定义列表管理对话框，选择所需的类型后，单击**确定**，即可完成设置自定义列表。

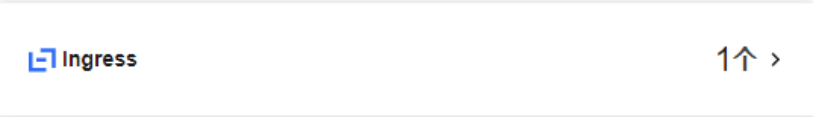


查看 Ingress 模块

Ingress 模块展示了集群 Ingress 总数。

查看 Ingress 列表

1. 在资产管理页面，单击**"Ingress 总数"**，进入 Service 列表页面，可查看全部 Ingress 资产。



2. 在 Ingress 列表页面，可按"集群名称、命名空间、地域"对 Ingress 资产进行筛选；单击**更多筛选**可按"Ingress 名称、VIP、Labels、后端服务"对 Ingress 资产进行筛选；或单击**搜索框**通过"Ingress 名称"关键字可对 Ingress 资产进行查找。

3. 找到目标 Ingress，单击**"Ingress 名称"**，右侧弹出抽屉展示该 Ingress 详情，页面可切换查看 Ingress 基本信息、转发配置和 YAML 信息。

自定义列表管理

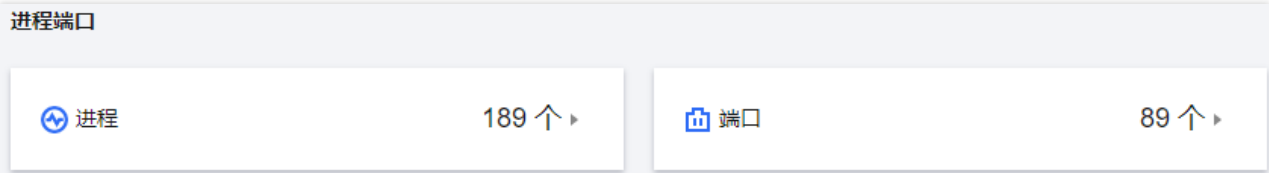
1. 在 Ingress 列表页面，单击设置图标，弹出自定义列表管理对话框。

2. 在自定义列表管理对话框，选择所需的类型后，单击**确定**，即可完成设置自定义列表。

进程端口

最近更新时间: 2024-08-23 15:08:00

本文档为您介绍进程端口功能提供进程和端口数量，以及如何查看进程列表和端口列表。



查看进程模块

进程模块展示了进程总数。

筛选进程列表

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

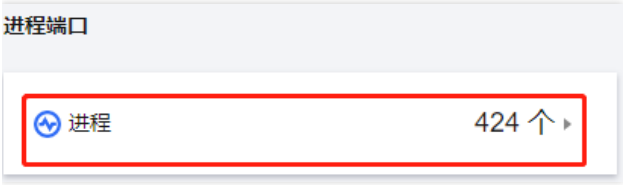
2. 在资产管理页面，单击"进程总数"，进入进程列表页面，可查看全部进程资产列表。

3. 在进程列表页面，单击搜索框，通过"运行用户、主机名、进程名"等关键字可对进程进行查找。

查看容器列表

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击"进程总数"，进入进程列表页面，可查看全部进程资产列表。



3. 在进程列表页面，单击“主机 IP”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

> **说明：**
>
> 在抽屉中，单击“数字”查看主机相关镜像数和相关容器数详情。

自定义列表管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击“进程总数”，进入进程列表页面，可查看全部进程资产列表。

3. 在进程列表页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

4. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

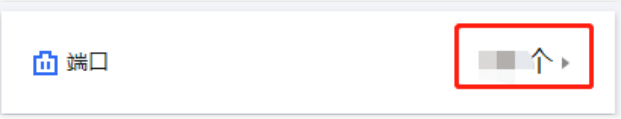
查看端口模块

端口模块展示了端口总数。

筛选端口列表

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击“端口总数”进入端口列表页面，可查看全部端口资产列表。

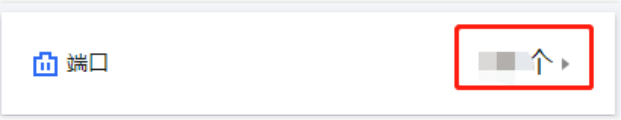


3. 在端口列表页面，单击搜索框，通过“主机 IP、进程名和宿主机端口”等关键字可对端口进行查找。

查看端口列表

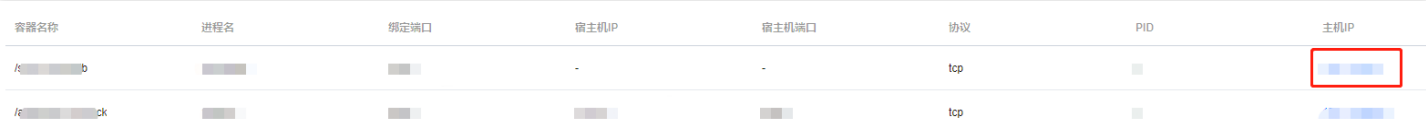
1. 登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击“端口总数”进入端口列表页面，可查看全部端口资产列表。



3. 在端口列表页面，单击“主机 IP”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

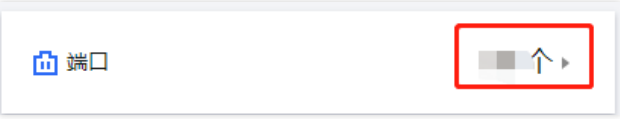
> **说明：**
>
> 在抽屉中，单击“数字”查看主机相关镜像数和相关容器数详情。



自定义列表管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击“端口总数”进入端口列表页面，可查看全部端口资产列表。



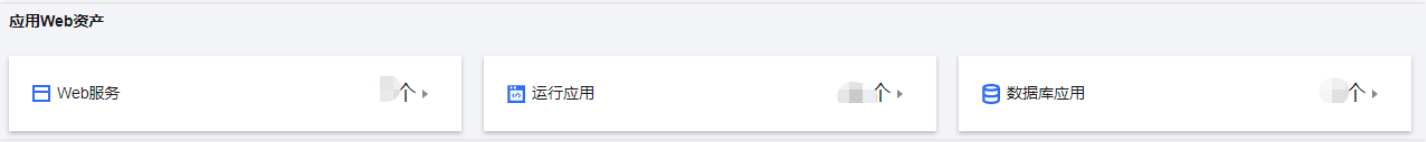
3. 在端口列表页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

4. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

应用Web资产

最近更新时间: 2024-08-23 15:08:00

本文档为您介绍应用 Web 资产功能，以及如何查看 Web 服务、运行应用和数据库应用数量。

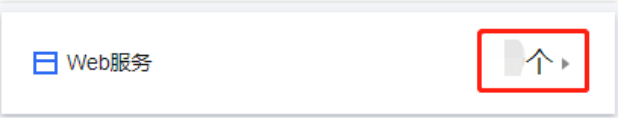


查看 Web 服务

筛选 Web 服务

1. 登录容器安全服务控制台，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击"Web 服务总数"进入Web 服务列表页面，可查看全部进程资产列表。



3. 在 Web 服务列表页面，可按服务类型对 Web 服务资产进行筛选，或搜索框通过"容器名称、主机名、启动用户"等关键字对 Web 服务进行查找。

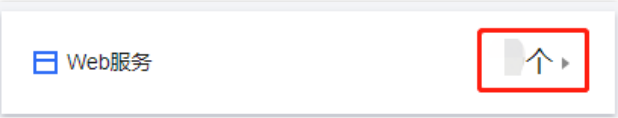
- 单击左上角的服务类型下拉框，按服务类型对 Web 服务资产进行筛选。

- 单击搜索框，可通过"容器名称、主机名、启动用户"等关键字对 Web 服务进行查找。

查看 Web 服务列表

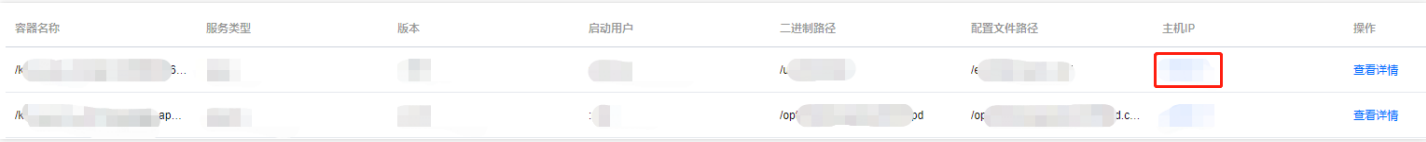
1. 登录容器安全服务控制台，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击"Web 服务总数"进入Web 服务列表页面，可查看全部进程资产列表。

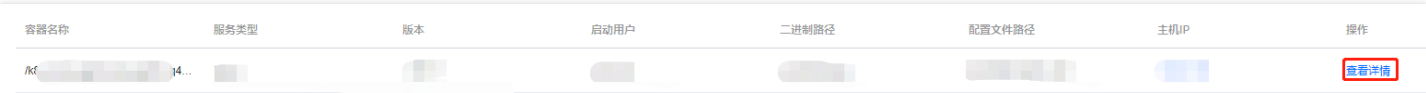


3. 在 Web 服务列表页面，主机 IP：单击"主机 IP"，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

> **说明：**
>
> 在抽屉中，可单击"数字"查看主机相关镜像数和相关容器数详情。



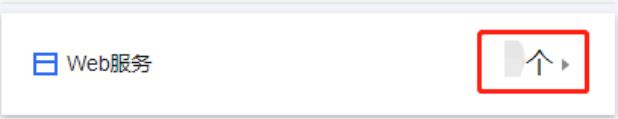
4. 在 Web 服务列表页面，单击**查看详情**，对话框展示 Web 应用服务详情，包括基本信息和关联进程列表。



自定义列表管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击"Web 服务总数"进入Web 服务列表页面，可查看全部进程资产列表。



3. 在 Web 服务列表页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

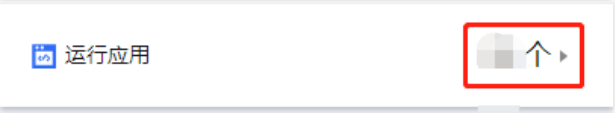
4. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

查看运行应用

筛选运行应用

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击"运行应用总数"，进入运行应用列表页面，可查看全部运行应用列表。



3. 在运行应用列表页面，单击搜索框，可通过"容器名称、主机 IP 和应用类别"等关键字对运行应用进行查找。

查看运行应用列表

1. 登录容器安全服务控制台，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击“运行应用总数”，进入运行应用列表页面，可查看全部运行应用列表。

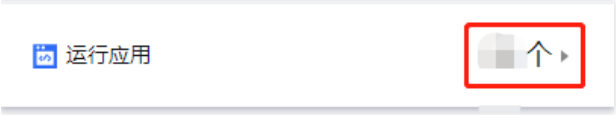
3. 在运行应用列表页面，单击“主机 IP”，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

4. 在资产管理页面，单击**查看详情**，对话框展示运行应用关联进程详情列表。

自定义列表管理

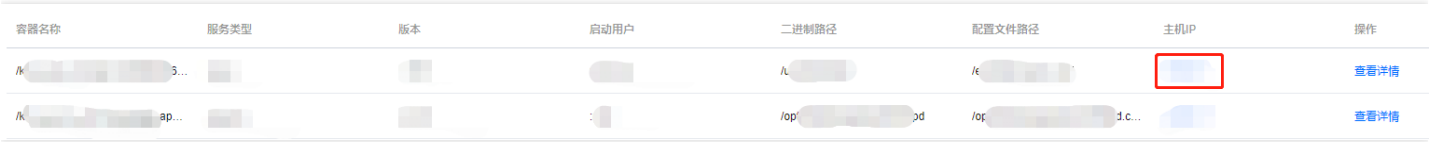
1. 登录容器安全服务控制台，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击“运行应用总数”，进入运行应用列表页面，可查看全部运行应用列表。



3. 在运行应用列表页面，单击 图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

> **说明：**
>
> 在抽屉中，可单击“数字”查看主机相关镜像数和相关容器数详情。



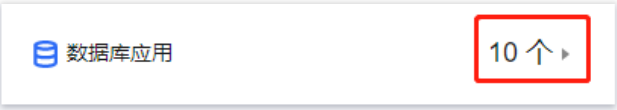
4. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

查看数据库应用

筛选数据库应用

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击“数据库应用总数”，进入运行应用列表页面，可查看全部数据库应用资产列表。

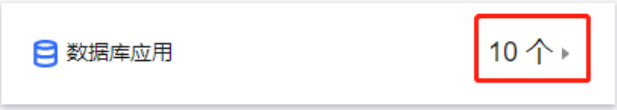


3. 在数据库应用资产列表页面，单击搜索框，通过"容器名称、主机IP和数据库类型"等关键字可对数据库应用进行查找。

查看数据库应用列表

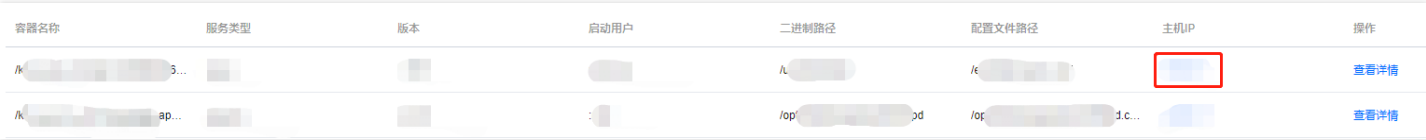
1. 登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击"数据库应用总数"，进入运行应用列表页面，可查看全部数据库应用资产列表。



3. 在数据库应用资产列表页面，单击"主机 IP"，右侧弹出抽屉展示主机详情，包括主机基本信息、Docker 信息、相关镜像数和相关容器数。

> **说明：**
>
> 在抽屉中，可单击"数字"查看主机相关镜像数和相关容器数详情。

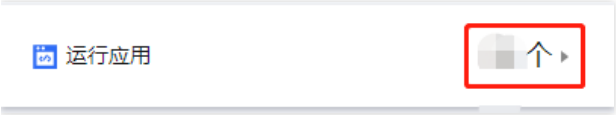


4. 在运行应用务列表页面，单击**查看详情**，对话框展示数据库服详情，包括基本信息和关联进程列表。

自定义列表管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击“运行应用总数”，进入运行应用列表页面，可查看全部运行应用列表。



3. 在数据库应用资产列表页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

4. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

漏洞管理
漏洞检测

最近更新时间: 2024-08-23 15:08:00

容器安全服务支持对本地镜像和仓库镜像上的漏洞，进行周期性和及时性的检测功能。支持对指定镜像和漏洞类别的检测，同时支持忽略漏洞等功能，可为您提供漏洞的风险、特征、严重等级及修复建议等信息，可视化界面有助于您更好的管理镜像的漏洞风险。

本文档将介绍如何使用漏洞管理功能，帮助您管理镜像的漏洞风险。漏洞管理功能支持一键检测系统漏洞、Web 应用漏洞及应急漏洞。

前提条件

已购买容器安全服务专业版。

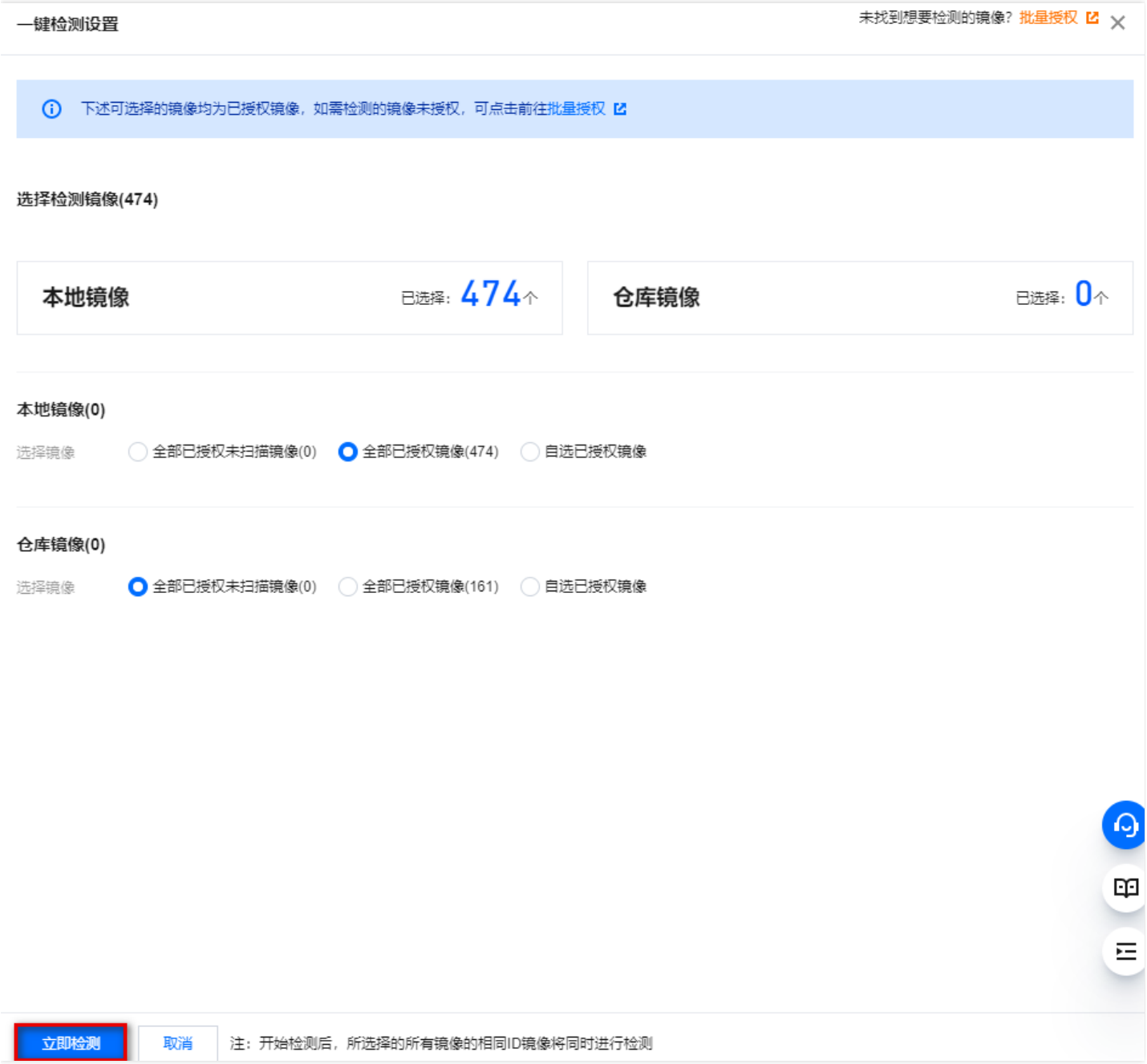
漏洞检测

1. 登录容器安全控制台，在左侧导航栏中选择**漏洞管理**，进入漏洞管理页面。

2. 在漏洞管理页面，可进行漏洞检测并查看漏洞检测数据，单击**一键检测**。

3. 在一键检测设置弹窗中，选择需要检测的镜像，单击**立即检测**，检测完成后，检测结果会以可视化图表的方式显示在漏洞管理页面。

> **说明：**
>
> - 需要先对镜像完成授权方可进行镜像检测。
> - 检测时间与检测镜像数量、镜像大小、是否第一次检测等因素有关，检测一般持续2-60分钟。



查看漏洞

1. 在漏洞管理页面，查看镜像检测到的系统漏洞、Web 应用漏洞、应急漏洞的漏洞信息。查看漏洞影响的本地镜像、仓库镜像、运行容器资产信息以及漏洞风险统计情况、TOP5漏洞、存在严重&高危漏洞镜像趋势。

- TOP5漏洞图：系统根据漏洞 CVSS 分数和动态风险等级等因素计算出漏洞 TOP5排名，并展示 TOP5漏洞的威胁等级、影响镜像数（只统计最新版本）和影响容器数量。

- 严重&高危漏洞镜像趋势图：展示存在有严重或高危漏洞的镜像（最新版本）的数量变化趋势，当切换为运行容器时，展示存在有严重或高危漏洞且启动了容器的镜像（最新版本）的数量变化趋势。可查看7天或30天的趋势图。

2. 在漏洞列表中，可以查看漏洞名称、威胁等级、CVE 编号、首次发现时间、最近检出时间等信息。

漏洞名称/标签	威胁等级	CVSS	CVE编号	影响本地镜像	影响仓库镜像	影响容器	漏洞类型	首次发现时间	最近检出时间	操作
[illegible]	高危			207	9	1	授权问题	2022-06-06 06:22:11	2022-06-07 14:53:47	查看详情
[illegible]	高危			210	9	50	越界写入	2022-06-06 06:22:11	2022-06-07 14:53:47	查看详情
[illegible] 远程利用	严重			220	9	2	代码注入	2022-06-06 06:22:11	2022-06-07 14:53:47	查看详情

字段说明：

- 漏洞名称：漏洞公开的命名。
- 威胁等级：根据漏洞的危险程度，将其划分为严重、高危、中危和低危四个等级。
- 首次发现时间：取第一次镜像检测出该漏洞的时间。
- 最近检出时间：取最近一次镜像检测出该漏洞的时间。
- 影响本地镜像（个）：表示所有检测出的镜像漏洞中，有多少个本地镜像存在该漏洞，即该漏洞影响的本地镜像数量。
- 影响仓库镜像（个）：表示所有检测出的镜像漏洞中，有多少个仓库镜像存在该漏洞，即该漏洞影响的仓库镜像数量。
- 影响容器（个）：表示所有检测出的镜像漏洞中，有多少个运行容器存在该漏洞，即该漏洞影响的运行的容器数量。

> **说明：**
>
> 影响容器数量为系统依据漏洞影响的本地镜像所启动的容器进行统计，容器数量目前为检测当时的统计数量，容器状态变化不会更新该统计值。

3. 在漏洞管理页面，支持根据影响资产紧急度和关注紧急度筛选查看相关漏洞列表。

- 影响资产紧急度说明
  - 仅展示影响容器的漏洞：该选项控制过滤影响容器数量不为零的漏洞列表。
  - 仅展示影响最新版本的镜像：该选项控制过滤展示最新版本镜像的漏洞列表。
- 关注紧急度说明
  - 高危及严重：漏洞威胁等级为严重或高危。
  - 重点关注：重点关注漏洞是系统依据风险紧急程度等条件判断得出的，需要优先重点关注的漏洞，通常包含有需要高优紧急处理的风险。
  - 有 POC 或 EXP：漏洞风险标签存在有 EXP、有 POC、EXP/POC 的漏洞。

- 远程 EXP：漏洞度量为 NetWork（远程利用）且存在 EXP 的漏洞。

4. 单击**更多筛选**，支持通过威胁等级、是否可修复、风险标签、CVE 编号、影响镜像 ID、影响镜像名称、影响容器 ID、影响容器名称、漏洞组件版本、漏洞组件名称搜索相关漏洞。

> **说明：**
>
> 基于影响镜像 ID、影响镜像名称、影响容器 ID、影响容器名称搜索漏洞为搜索相关漏洞的可视化信息，相关漏洞的影响本地镜像数量、影响仓库镜像数量、影响容器数量不会变化。

查看漏洞详情

1. 在漏洞管理页面下方，查看检测到的漏洞页面的漏洞信息概览。

2. 在漏洞管理页面，单击该漏洞的**漏洞名称**或操作列的**查看详情**。

3. 在漏洞详情页面，可以查看漏洞详情、影响本地镜像、影响仓库镜像和影响容器。

- 漏洞详情：包含漏洞描述、漏洞类型、危险等级、披露时间、修复方案、影响组件范围以及漏洞特征等信息。

> **说明：**
>
> - 漏洞详情影响范围中的组件及其版本来源为国家漏洞数据库（NVD）中漏洞 CPE 的 Vendor Product 信息，不代表检测的镜像中存在该组件，该影响范围组件名称与影响镜像下实际组件名称可能不一致。
> - 要查看镜像中检出的实际受影响组件，可进入影响本地镜像或影响仓库镜像页面，单击镜像左侧**展开按钮**或单击操作列的**查看组件**。

- 影响本地镜像：查看该漏洞影响本地镜像列表，支持通过镜像名称、组件名称、IP 等信息搜索镜像，支持查看镜像关联主机数和关联容器数。
- 影响仓库镜像：查看该漏洞影响仓库镜像列表，支持通过仓库名称、仓库地址等信息搜索镜像。
- 影响容器：查看该漏洞影响容器列表，支持通过容器名称、容器 ID 等信息搜索镜像。

> **说明：**
>
> 当容器状态发生变化时可能导致影响容器列表数据与漏洞列表中影响容器数不一致。

镜像风险管理
概述

最近更新时间: 2024-08-23 15:08:00

镜像安全可针对本地镜像、仓库镜像提供一键检测功能，支持对漏洞、木马病毒及敏感信息等多维度安全扫描。

镜像安全风险

- 镜像是容器的静态表示形式，镜像的安全决定了容器运行时的安全。
- 镜像的安全风险分布在创建过程、获取来源、获取途径等方面。镜像有以下情况可能存在危险：
  - 镜像存在漏洞或被插入恶意脚本，那么生成的容器也可能产生漏洞或被恶意利用。

> **说明：**
>
> 例如：攻击者可构造特殊的镜像压缩文件，在编译时触发漏洞获取执行任意代码的权限。

- 在镜像中没有指定 USER，默认以 root 用户的身份运行该镜像创建的容器，当该容器遭到攻击，那么宿主机的 root 访问权限也可能会被获取。
- 在镜像文件中存储了固定密码等敏感信息并对外进行发布，则可能导致数据泄露的风险。
- 在镜像的编写中添加了不必要的应用，如 SSH、Telnet 等，则会产生攻击面扩大的风险。

仓库镜像安全风险

镜像仓库作为搭建私有镜像存储仓库的工具，主要安全风险来自仓库本身的安全风险和镜像拉取过程中的传输安全风险。

- 仓库自身安全：镜像仓库特别是私有镜像仓库若被恶意攻击者所控制，那么其中所有镜像的安全性将无法得到保证。

> **说明：**
>
> 例如：私有镜像仓库由于配置不当而开启了2357端口，将会导致私有仓库暴露在公网中，攻击者可直接访问私有仓库并篡改镜像内容，造成仓库内镜像的安全隐患。

- 镜像拉取安全：容器镜像从镜像仓库到用户端的完整性也是镜像安全需关注的内容。

> **说明：**
>
> 例如：用户以明文形式拉取镜像，在与镜像仓库交互的过程中容易遭遇中间人攻击，会导致拉取的镜像在传输过程中被篡改或被冒名发布恶意镜像，造成镜像仓库和用户双方的安全风险。

本地镜像

最近更新时间: 2024-08-23 15:08:00

本文档为您介绍本地镜像功能，并指导您开启扫描数据和查看本地镜像列表。

开启扫描数据

扫描数据展示模块中提供最近扫描检测后的存在风险的镜像数量和镜像总数，镜像存在的安全漏洞、木马病毒和敏感信息数量。

开启一键扫描

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**镜像风险管理** > **本地镜像**。

2. 在本地镜像页面，单击右侧**一键扫描**，可重新扫描获取最新镜像数据或镜像风险信息。

3. 在扫描设置页面，可根据需求选择检测风险类别和镜像范围。

- 检测风险类别：安全漏洞和敏感信息。
- 镜像范围：全部镜像和自选镜像。其中单击所需的自选镜像 或 图标，即可选中或删除自选镜像。

> **说明：**
>
> 支持按住 shift 键进行多选。

4. 选择所需内容后，单击**立即扫描**，即可开始扫描。

> **注意：**

> 开始扫描后，所选择的所有镜像的相同 ID 镜像将同时进行扫描。

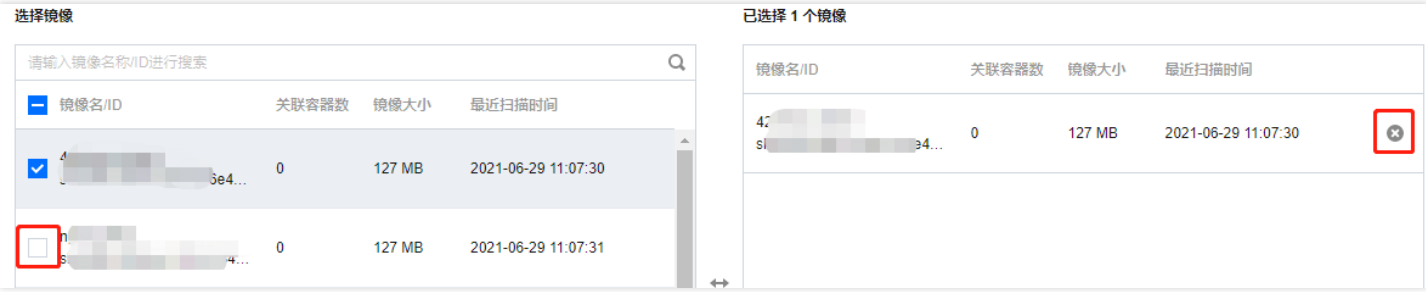
开启定时扫描

1. 在本地镜像页面，单击右侧**定时扫描设置**，可自定义设置是否开启定时扫描功能。

2. 在定时扫描设置页面，单击开启**扫描开关**，并根据需求设置定时扫描时间、检测风险类别和镜像范围。

- 定时扫描时间：可以选择固定周期：1天、7天、15天、30天；以及具体更新时间点。
- 检测风险类别：按需选择安全漏洞、敏感信息和木马病毒。
- 镜像范围：全部镜像和自选镜像。其中单击所需的自选镜像勾选或删除图标，即可选中或删除自选镜像。

> **说明：**
>
> 支持按住 shift 键进行多选。



3. 选择所需内容后，单击**设置**或**取消**，即可完成或取消设置。

开启数据更新

在本地镜像页面，单击右侧**数据更新** > **确认**，可对所有镜像相关安全信息进行立即更新。

> **说明：**
>
> 最长时间需要1~3分钟。

查看本地镜像列表

授权镜像事件

1. 在本地镜像页面，单击**授权**，将未授镜像被授权安全扫描，弹出"授权确认"窗口。

2. 在“授权确认”窗口，单击**确认**，此镜像将被授权安全扫描。

> **说明：**
>
> 确认后，此镜像将被授权安全扫描，操作将消耗1个镜像授权。

筛选镜像资产

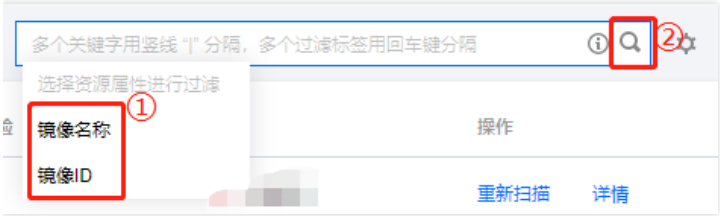
在本地镜像页面，可通过以下操作对镜像资产进行筛选：

- 在本地镜像页面，单击扫描状态下拉框，按扫描状态对镜像资产进行筛选。

- 在本地镜像页面，单击安全状态下拉框，按安全状态对镜像资产进行筛选。

- 在本地镜像页面，勾选仅展示重点关注镜像，可根据系统依据风险紧急程度等条件判断得出的重点关注镜像资产。

- 在本地镜像页面，搜索框通过“镜像名称、镜像 ID”等关键词对镜像资产进行查询。



导出镜像资产

在本地镜像页面，勾选所需的本地镜像后，单击导出图标即可导出镜像资产。

查看列表详情

1. 在本地镜像页面，单击"镜像名称"，右侧弹出抽屉展示镜像详情。

> **说明：**
>
> - 镜像风险：镜像扫描是否成功、安全漏洞数量、木马病毒数量和敏感信息数量。
> - 镜像详情：镜像名称、镜像 ID、镜像大小、操作系统类型。
> - 安全漏洞列表：可按漏洞威胁等级对镜像安全漏洞事件进行筛选，或按漏洞名称检索安全漏洞事件。单击 **查看详情** 可查看漏洞详情及其修复建议。
> - 木马病毒列表：可按木马病毒威胁等级对镜像安全事件进行筛选，或按文件名称检索安全事件。单击 **查看详情** 可查看木马病毒详情及其处置建议。
> - 敏感信息列表：可按敏感信息威胁等级、敏感信息名称和类型对安全事件进行筛选。
> - 镜像构建历史：镜像构建历史日志。

2. 在本地镜像页面，单击"关联主机数"，弹出关联主机详情弹窗，展示了主机名称、主机 IP、Docker 版本等信息。

> **说明：**
>
> 若关联多个主机，还可以通过以下操作筛主机：
>
> - 单击主机状态下拉框，按主机状态对主机进行筛选。
> - 单击搜索框通过"主机名、业务组、Docker 版本"等关键词对主机进行查询。

3. 在本地镜像页面，单击"关联容器数"，弹出关联的容器弹窗，展示了容器名称、容器 ID、容器运行状态、CMD、最近更新时间。

> **说明：**
>
> 若关联多个容器，还可以通过以下操作筛容器：
>
> - 单击状态下拉框，按容器状态对容器进行筛选。
> - 输入主机名称单击“搜索”图标，对主机进行查询。

4. 在本地镜像页面，单击**详情**，右侧抽屉展示镜像详情，展示内容可查看 镜像名称。

扫描镜像事件

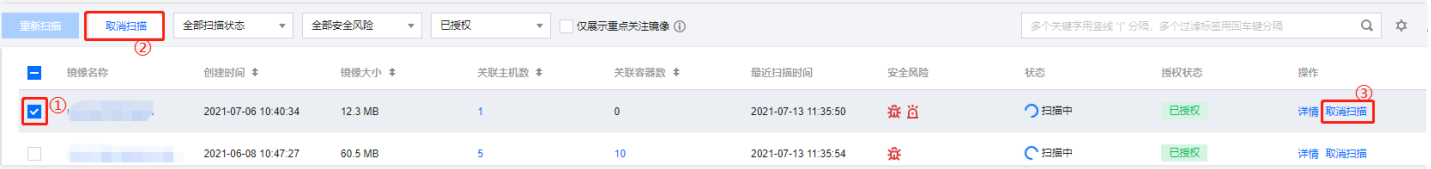
1. 在本地镜像页面，对镜像扫描状态为“未扫描”时，单击**立即扫描** > **确定**，对镜像进行立即扫描。

2. 在本地镜像页面，上一个扫描任务停止后，单击**重新扫描**，对镜像重新扫描。

> **说明：**
>
> 可单击选框勾选多个镜像后，单击②处 **重新扫描** 进行批量重新扫描。

3. 在本地镜像页面，镜像扫描状态为“扫描中”时，单击**取消扫描**，取消扫描镜像。

> **说明：**
>
> 可单击选框勾选多个镜像后，单击②处 **取消扫描** 批量取消扫描任务。



自定义列表管理

1. 在本地镜像页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

2. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 创建时间：镜像创建时间。

2. 最近扫描时间：显示最近一次扫描时间。

3. 安全风险：展示容器存在的安全风险类型。

4. 状态：展示容器扫描状态，包括已扫描、未扫描、扫描中、已取消和扫描异常。

> **说明：**
>
> 扫描异常时建议重新扫描。

仓库镜像

最近更新时间: 2024-08-23 15:08:00

本文档为您介绍仓库镜像功能，并指导您开启扫描数据和查看仓库镜像列表。

> **说明：**
>
> 支持的镜像仓库类型：
>
> - 腾讯云容器镜像服务 TCR/CCR。
> - 第三方镜像仓 Harbor。

前提条件

已购买容器安全服务镜像安全 [增值功能]。

接入容器镜像服务

容器安全服务与容器镜像服务已默认集成，支持对 TCR 和 CCR 仓库进行镜像扫描。

> **说明：**
>
> - 容器安全服务默认通过公网请求 TCR 仓库资产，若您的仓库实例启用了访问控制，使用前请先添加服务 IP 地址段白名单，或切换网络类型。在仓库镜像页面，单击页面上方的**操作指南**展开弹窗，按照配置方法添加 IP 地址白名单或切换网络类型使用 VPC 网络。
> - 首次使用时需手动进行仓库镜像资产数据更新，单击仓库镜像页面右上方的**数据更新**，更新仓库镜像资产，首次同步时间可能较长。
> - 后台每天凌晨0点至3点间会自动同步仓库镜像资产数据。

接入第三方镜像仓 Harbor

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**镜像风险管理** > **仓库镜像**。

2. 在仓库镜像页面，单击右上角的**镜像仓管理**。

3. 在镜像仓库列表中，单击**新增镜像仓**。

4. 在添加镜像仓弹窗中，配置相关参数，单击**确定**。

参数说明：

参数名称	说明
实例名称	填写镜像仓实例名称，实例名称唯一，不可为空
仓库类型	选择第三方镜像仓库类型。目前支持选择harbor仓。
版本	选择第三方镜像仓库的版本。支持选择以下版本： - V1：镜像仓库版本为1.X.X。 - V2：镜像仓库版本为2.X.X及以上。
网络类型	选择第三方镜像仓库的网络访问类型。目前支持**公网**。
地域	选择第三方镜像仓库所在区域，Harbor 类型为默认值“默认地域”。
地址	输入第三方镜像仓库访问地址。
用户名	输入访问第三方镜像仓库的用户名。
密码	输入访问第三方镜像仓库的密码。
限速	选择每小时可同步拉取的镜像个数。默认为不限制。可选值：5、10、20、50、100、500、1000、无限制
验证远程证书	确定镜像同步是否要验证远程镜像仓库实例的证书，如果远程实例使用的是自签或者非信任证书，不要勾选此项。默认为勾选。

开启扫描数据

在 [仓库镜像页面] 扫描数据展示模块中提供最近扫描检测后的存在风险的镜像数量和镜像总数，镜像存在的安全漏洞、木马病毒和敏感信息数量。

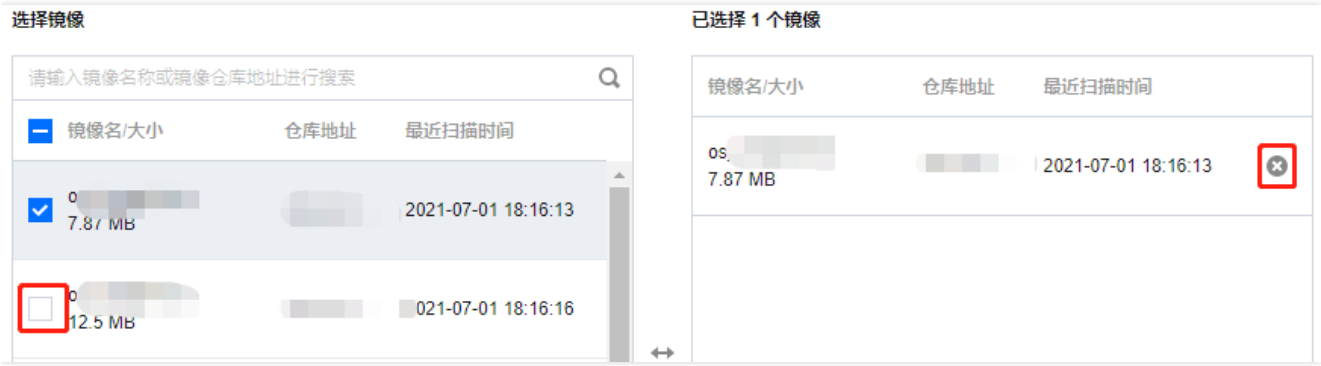
开启一键扫描

1. 在仓库镜像页面，单击右侧**一键扫描**，可获取最新镜像数据或镜像风险信息。

2. 在扫描设置页面，可根据需求选择检测风险类别和镜像范围。

- 检测风险类别：包含安全漏洞和敏感信息。
- 镜像范围：全部镜像和自选镜像。其中单击所需的自选镜像勾选图标，即可选中或删除自选镜像。

> **说明：**
>
> 支持按住 shift 键进行多选。



3. 选择所需内容后，单击**立即扫描**，即可开始扫描。

> **注意：**
>
> 开始扫描后，所选择的所有镜像的相同 ID 镜像将同时进行扫描。

开启定时扫描

1. 在仓库镜像页面，单击右侧**定时扫描设置**，可自定义设置是否开启定时扫描功能。

> **注意：**
>
> 开始扫描后，所选择的所有镜像的相同 ID 镜像将同时进行扫描。

2. 在定时扫描设置页面，单击开启**扫描开关**，并根据需求设置定时扫描时间、检测风险类别和镜像范围。

- 定时扫描时间：可以选择固定周期：1天、7天、15天、30天；以及具体更新时间点。
- 检测风险类别：单击 图标、按需选择安全漏洞、敏感信息和木马病毒。
- 镜像范围：全部镜像和自选镜像。其中单击所需的自选镜像勾选或删除图标，即可选中或删除自选镜像。

> **说明：**

> 支持按住 shift 键进行多选。

3. 选择所需内容后，单击**设置**或**取消**，即可完成或取消设置。

查看仓库镜像列表

登录 [容器安全服务控制台]，在左侧导航中，单击**镜像风险管理** > **仓库镜像**，进入仓库镜像页面。

授权镜像事件

1. 在仓库镜像页面，单击**授权**，将未授镜像被授权安全扫描，弹出"授权确认"窗口。

2. 在"授权确认"窗口，单击**确认**，此镜像将被授权安全扫描。

> **说明：**
>
> 确认后，此镜像将被授权安全扫描，操作将消耗1个镜像授权。

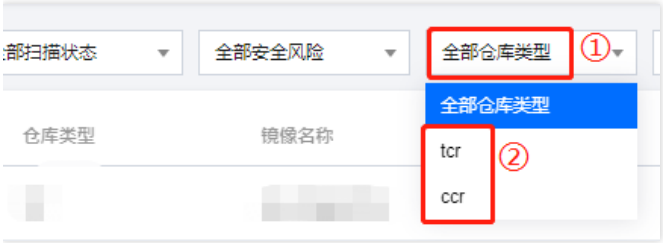
筛选镜像资产

在仓库镜像页面，可通过以下操作对镜像资产进行筛选：

- 在仓库镜像页面，单击扫描状态下拉框，按扫描状态对镜像资产进行筛选。

- 在仓库镜像页面，单击安全状态下拉框，按安全状态对镜像资产进行筛选。

- 在仓库镜像页面，单击仓库类型下拉框，按仓库类型对镜像资产进行筛选。

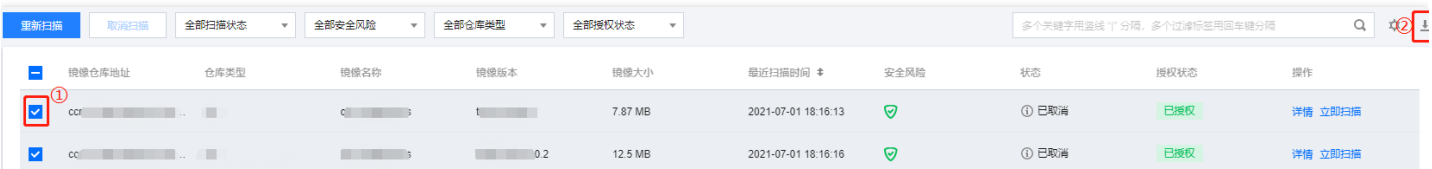


- 在仓库镜像页面，单击授权状态下拉框，按授权状态对镜像资产进行筛选。

- 在仓库镜像页面，单击搜索框，可通过"镜像名称、镜像 Digest"等关键词对镜像资产进行查询。

导出镜像资产

在仓库镜像页面，勾选所需的镜像仓库后，单击导出图标即可导出镜像资产。



查看列表详情

在仓库镜像页面，单击**详情**，右侧抽屉展示镜像详情，可查看镜像风险、镜像详情和安全漏洞列表等信息。

> **说明：**
>
> - 镜像风险：镜像扫描是否成功、安全漏洞数量、木马病毒数量和敏感信息数量。
> - 镜像详情：镜像名称、镜像Digest、镜像大小。
> - 安全漏洞列表：可按漏洞威胁等级对镜像安全漏洞事件进行筛选，或按漏洞名称检索安全漏洞事件。单击**查看详情**查看漏洞详情及其修复建议。
> - 木马病毒列表：可按木马病毒威胁等级对镜像安全事件进行筛选，或按文件名称检索安全事件。单击**查看详情**查看木马病毒详情及其处置建议。
> - 敏感信息列表：可按敏感信息威胁等级、敏感信息名称和类型对安全事件进行筛选。
> - 镜像构建历史：镜像构建历史日志。

扫描镜像事件

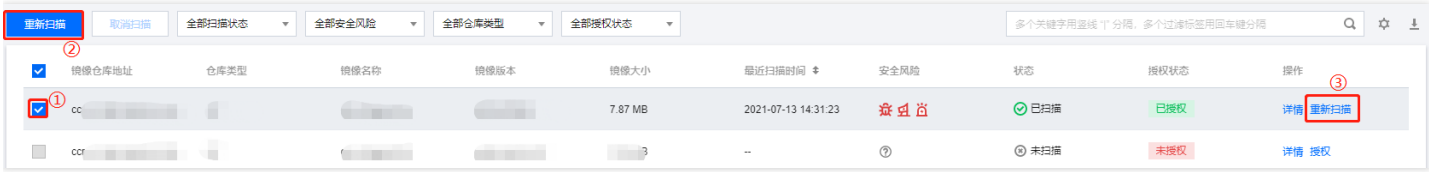
1. 在仓库镜像页面，对镜像扫描状态为“未扫描”时，单击**立即扫描** > **确定**，对镜像进行立即扫描。

2. 在仓库镜像页面，镜像扫描状态为“扫描中”时，单击**取消扫描**，取消扫描镜像。

> **说明：**
>
> 可单击选框勾选多个镜像后，单击②处**取消扫描**批量取消扫描任务。

3. 在仓库镜像页面，上一个扫描任务停止后，单击**重新扫描**，对镜像重新扫描。

> **说明：**
>
> 可单击选框勾选多个镜像后，单击②处**重新扫描**进行批量重新扫描。



自定义列表管理

1. 在仓库镜像页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

2. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表字段说明

1. 镜像仓库地址：仓库镜像来源地址。

2. 仓库类型：镜像仓库的类型，目前包括 tcr、ccr 等。

3. 镜像版本：仓库镜像的版本号。

4. 最近扫描时间：显示最近一次扫描时间。

5. 安全风险：展示容器存在的安全风险类型。

6. 状态：展示容器扫描状态，包括已扫描、未扫描、扫描中、已取消和扫描异常。

> **注意：**
>
> 扫描异常时建议重新扫描。

镜像拦截事件

最近更新时间: 2024-08-23 15:08:00

用户可在 [镜像拦截策略页面]配置告警和拦截策略。镜像拦截策略支持您对存在严重安全问题的镜像进行容器启动拦截，避免恶意镜像运行容器业务。

- 创建并生效拦截策略后，约3-5分钟左右生效。生效后，如命中的风险镜像存在启动容器行为，系统将按照策略配置的告警、拦截要求，对镜像启动行为进行告警、或拦截容器启动并上报拦截记录。
- 目前支持拦截的镜像类型：存在严重&高危漏洞、木马病毒、敏感信息风险的镜像，特权模式启动镜像。
- 拦截特权模式镜像仅支持配置一条规则，如需修改拦截镜像的范围，可编辑调整已配置规则。

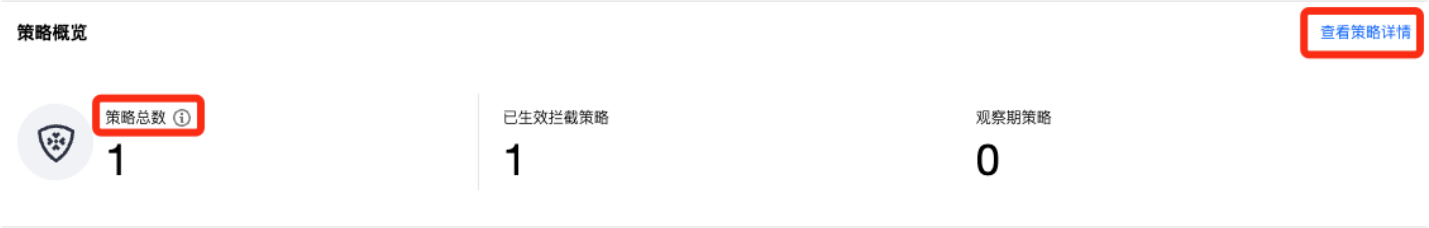
事件概览

用户配置镜像启动拦截策略后，如策略立即生效，则目标风险镜像启动容器时，将实时拦截镜像启动行为并上报事件记录；如策略配置了观察期，观察期仅告警不拦截，则目标风险镜像启动容器时，将实时上报镜像启动行为记录。两种情况均会产生事件记录。

事件概览中，将对每日镜像启动拦截事件和仅告警的事件进行统计，展示近7日两类事件的趋势图和当前的事件总数。

策略概览

在 **镜像拦截策略页面** 配置告警和拦截策略后，系统将统计开启的策略总数，以及其包含的已生效拦截策略和观察期策略数量。可在此部分单击**查看策略详情**，跳转**策略管理** > **镜像拦截策略**页面查看镜像拦截策略详情。



事件列表

事件列表中记录的为已生效拦截策略产生的镜像启动拦截事件和观察期策略产生的镜像启动告警事件。用户可通过事件类型、执行动作、最近生成时间等进行筛选，或通过命中策略、镜像名称、镜像 ID、镜像所在节点名称、节点内网 IP、节点外网 IP 等进行关键字检索。

- 事件类型包括：风险镜像拦截，即镜像包括某些漏洞、木马或敏感信息，需对包含这些风险的镜像进行拦截；特权镜像拦截，即镜像以特权模式启动容器时，进行拦截。
- 执行动作包括：拦截成功，即已生效拦截策略产生的镜像启动拦截事件；告警，即观察期策略产生的镜像启动告警事件。
- 用户可单击操作列的**详情**，查看事件详情，包括事件详情、命中策略、影响范围、风险描述和解决方案。
- 事件详情：系统会对同一镜像的同一拦截或告警事件进行聚合，聚合时间为当天。此部分展示拦截或拦截事件的事件类型、事件数量和发生的时间段。
- 命中策略：展示已生效拦截策略或观察期策略的名称、类型、启动状态、策略状态、开始拦截时间、策略描述和策略拦截内容。用户可单击策略名称/策略类型旁的**详情**，查看此条事件关联的策略详情。
- 影响范围：展示需拦截的目标镜像的名称、镜像 ID、镜像所在节点的名称和 IP 等。
- 风险描述：展示详细的拦截事件或告警事件的原因，例如由于存在严重漏洞，命中拦截策略。同时展示详细的镜像启动参数。
- 解决方案：建议用户对存在漏洞、木马病毒或敏感信息的镜像进行修复，避免影响业务。

集群安全管理
集群检查

最近更新时间: 2024-08-23 15:08:00

集群检查功能提供集群检查列表、集群风险统计、集群检查详情、检查项管理等功能，通过集群检查对指定集群安装检查组件并执行风险检查，查看集群风险详情。

安装集群检查组件

1. 登录 [容器安全服务控制台]，在左侧导航单击**集群安全管理** > **集群检查**。

2. 在集群检查页面，已内置每1小时定期同步集群资产；单击**同步资产**，可进行手动同步集群资产。

> **说明：**
>
> - 目前集群检查列表支持同步的集群资产为 TKE 托管集群 和 TKE 独立集群。
> - 首次使用集群安全时，需要手动进行一次"同步资产"，后续系统会进行自动同步。

3. 在集群检查页面，支持为单个集群或多个集群安装组件。

- 单个：选择所需集群 ID，单击**安装检查组件**或**安装组件**，弹出"确认安装"窗口。

- 多个：选择多个集群 ID，单击**安装组件**，弹出"确认安装"窗口。

4. 在“确认安装”窗口中，单击**确定**，即可为指定集群安装组件。

5. 确认安装后，系统将在集群内所有节点部署 DaemonSet 组件，安装成功后检查组件状态将变更为运行中状态。

> **说明：**
>
> - 集群安装检查组件会在该集群 kube-system 命名空间下安装名称为 cluster-security-defender 的 DaemonSet 类型负载，集群安全检查需确保该 DaemonSet 工作负载正常运行。
> - DaemonSet 对集群运行和性能无影响，占用资源限制为：
> - cpu: 100-250m
> - mem: 100Mi-250Mi.
> - 若需要删除集群检查组件可登录 容器服务控制台 ，在集群详情页面单击**工作负载**，选择 DaemonSet，在 kube-system 命名空间下选择 cluster-security-defender 操作单击**更多** > **删除**。

执行集群检查

在 [集群检查页面]，检查组件安装成功后系统会自动执行一次集群检查，您也可指定集群单击**重新检查**或指定多个集群单击**批量检查**执行集群检查。

> **说明：**
>
> 集群检查组件默认为未安装状态，执行集群检查前需要先安装检查组件。

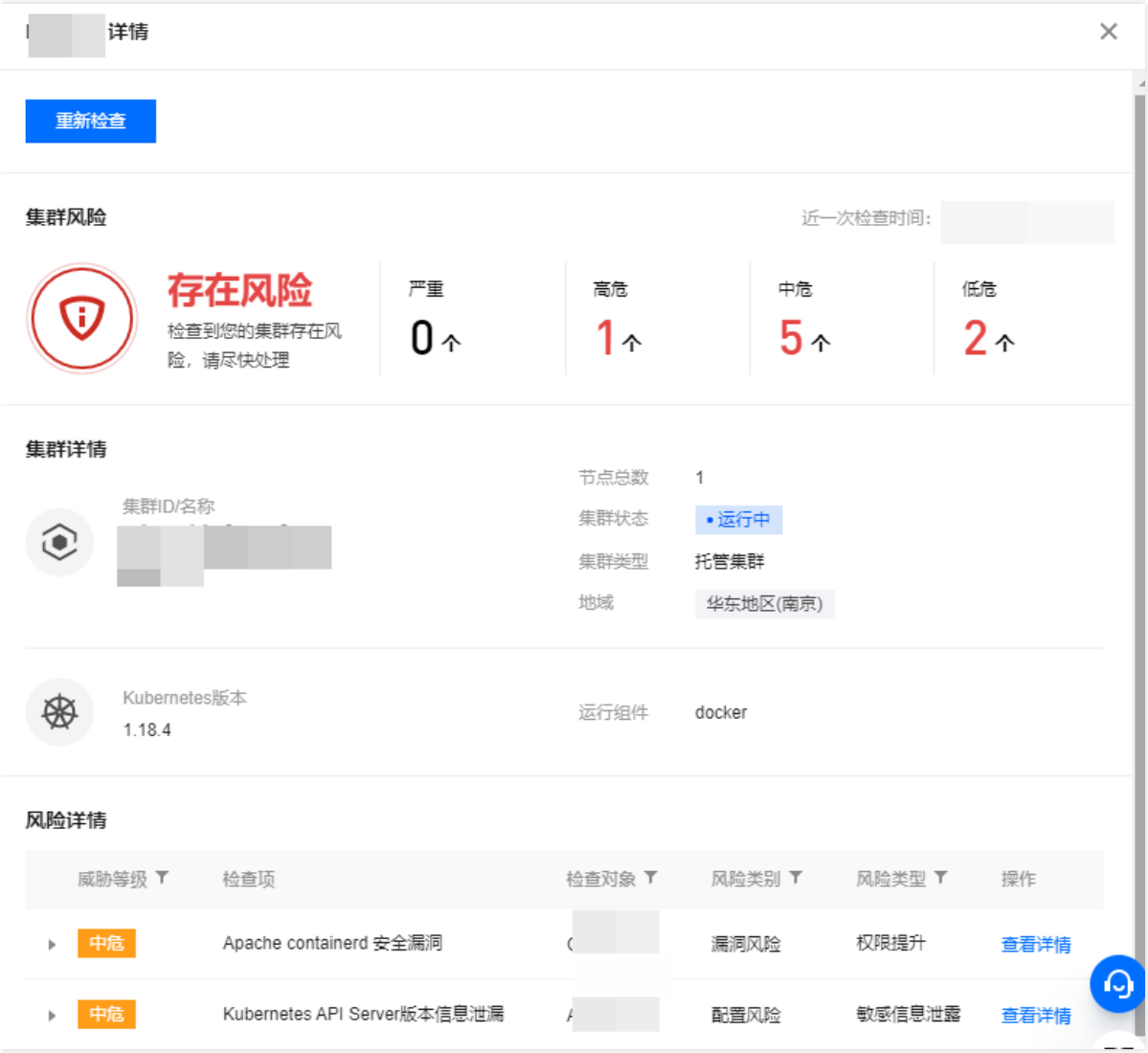
查看集群检查结果

1. 在 [集群检查页面]，集群统计卡片展示集群总数、无风险集群数量以及未检查集群数量。

2. 集群风险卡片展示已检查集群中存在风险的风险集群数量、严重风险的集群数量、高危风险的集群数量、中危风险的集群数量和低危风险的集群数量。

3. 在集群检查页面，单击集群列表操作列的**查看详情**，进入“集群风险详情”页面。

4. 在“集群风险详情”页面，展示了当前集群所有被检出的集群风险、集群详情和风险详情。



5. 在风险详情列表，选择所需风险检查项，单击**查看详情**，进入“风险检查项详情”页面。

6. 在“风险检查项详情”页面，展示该风险检测项的风险详情、风险描述、解决方案以及当前集群的影响资产范围。

开启自动检查

单个开启自动检测

1. 在 [集群检查页面]，选择所需集群，单击自动检查的开关按钮，弹出“确认开启”窗口。

2. 在“确认开启”窗口中，单击**确定**，即可为当前集群开启自动检查。

> **说明：**
>
> 确认后，自动检查将开启。检测内容如下：
>
> - 当集群节点有新增时，自动对集群新增节点进行一次检查。
> - 每日凌晨将对集群所有节点进行一次检查。

批量开启自动检测

在 [集群检查页面]，选择多个集群，单击**批量检测**，即可批量开启集群自动检查。

> **说明：**
>
> 集群自动检查默认为关闭状态，集群自动检查说明如下：
>
> - 当集群节点有新增时，自动对集群新增节点进行一次检查。
> - 每日凌晨将对集群所有节点进行一次检查。

管理集群检查项

1. 在 [集群检查页面]，单击界面右上角的**检测项管理**，进入检查项设置页面。

2. 在检查项设置页面，检查项列表展示了系统执行集群检查的所有检查项，单击**查看详情**可查看检查项的详细信息。

自建集群

最近更新时间: 2024-08-23 15:08:00

接入自建集群

本文介绍接入自建集群的步骤，您可以将自建集群接入容器安全服务进行统一管理，对自建集群开展集群风险检查和管理。

限制条件

接入自建集群节点规模小于500节点。

操作步骤

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**集群安全管理** > **集群检查**。

2. 在集群检查页面，单击**接入自建集群**。

3. 在集群信息设置页面，配置相关参数，单击**下一步**。

参数说明：

参数组	参数	说明	可选项
基础信息设置	集群名称	输入自建集群的名称，64字符以内	-
	集群环境	选择自建集群的类型	Kubernetes,Openshift
	集群版本	选择集群环境的集群版本	K8s 集群支持1.13以上版本
网络信息设置	网络类型	选择通过公网或通过 VPC 网络接入自建集群	公网、VPC
	所在地域	选择自建集群所在的地域，公网类型无地域限制	-
	VPC ID	当网络类型使用 VPC 时，选择集群所在网络的 VPC 信息	-
	API Server地址	当网络类型使用 VPC 时，选择集群 API Server 后端服务类型	服务器、负载均衡
集群检查组件	安装检查组件	选择自动或者自行手动安装集群检查的组件	- 自动安装检查组件并进行一次集群检查 - 不安装检查组件，接入后自行安装组件并下发集群安装
	自动检查	是否开启集群的自动检查功能	- 开启 - 关闭

4. 在上传配置文件，单击**选择文件**，上传本地文件后，单击**完成接入**即可接入自建集群。

> 注意：
>
> - 公网方式接入自建集群，如果您的集群有**设置访问控制策略**，需单击 **IP 白名单地址**添加页面中的 IP 地址。
> - 您需要在服务器上生成 K8s 配置文件后，才能上传该配置文件。生成K8s 配置文件的具体操作，请参见 生成 K8S 配置文件。
> - 上传配置文件，大小需要在 1M 以内。

生成 K8s 配置文件

本文指导您生成容器安全需要的最小化权限 K8s 配置文件。您可参照文档步骤生成配置文件，或者参见 **一键脚本**。

前提条件

• 已在服务器上搭建 K8s 集群。具体操作，请参见 K8s 中文官方文档。 • 已安装 Docker 服务。

操作步骤

1. 以 root 身份登录 k8s 集群 master 所在服务器。

2. 输入如下命令，创建命名空间和权限绑定。

```
# 1. 创建命名空间： tcss
# 2. 创建命名空间tcss下的管理角色： tcss-admin
# 3. 绑定角色tcss-admin和用户tcss
# 4. 创建秘钥并绑定服务账号： tcss-agent-secret，tcss-agent
# 5. 创建只读的集群角色： security-clusterrole
# 6. 绑定集群角色security-clusterrole到服务账号tcss-agent

---
apiVersion: v1
kind: Namespace
```

```
metadata:
name: tcss


---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
namespace: tcss
name: tcss-admin
rules:
- apiGroups: ["extensions", "apps", ""]
resources: ["*"]
verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]

---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
name: tcss-admin-rb
namespace: tcss
subjects:
- kind: User
name: tcss
apiGroup: rbac.authorization.k8s.io
roleRef:
kind: Role
name: tcss-admin
apiGroup: rbac.authorization.k8s.io


---
apiVersion: v1
kind: Secret
metadata:
name: tcss-agent-secret
namespace: tcss
annotations:
kubernetes.io/service-account.name: tcss-agent
type: kubernetes.io/service-account-token


---
apiVersion: v1
kind: ServiceAccount
metadata:
name: tcss-agent
namespace: tcss
secrets:
- name: tcss-agent-secret
namespace: tcss


---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
name: security-clusterrole
rules:
- apiGroups: ["", "v1"]
resources: ["namespaces", "pods", "nodes"]
verbs: ["get", "list"]
- apiGroups: ["apps"]
```

```
resources: ["replicasets", "daemonsets", "deployments", "statefulsets"]
verbs: ["get", "list"]
- apiGroups: ["networking.k8s.io"]
resources: ["networkpolicies"]
verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
- apiGroups: ["batch"]
resources: ["jobs", "cronjobs"]
verbs: ["get", "list"]
- apiGroups: ["rbac.authorization.k8s.io"]
resources: ["clusterroles", "clusterrolebindings"]
verbs: ["get"]
- apiGroups: ["networking.k8s.io", "extensions"]
resources: ["ingresses"]
verbs: ["get", "list"]

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
name: security-clusterrolebinding
roleRef:
apiGroup: rbac.authorization.k8s.io
kind: ClusterRole
name: security-clusterrole
subjects:
- kind: ServiceAccount
name: tcss-agent
namespace: tcss
- kind: User
name: tcss
apiGroup: rbac.authorization.k8s.io
```

> **说明：**
>
> 执行上述命令，如果能显示 pod 或者显示当前命名空间下没有相关资源，则表示该集群配置是可用的，上传该文件 /root/tcss.conf 即可。

一键脚本

在 mater 节点中，您可基于以下一键脚本代码一键快速生成集群配置文件：

> **说明：**
>
> 环境需要提前安装 openssl。

```
#!/bin/bash

set -e;

# API_SERVER 需要设置为公网可访问的地址和端口
# API_SERVER=https://xx.xx.xx.xx:xxxx

# 以下路径,用户根据集群实际情况设定
KUBECONFIG_TARGET=/root/tcss.conf
CA_FILE=/etc/kubernetes/ca.crt
CAKEY_FILE=/etc/kubernetes/ca.key
TCSS_TMPDIR=/tmp/tcss
# 如果是OpenShift环境，可以更换为 oc
KUBECTL_CMD=kubectl


if [ ! $API_SERVER ]; then
echo "API_SERVER does not set.";
exit 1;
```

```
fi
if ! which kubectl ; then
echo "kubectl does not exist.";
exit 1;
fi
if [ ! -f "$CA_FILE" ]; then
echo "$CA_FILE does not exist.";
exit 1;
fi
if [ ! -f "$CAKEY_FILE" ]; then
echo "$CAKEY_FILE does not exist.";
exit 1;
fi
if [ ! -d $TCSS_TMPDIR ]; then
mkdir -p $TCSS_TMPDIR;
fi

cat <<EOF > $TCSS_TMPDIR/tcss_res.yaml
---
apiVersion: v1
kind: Namespace
metadata:
name: tcss

---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
namespace: tcss
name: tcss-admin
rules:
- apiGroups: ["extensions", "apps", ""]
resources: ["*"]
verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]

---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
name: tcss-admin-rb
namespace: tcss
subjects:
- kind: User
name: tcss
apiGroup: rbac.authorization.k8s.io
roleRef:
kind: Role
name: tcss-admin
apiGroup: rbac.authorization.k8s.io

---
apiVersion: v1
kind: Secret
metadata:
name: tcss-agent-secret
namespace: tcss
annotations:
kubernetes.io/service-account.name: tcss-agent
type: kubernetes.io/service-account-token

---
apiVersion: v1
kind: ServiceAccount
```

```
metadata:
name: tcss-agent
namespace: tcss
secrets:
- name: tcss-agent-secret
namespace: tcss

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
name: security-clusterrole
rules:
- apiGroups: ["", "v1"]
resources: ["namespaces", "pods", "nodes"]
verbs: ["get", "list"]
- apiGroups: ["apps"]
resources: ["replicasets", "daemonsets", "deployments", "statefulsets"]
verbs: ["get", "list"]
- apiGroups: ["networking.k8s.io"]
resources: ["networkpolicies"]
verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
- apiGroups: ["batch"]
resources: ["jobs", "cronjobs"]
verbs: ["get", "list"]
- apiGroups: ["rbac.authorization.k8s.io"]
resources: ["clusterroles", "clusterrolebindings"]
verbs: ["get"]
- apiGroups: ["networking.k8s.io", "extensions"]
resources: ["ingresses"]
verbs: ["get", "list"]

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
name: security-clusterrolebinding
roleRef:
apiGroup: rbac.authorization.k8s.io
kind: ClusterRole
name: security-clusterrole
subjects:
- kind: ServiceAccount
name: tcss-agent
namespace: tcss
- kind: User
name: tcss
apiGroup: rbac.authorization.k8s.io
EOF

# echo "generate tcss resource file ($TCSS_TMPDIR/tcss_res.yaml) success."

$KUBECTL_CMD apply -f $TCSS_TMPDIR/tcss_res.yaml;

# 创建User私钥 tcss.key。
openssl genrsa -out $TCSS_TMPDIR/tcss.key 2048
# 创建证书签署请求 tcss.csr
openssl req -new -key $TCSS_TMPDIR/tcss.key -out $TCSS_TMPDIR/tcss.csr -subj "/O=K8s/CN=tcss"
# 签署证书 生成 tcss.crt
openssl x509 -req -in $TCSS_TMPDIR/tcss.csr -CA $CA_FILE -CAkey $CAKEY_FILE -CAcreateserial -out $TCSS_TMPDIR/tcss.crt -days 365

# 创建并设置集群配置
$KUBECTL_CMD config set-cluster tcss --server=$API_SERVER --certificate-authority=$CA_FILE --embed-certs=true --kubeconfig=$KUB
```

```
ECONFIG_TARGET
# 创建并设置用户配置
$KUBECTL_CMD config set-credentials tcss --client-certificate=$TCSS_TMPDIR/tcss.crt --client-key=$TCSS_TMPDIR/tcss.key --embed-ce
rts=true --kubeconfig=$KUBECONFIG_TARGET
# 设置context配置
$KUBECTL_CMD config set-context tcss@tcss --cluster=tcss --user=tcss --kubeconfig=$KUBECONFIG_TARGET
# 切换context配置
$KUBECTL_CMD config use-context tcss@tcss --kubeconfig=$KUBECONFIG_TARGET

echo "generate KUBECONFIG file success. $KUBECONFIG_TARGET"
```

生成 Openshift 配置文件

本文指导您生成容器安全需要的最小化权限 OpenShift 配置文件。您可参照文档步骤生成配置文件，或者参见 **一键脚本**。

前提条件

1. 已在服务器上搭建 K8s 集群。具体操作，请参见 K8s 中文官方文档。

2. 已安装 Docker 服务。

3. 暂仅支持 OpenShift3.0及以上版本接入，低于该版本可能存在不确定性问题。

操作步骤

> **说明：**
>
> 整体接入思路和 Kubernetes 类似，只涉及相关路径和命令行工具区别，如果集群 master 节点上已经安装的 kubectl 工具，则可以完全同 Kubernetes 集群接入方式进行接入。

1. 以 root 身份登录 OpenShift 集群 master 所在服务器。

2. 输入如下命令，创建命名空间和权限绑定。

```
# 1. 创建命名空间： tcss
# 2. 创建命名空间tcss下的管理角色： tcss-admin
# 3. 绑定角色tcss-admin和用户tcss
# 4. 创建秘钥并绑定服务账号： tcss-agent-secret，tcss-agent
# 5. 创建只读的集群角色： security-clusterrole
# 6. 绑定集群角色security-clusterrole到服务账号tcss-agent

---
apiVersion: v1
kind: Namespace
metadata:
name: tcss


---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
namespace: tcss
name: tcss-admin
rules:
- apiGroups: ["extensions", "apps", ""]
resources: ["*"]
```

```
verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]

---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
name: tcss-admin-rb
namespace: tcss
subjects:
- kind: User
name: tcss
apiGroup: rbac.authorization.k8s.io
roleRef:
kind: Role
name: tcss-admin
apiGroup: rbac.authorization.k8s.io


---
apiVersion: v1
kind: Secret
metadata:
name: tcss-agent-secret
namespace: tcss
annotations:
kubernetes.io/service-account.name: tcss-agent
type: kubernetes.io/service-account-token


---
apiVersion: v1
kind: ServiceAccount
metadata:
name: tcss-agent
namespace: tcss
secrets:
- name: tcss-agent-secret
namespace: tcss


---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
name: security-clusterrole
rules:
- apiGroups: ["", "v1"]
resources: ["namespaces", "pods", "nodes"]
verbs: ["get", "list"]
- apiGroups: ["apps"]
resources: ["replicasets", "daemonsets", "deployments", "statefulsets"]
verbs: ["get", "list"]
- apiGroups: ["networking.k8s.io"]
resources: ["networkpolicies"]
verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
- apiGroups: ["batch"]
resources: ["jobs", "cronjobs"]
verbs: ["get", "list"]
- apiGroups: ["rbac.authorization.k8s.io"]
resources: ["clusterroles", "clusterrolebindings"]
verbs: ["get"]
- apiGroups: ["networking.k8s.io", "extensions"]
resources: ["ingresses"]
```

```
verbs: ["get", "list"]

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
name: security-clusterrolebinding
roleRef:
apiGroup: rbac.authorization.k8s.io
kind: ClusterRole
name: security-clusterrole
subjects:
- kind: ServiceAccount
name: tcss-agent
namespace: tcss
- kind: User
name: tcss
apiGroup: rbac.authorization.k8s.io
```

3. 进入配置目录（/etc/origin/master/），输入如下命令，创建证书。

```
# 创建User私钥 tcss.key。
openssl genrsa -out tcss.key 2048

# 创建证书签署请求 tcss.csr
openssl req -new -key tcss.key -out tcss.csr -subj "/O=K8s/CN=tcss"

# 签署证书 生成 tcss.crt
openssl x509 -req -in tcss.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out tcss.crt -days 365
```

4. 输入如下命令，创建集群配置文件。

```
# 创建并设置集群配置, 其中需要主要 server 地址必须为公网可访问地址
KUBECONFIG=/root/tcss.conf oc config set-cluster tcss --server=https://xx.xx.xx.xx:60002 --certificate-authority=/etc/origin/master/ca.crt --embed-certs=true --kubeconfig=/root/tcss.conf

# 创建并设置用户配置
KUBECONFIG=/root/tcss.conf oc config set-credentials tcss --client-certificate=tcss.crt --client-key=tcss.key --embed-certs=true --kubeconfig=/root/tcss.conf

# 设置context配置
KUBECONFIG=/root/tcss.conf oc config set-context tcss@tcss --cluster=tcss --user=tcss --kubeconfig=/root/tcss.conf

# 切换context配置
KUBECONFIG=/root/tcss.conf oc config use-context tcss@tcss --kubeconfig=/root/tcss.conf
```

5. 输入如下命令，验证集群配置文件并上传配置。

```
KUBECONFIG=/root/tcss.conf oc -n tcss get pod
```

> **说明：**
>
> 执行上述命令，如果能显示pod或者显示当前命名空间下没有相关资源则表示该集群配置是可用的，上传该文件 /root/tcss.conf 即可。

一键脚本

在 mater 节点中，您可基于以下一键脚本代码一键快速生成集群配置文件：

> **说明：**
>
> 环境需要提前安装 openssl。

```
#!/bin/bash

set -e;

# API_SERVER 需要设置为公网可访问的地址和端口
# API_SERVER=https://xx.xx.xx.xx:xxxx

# 以下路径,用户根据集群实际情况设定
KUBECONFIG_TARGET=/root/tcss.conf
CA_FILE=/etc/kubernetes/ca.crt
CAKEY_FILE=/etc/kubernetes/ca.key
TCSS_TMPDIR=/tmp/tcss
KUBECTL_CMD=oc


if [ ! $API_SERVER ]; then
echo "API_SERVER does not set.";
exit 1;
fi
if ! which $KUBECTL_CMD ; then
echo "$KUBECTL_CMD does not exist.";
exit 1;
fi
if [ ! -f "$CA_FILE" ]; then
echo "$CA_FILE does not exist.";
exit 1;
fi
if [ ! -f "$CAKEY_FILE" ]; then
echo "$CAKEY_FILE does not exist.";
exit 1;
fi
if [ ! -d $TCSS_TMPDIR ]; then
mkdir -p $TCSS_TMPDIR;
fi

cat <<EOF > $TCSS_TMPDIR/tcss_res.yaml
---
apiVersion: v1
kind: Namespace
metadata:
name: tcss

---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
namespace: tcss
name: tcss-admin
rules:
- apiGroups: ["extensions", "apps", ""]
resources: ["*"]
verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]

---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
name: tcss-admin-rb
namespace: tcss
subjects:
- kind: User
name: tcss
```

```
apiGroup: rbac.authorization.k8s.io
roleRef:
kind: Role
name: tcss-admin
apiGroup: rbac.authorization.k8s.io

---
apiVersion: v1
kind: Secret
metadata:
name: tcss-agent-secret
namespace: tcss
annotations:
kubernetes.io/service-account.name: tcss-agent
type: kubernetes.io/service-account-token

---
apiVersion: v1
kind: ServiceAccount
metadata:
name: tcss-agent
namespace: tcss
secrets:
- name: tcss-agent-secret
namespace: tcss

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
name: security-clusterrole
rules:
- apiGroups: ["", "v1"]
resources: ["namespaces", "pods", "nodes"]
verbs: ["get", "list"]
- apiGroups: ["apps"]
resources: ["replicasets", "daemonsets", "deployments", "statefulsets"]
verbs: ["get", "list"]
- apiGroups: ["networking.k8s.io"]
resources: ["networkpolicies"]
verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
- apiGroups: ["batch"]
resources: ["jobs", "cronjobs"]
verbs: ["get", "list"]
- apiGroups: ["rbac.authorization.k8s.io"]
resources: ["clusterroles", "clusterrolebindings"]
verbs: ["get"]
- apiGroups: ["networking.k8s.io", "extensions"]
resources: ["ingresses"]
verbs: ["get", "list"]

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
name: security-clusterrolebinding
roleRef:
apiGroup: rbac.authorization.k8s.io
kind: ClusterRole
name: security-clusterrole
subjects:
- kind: ServiceAccount
name: tcss-agent
```

```
namespace: tcss
- kind: User
name: tcss
apiGroup: rbac.authorization.k8s.io
EOF

# echo "generate tcss resource file ($TCSS_TMPDIR/tcss_res.yaml) success."

$KUBECTL_CMD apply -f $TCSS_TMPDIR/tcss_res.yaml;
$KUBECTL_CMD adm policy add-scc-to-user privileged -n tcss -z tcss-agent;
$KUBECTL_CMD adm policy add-scc-to-user hostaccess -n tcss -z tcss-agent;
$KUBECTL_CMD adm policy add-scc-to-user privileged tcss;
$KUBECTL_CMD adm policy add-scc-to-user hostaccess tcss;
oc adm policy add-cluster-role-to-user cluster-reader tcss;

# 创建User私钥 tcss.key。
openssl genrsa -out $TCSS_TMPDIR/tcss.key 2048
# 创建证书签署请求 tcss.csr
openssl req -new -key $TCSS_TMPDIR/tcss.key -out $TCSS_TMPDIR/tcss.csr -subj "/O=K8s/CN=tcss"
# 签署证书 生成 tcss.crt
openssl x509 -req -in $TCSS_TMPDIR/tcss.csr -CA $CA_FILE -CAkey $CAKEY_FILE -CAcreateserial -out $TCSS_TMPDIR/tcss.crt -days 365

# 创建并设置集群配置
KUBECONFIG=$KUBECONFIG_TARGET $KUBECTL_CMD config set-cluster tcss --server=$API_SERVER --certificate-authority=$CA_FILE --
embed-certs=true --kubeconfig=$KUBECONFIG_TARGET
# 创建并设置用户配置
KUBECONFIG=$KUBECONFIG_TARGET $KUBECTL_CMD config set-credentials tcss --client-certificate=$TCSS_TMPDIR/tcss.crt --client-ke
y=$TCSS_TMPDIR/tcss.key --embed-certs=true --kubeconfig=$KUBECONFIG_TARGET
# 设置context配置
KUBECONFIG=$KUBECONFIG_TARGET $KUBECTL_CMD config set-context tcss@tcss --cluster=tcss --user=tcss --kubeconfig=$KUBECO
NFIG_TARGET
# 切换context配置
KUBECONFIG=$KUBECONFIG_TARGET $KUBECTL_CMD config use-context tcss@tcss --kubeconfig=$KUBECONFIG_TARGET

echo "generate KUBECONFIG file success. $KUBECONFIG_TARGET"
```

风险分析

最近更新时间: 2024-08-23 15:08:00

风险分析功能展示所有已检查集群存在的风险统计，包括风险节点趋势以及风险项信息。

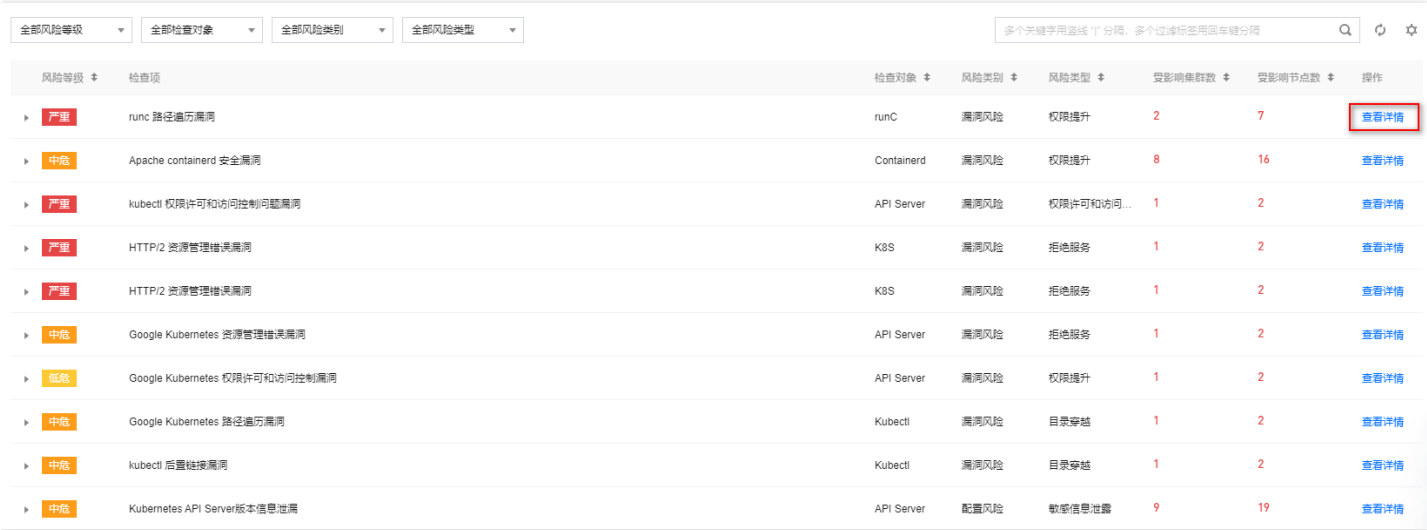
查看风险节点统计

1. 登录 [容器安全服务控制台]，在左侧导航单击**集群安全管理** > **风险分析**。

2. 在风险分析页面的查案风险节点统计卡片，展示集群检查所发现的风险节点数量以及过去七天内风险节点的数量趋势，包括严重风险节点和趋势、高危风险节点和趋势、中危风险节点和趋势、低危风险节点和趋势。

查看风险项信息

在 [风险分析页面]的风险项列表，展示了当前集群检查发现的所有风险项，风险项信息包括风险等级、检查项信息、检查对象、风险类别、风险类型、受影响集群数、受影响节点数。单击风险项的**查看详情**，进入风险项详情弹窗，可查看当前风险项的风险详情、风险描述、解决方案以及风险的所有影响范围。



基线管理

概述

最近更新时间: 2024-08-23 15:08:00

安全基线支持 CIS Benchmark 标准并结合腾讯云鼎实验室最佳基线配置实践，可对容器、镜像、主机、kubernetes 资产环境 配置进行安全标准检查，多维度展现容器资产的基线合规情况并帮助建立容器运行环境下的最佳基线配置，减少攻击面。

容器

最近更新时间: 2024-08-23 15:08:00

容器页面展示容器资产的基线合规情况，包括基线概览、检测信息、容器检测项结果列表。

查看容器概览

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **容器**。

2. 在容器页面，基线概览窗口展示合规容器占比百分比和严重、高危、中危、低危四个威胁等级的检测项数量。

> **说明：**
>
> 合规容器占比百分比计算逻辑为：合规容器资产数量/容器总数（含检查失败数量）。

3. 在容器页面，单击百分比中的**查看**，可在弹出的容器抽屉中查看容器资产的检测结果列表。

4. 在容器抽屉中，单击搜索框，可通过“基线检测项和 ID”关键词对容器资产的检测结果进行查询。

5. 在容器抽屉中，单击 图标勾选所需的容器基线检测项后，单击**重新检查** > **确定**，对选中的容器基线检测项进行重新检测。

6. 在容器抽屉中，单击**基线检测项**，可查看指定容器的基线检测情况。

查看检测信息

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **容器**。

2. 在容器页面，检测信息窗口展示容器资产最近一次的基线检测时间、检测耗时和自动检测周期配置。

3. 在容器页面，单击**重新检测**，可立即对容器资产进行一次基线检测。

4. 在容器页面，单击**基线设置**，可设置基线策略和基线忽略列表。

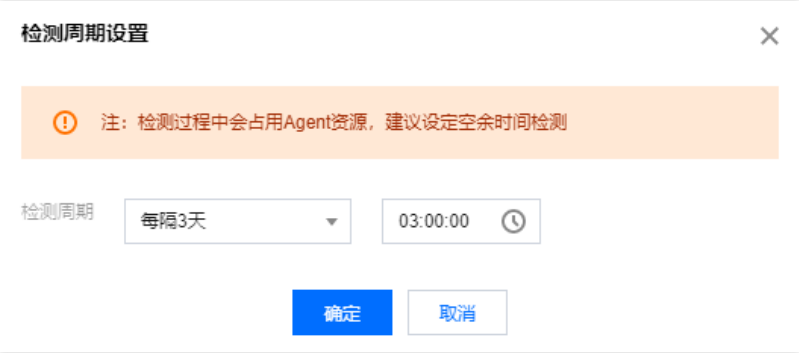
设置基线策略

基线策略设置展示当前资产检测的基线标准，基线检查项数量。

1. 在基线策略设置页面，可通过单击开关图标开关开启或关闭当前基线标准的周期性检测。

2. 在基线策略设置页面，单击**检测周期设置**，弹出检测周期设置弹窗，可在检测周期设置弹窗中设定检测周期。

3. 在检测周期设置弹窗，可设置检测周期为：1天、3天、7天，以及设定具体时间点。



4. 单击**确定**，即可完成检测周期设置。

基线忽略列表

基线忽略列表展示了忽略的容器基线检测项。

1. 在基线忽略列表页面，单击搜索框，可通过"基线检测项"关键词对容器基线检测项进行查询。

2. 在基线忽略列表页面，单击 图标勾选所需的容器基线检测项后，单击**取消忽略**，将会对选中的容器基线检测项取消忽略。

> **说明：**
>
> 检测项取消忽略后，检测内容将恢复正常检测。

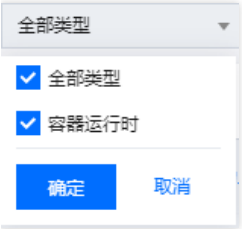
查看检测结果列表

筛选刷新基线检测项

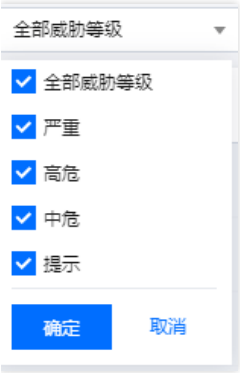
1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **容器**。

2. 在容器页面，单击搜索框，可通过"ID 和基线检测项"关键词对容器基线检测项进行查询。

3. 在容器页面，单击左上角的类型下拉框，按类型对容器基线检测项进行筛选。



4. 在容器页面，单击左上角的威胁等级下拉框，按威胁等级对容器基线检测项进行筛选。



5.在容器页面，单击操作栏右侧刷新图标，即可刷新容器基线检测项。

重新检测基线检测项

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **容器**。

2. 在容器页面，单击勾选所需容器基线检测项后，单击**重新检测** > **确认**，可对容器基线检测项产进行重新检测。

> **说明：**
>
> 选定多个容器基线检测项，单击②处的**重新检测**，可进行批量检测。

忽略基线检测项

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **容器**。

2. 在容器页面，单击勾选所需基线检测项后，单击**忽略** > **确定**，可对基线检测项进行忽略。

> **说明：**
>
> 选定多个基线检测项，单击②处的**忽略**，可进行批量忽略。

自定义列表管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **容器**。

2. 在容器页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 基线检测项：单击“基线检测项”，可查看检测项详情。

2. 未通过检测项：未通过的检测项数量。

3. 检测结果：存在未通过的检测项检测结果为未通过，所有检测项通过则检测结果为已通过。

4. 最近检测时间：最近一次的检测时间。

镜像

最近更新时间: 2024-08-23 15:08:00

镜像页面展示镜像资产的基线合规情况，包括基线概览、检测信息、镜像检测项结果列表。

查看镜像概览

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **镜像**。

2. 在镜像页面，基线概览窗口展示合规镜像占比百分比严重、高危、中危、低危四个威胁等级的检测项数量。

> **说明：**
>
> 合规镜像占比百分比计算逻辑为：合规镜像资产数量/镜像总数（含检查失败数量）。

3. 在镜像页面，单击百分比中的**查看**，可在弹出的镜像抽屉中查看镜像资产的检测结果列表。

4. 在镜像抽屉中，单击搜索框，可通过“基线检测项和 ID”关键词对镜像资产的检测结果进行查询。

5. 在镜像抽屉中，单击 图标勾选所需的镜像基线检测项后，单击**重新检测** > **确定**，将会对选中的资产基线检测项进行重新检测。

> **说明：**
>
> 选定多个镜像基线检测项，单击②处的**重新检测**，可进行批量重新检测。

6. 在镜像抽屉中，单击**基线检测项**，可查看指定镜像的基线检测情况。

查看检测信息

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **镜像**。

2. 在镜像页面，检测信息窗口展示镜像资产最近一次的基线检测时间、检测耗时和自动检测周期配置。

3. 在镜像页面，单击**重新检测**，可立即对镜像资产进行一次基线检测。

4. 在镜像页面，单击**基线设置**，可设置基线策略和基线忽略列表。

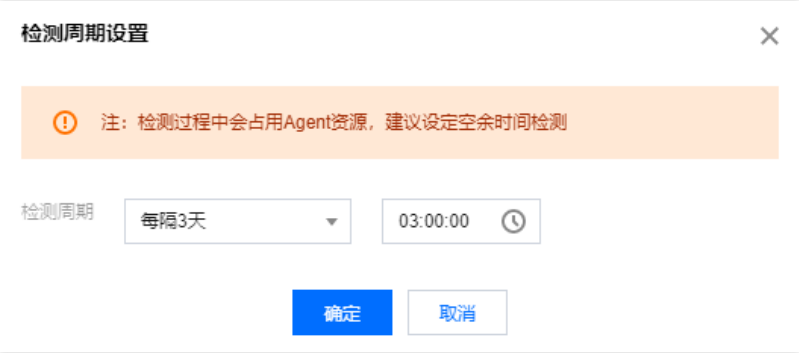
设置基线策略

基线策略设置展示当前资产检测的基线标准，基线检查项数量。

1. 在基线策略设置页面，可通过单击开关图标开关开启或关闭当前基线标准的周期性检测。

2. 在基线策略设置页面，单击**检测周期设置**，弹出检测周期设置弹窗，可在检测周期设置弹窗中设定检测周期。

3. 在检测周期设置弹窗，可设置检测周期为：1天、3天、7天，以及设定具体时间点。



4. 单击**确定**，即可完成检测周期设置。

基线忽略列表

基线忽略列表展示了忽略的镜像基线检测项。

1. 在基线忽略列表页面，单击搜索框，可通过"基线检测项"关键词对镜像基线检测项进行查询。

2. 在基线忽略列表页面，单击 图标勾选所需的镜像基线检测项后，单击**取消忽略**，将会对选中的镜像基线检测项取消忽略。

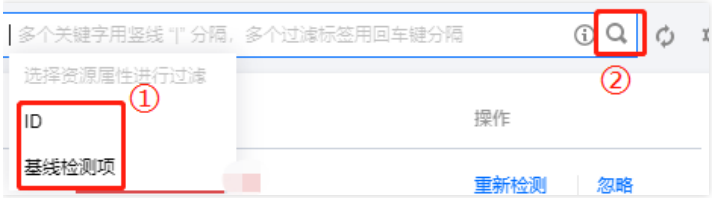
> **说明：**
>
> 检测项取消忽略后，检测内容将恢复正常检测。

查看检测结果列表

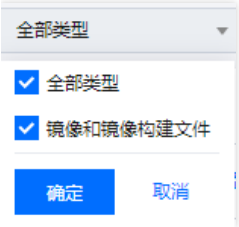
筛选刷新基线检测项

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **镜像**。

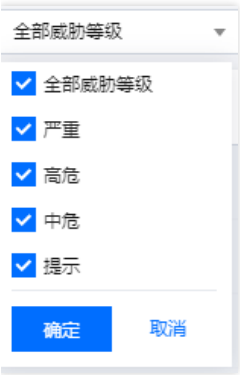
2. 在镜像页面，单击搜索框，可通过"ID 和基线检测项"关键词对镜像基线检测项进行查询。



3. 在镜像页面，单击左上角的类型下拉框，按类型对镜像基线检测项进行筛选。



4. 在镜像页面，单击左上角的威胁等级下拉框，按威胁等级对镜像基线检测项进行筛选。



5. 在镜像页面，单击操作栏右侧刷新图标，即可刷新事件列表。

重新检测基线检测项

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **镜像**。

2. 在镜像页面，单击勾选所需镜像基线检测项后，单击**重新检测** > **确认**，可对镜像基线检测项进行重新检测。

> **说明：**
>
> 选定多个镜像基线检测项，单击②处的**重新检测**，可进行批量检测。

忽略基线检测项

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **镜像**。

2. 在镜像页面，单击勾选所需基线检测项后，单击**忽略** > **确定**，可对基线检测项进行忽略。

> **说明：**
>
> 选定多个基线检测项，单击②处的**忽略**，可进行批量忽略。

自定义列表管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **镜像**。

2. 在镜像页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. ID：检测项ID，该ID全局唯一。

2. 基线检测项：检测内容，单击“基线检测项”，可查看检测项详情。

3. 类型：检测项的类型。

4. 基线标准：检测项所属基线标准。

5. 威胁等级：检测项的威胁等级定义，含严重、高危、中危、底危、提示。

6. 检测结果：展示当前检测项下通过的资产数量和未通过的资产数量。

7. 操作：重新检测和忽略。

Docker主机

最近更新时间: 2024-08-23 15:08:00

Docker 主机页面展示主机资产的基线合规情况，包括基线概览、检测信息、主机检测项结果列表。

查看 Docker 主机概览

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **Docker 主机**。

2. 在 Docker 主机页面，基线概览窗口展示合规主机占比百分比中严重、高危、中危、低危四个威胁等级的检测项数量。

> **说明：**
>
> 合规 Docker 主机占比百分比计算逻辑为：合规 Docker 主机资产数量/Docker 主机总数（含检查失败数量）。

3. 在 Docker 主机页面，单击百分比中的**查看**，可在弹出的主机抽屉中查看主机资产的检测结果列表。

4. 在 Docker 主机抽屉中，单击搜索框，可通过"基线检测项和 ID"关键词对主机资产的检测结果进行查询。

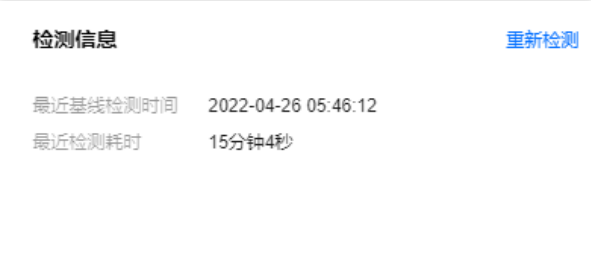
5. 在 Docker 主机抽屉中，单击 图标勾选所需的 Docker 主机基线检测项后，单击**重新检测** > **确定**，将会对选中的基线检测项进行重新检测。

> **说明：**
>
> 选定多个主机基线检测项，单击②处的**重新检测**，可进行批量重新检测。

6. 在 Docker 主机抽屉中，单击**基线检测项**，可查看指定 Docker 主机的基线检测情况。

查看检测信息

1. 在 Docker 主机页面，检测信息窗口展示主机资产最近一次的基线检测时间、检测耗时和自动检测周期配置。



2. 在 Docker 主机页面，单击**重新检测**，可立即对主机资产进行一次基线检测。

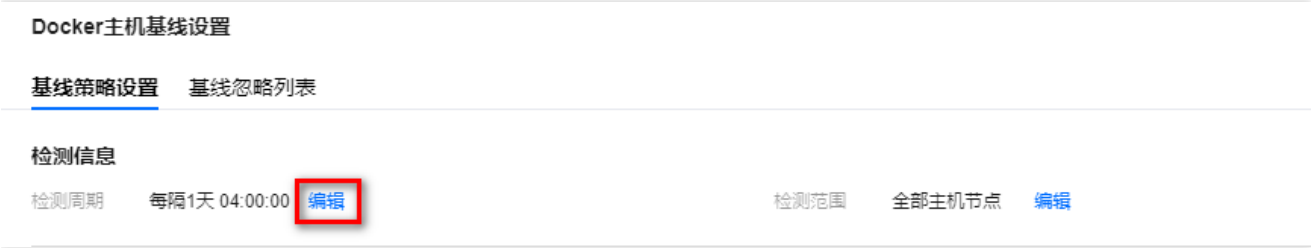
3. 在 Docker 主机页面，单击**基线设置**，可设置基线策略和基线忽略列表。

设置基线策略

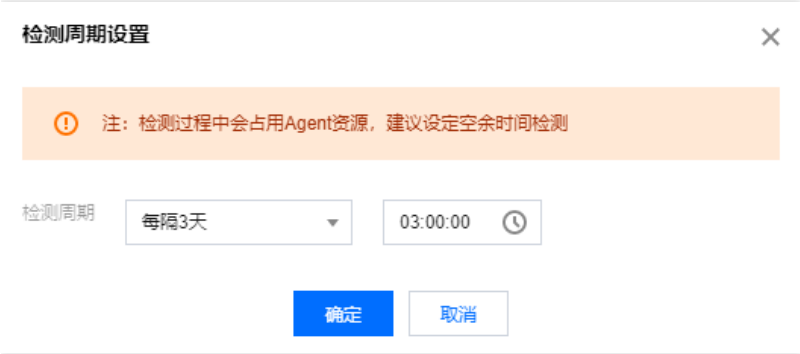
基线策略设置展示当前资产检测的基线标准，基线检查项数量。

1. 在基线策略设置页面，可通过单击开关图标开关开启或关闭当前基线标准的周期性检测。

2. 在基线策略设置页面，单击检测周期的**编辑**，弹出检测周期设置弹窗，可在检测周期设置弹窗中设定检测周期。



3. 在检测周期设置弹窗，可设置检测周期为：1天、3天、7天，以及设定具体时间点。



4. 单击**确定**，即可完成检测周期设置。

基线忽略列表

基线忽略列表展示了忽略的主机基线检测项。

1. 在基线忽略列表页面，单击搜索框，可通过"基线检测项、主机名称、主机 IP"关键词对主机基线检测项进行查询。

2. 在基线忽略列表页面，单击 图标勾选所需的主机基线检测项后，单击**取消忽略**，将会对选中的主机基线检测项取消忽略。

> **说明：**
>
> 检测项取消忽略后，检测内容将恢复正常检测。

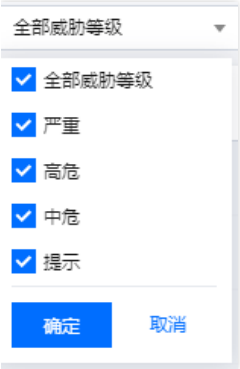
查看检测结果列表

筛选刷新基线检测项

1. 在 Docker 主机页面，单击搜索框，可通过"ID 和基线检测项"关键词对 Docker 主机基线检测项进行查询。

2. 在 Docker 主机页面，单击左上角的类型下拉框，按类型对 Docker 主机基线检测项进行筛选。

3. 在 Docker 主机页面，单击左上角的威胁等级下拉框，按威胁等级对 Docker 主机基线检测项进行筛选。



4. 在 Docker 主机页面，单击操作栏右侧刷新图标，即可刷新事件列表。

重新检测基线检测项

在 Docker 主机页面，单击勾选所需 Docker 主机基线检测项后，单击**重新检测** > **确认**，可对主机基线检测项进行重新检测。

> **说明：**
>
> 选定多个主机基线检测项，单击②处的**重新检测**，可进行批量检测。

忽略基线检测项

在 Docker 主机页面，单击勾选所需基线检测项后，单击**忽略** > **确定**，可对基线检测项进行忽略。

> **说明：**
>
> 选定多个基线检测项，单击②处的**忽略**，可进行批量忽略。

自定义列表管理

1. 在 Docker 主机页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

2. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. ID：检测项ID，该ID全局唯一。

2. 基线检测项：检测内容，单击“基线检测项”，可查看检测项详情。

3. 类型：检测项的类型。

4. 基线标准：检测项所属基线标准。

5. 威胁等级：检测项的威胁等级定义，含严重、高危、中危、底危、提示。

6. 检测结果：展示当前检测项下通过的资产数量和未通过的资产数量。

7. 操作：重新检测和忽略。

Kubernetes

最近更新时间: 2024-08-23 15:08:00

Kubernetes 页面基于 CIS Kubernetes Benchmark 标准展示 K8S 资产的基线合规情况，包括基线概览、检测信息、Kubernetes 检测项结果列表。

查看 Kubernetes 概览

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **Kubernetes**。

2. 在 Kubernetes 页面，基线概览窗口展示合规 K8S 检测项通过率占比以及严重、高危、中危、低危四个威胁等级的检测项数量。

> **说明：**
>
> 检测项通过率计算逻辑为：通过的检测项数量/检测项总数。

3. 在 Kubernetes 页面，单击百分比中的**查看**，可在弹出的抽屉中查看 Kubernetes 资产的检测结果列表。

4. 在 Kubernetes 页面，单击搜索框，可通过"ID 和基线检查项"关键词对 Kubernetes 基线检测项的检测结果进行查询。

5. 在 Kubernetes 页面，单击 图标勾选所需的 Kubernetes 基线检测项后，单击**重新检测** > **确定**，将会对选中的 Kubernetes 基线检测项进行重新检测。

> **说明：**
>
> 选定多个 Kubernetes 基线检测项，单击②处的**重新检测**，可进行批量重新检测。

查看检测信息

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **Kubernetes**。

2. 在 Kubernetes 页面，检测信息窗口展示 Kubernetes 基线检测项最近一次的基线检测时间、检测耗时和自动检测周期配置。

3. 在 Kubernetes 页面，单击**重新检测**，可立即对 Kubernetes 基线检测项进行一次基线检测。

4. 在 Kubernetes 页面，单击**基线设置**，可设置基线策略和基线忽略列表。

设置基线策略

基线策略设置展示当前资产检测的基线标准，基线检查项数量。

1. 在基线策略设置页面，可通过单击开关图标开关开启或关闭当前基线标准的周期性检测。

2. 在基线策略设置页面，单击检测周期的**编辑**，弹出检测周期设置弹窗，可在检测周期设置弹窗中设定检测周期。

3. 在检测周期设置弹窗，可设置检测周期为：1天、3天、7天，以及设定具体时间点。

4. 单击**确定**，即可完成检测周期设置。

基线忽略列表

基线忽略列表展示了忽略的容器基线检测项。

1. 在基线忽略列表页面，单击搜索框，可通过"基线检测项、主机名称、主机 IP"关键词对 Kubernetes 基线检测项进行查询。

2. 在基线忽略列表页面，单击 图标勾选所需的 Kubernetes 资产后，单击**取消忽略**，将会对选中的 Kubernetes 基线检测项取消忽略。

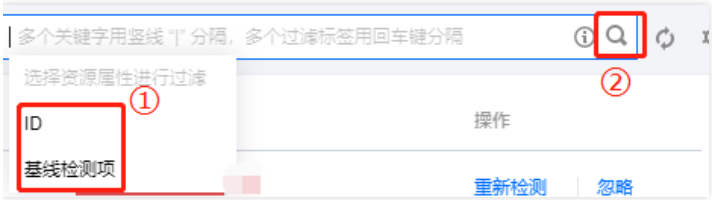
> **说明：**
>
> 检测项取消忽略后，检测内容将恢复正常检测。

查看检测结果列表

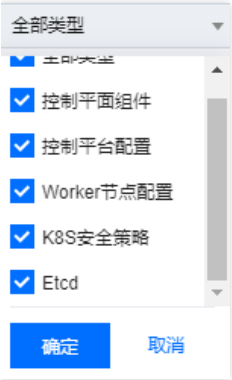
筛选刷新基线检测项

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **Kubernetes**。

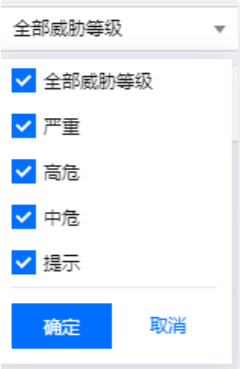
2. 在 Kubernetes 页面，单击搜索框，可通过"基线检测项"关键词对 Kubernetes 基线检测项进行查询。



3. 在 Kubernetes 页面，单击左上角的类型下拉框，按类型对 Kubernetes 基线检测项进行筛选。



4. 在 Kubernetes 页面，单击左上角的威胁等级下拉框，按威胁等级对 Kubernetes 基线检测项进行筛选。



5. 在 Kubernetes 页面，单击操作栏右侧刷新图标，即可刷新Kubernetes 基线检测项。

重新检测基线检测项

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **Kubernetes**。

2. 在 Kubernetes 页面，单击勾选所需 Kubernetes 基线检测项后，单击**重新检测** > **确认**，可对 Kubernetes 基线检测项进行重新检测。

> 说明：

> 选定多个 Kubernetes 基线检测项，单击②处的**重新检测**，可进行批量检测。

忽略基线检测项

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **Kubernetes**。

2. 在 Kubernetes 页面，单击勾选所需 Kubernetes 基线检测项后，单击**忽略** > **确定**，可对 Kubernetes 基线检测项进行忽略。

> **说明：**
>
> 选定多个 Kubernetes 基线检测项，单击②处的**忽略**，可进行批量忽略。

自定义列表管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**基线管理** > **Kubernetes**。

2. 在 Kubernetes 页面，单击刷新图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. ID：检测项ID，该ID全局唯一。

2. 基线检测项：检测内容，单击“基线检测项”，可查看检测项详情。

3. 类型：检测项的类型。

4. 基线标准：检测项所属基线标准。

5. 威胁等级：检测项的威胁等级定义，含严重、高危、中危、底危、提示。

6. 检测结果：展示当前检测项下通过的资产数量和未通过的资产数量。

7. 操作：重新检测和忽略。

运行时安全
概述

最近更新时间: 2024-08-23 15:08:00

运行时安全支持自适应识别黑客攻击，实时监控和防护容器运行时安全，提供容器逃逸、反弹 Shell 和文件查杀安全功能。

- 容器逃逸：指的是容器利用系统漏洞，“逃逸”出了其自身所拥有的权限，实现了对宿主机和宿主机上其他容器的访问。由于容器与宿主机共享操作系统内核，为了避免容器获取宿主机的 root 权限，通常不允许采用特权模式运行容器。按照入侵者执行容器逃逸的顺序，容器安全服务将风险事件类型划分为三类，分别是：风险容器、程序提权、容器逃逸。
- 风险容器：指当前容器存在部分潜在风险行为，可能会存在被提权或被逃逸的风险，包含敏感路径挂载、特权容器。
- 程序提权：指当前容器出现了提权的风险行为，可能会进一步导致其逃逸，需要您进行关注。
- 容器逃逸：指当前容器已经出现了逃逸行为，此时您应该立即对出现的风险事件进行关注，并立即通过推荐解决方案进行对应的处置响应。
- 反弹shell：基于腾讯云安全技术及多维度多手段，对 Shell 反向连接行为进行识别记录，为您运行时容器提供反弹 Shell 行为的实时监控能力。
- 文件查杀：通过实时监测运行容器调用的文件是否存在风险；或手动触发一键扫描，检查容器内是否存在恶意的木马病毒、webshell 等。

容器逃逸

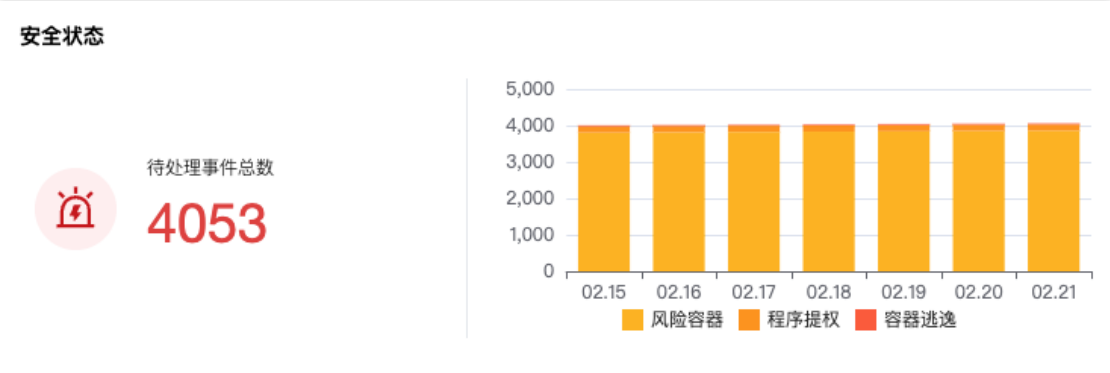
最近更新时间: 2024-08-23 15:08:00

事件列表

查看设置状态

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**运行时安全** > **容器逃逸**，进入容器逃逸页面。

2. 在容器逃逸页面，安全状态模块展示是否存在容器逃逸事件。如检测发现容器逃逸事件，建议立即处理。



3. 在容器逃逸页面，监控状态模块展示系统支持检测的容器逃逸事件类型，单击可开启图标，可自定义设置监控状态。

查看容器逃逸列表

登录 [容器安全服务控制台]，在左侧导航中，单击**运行时安全** > **容器逃逸**，进入容器逃逸页面。

筛选刷新容器逃逸

1. 在容器逃逸页面，单击搜索框，可通过"容器名称、镜像名称和节点名称"等关键词对容器逃逸事件进行查询。

2. 在容器逃逸页面，单击操作栏右侧刷新图标，即可刷新容器逃逸事件。

导出容器逃逸

在容器逃逸页面，单击勾选所需的容器逃逸事件后，单击导出图标即可导出容器逃逸事件。

> **说明：**
>
> 可单击)图标勾选多个逃逸事件后，单击 图标可进行批量导出。

事件状态处理

在容器逃逸页面，可对容器逃逸事件进行标记已处理、忽略和删除处理。

- 标记已处理：单击勾选所需的容器逃逸事件后，单击**标记已处理** > **确定**，即可将选中事件标记已处理。

> **说明：**
>
> 建议您参照事件详情中的"解决方案"，人工对该事件风险进行处理，可将事件标记为已处理。

- 忽略：单击勾选所需的容器逃逸事件后，单击**忽略** > **确定**，即可将选中事件忽略。

> **说明：**
>
> 仅将已选事件进行忽略，若再有相同事件发生依然会进行告警。

- 删除：单击勾选所需的容器逃逸事件后，单击**删除** > **确定**，即可将选中事件删除。

> **注意：**
>
> 删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

查看列表详情

1. 在容器逃逸页面，单击事件类型左侧展开图标，可查看事件描述。

2. 在容器逃逸页面， 单击“容器名称/ID ”或”镜像名称/ID”，可跳转至对应的资产管理列表。

3. 在容器逃逸页面，单击**查看详情**，右侧抽屉展示事件详情信息，包括告警事件详情、进程信息和事件描述。

4. 在容器逃逸页面，事件状态包含已处理、已忽略和待处理。可对不同状态的事件进行以下操作：

- 已处理：单击**删除**，并在弹窗中进行二次确认删除，可将事件删除。

> **说明：**
>
> 删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

- 待处理：单击**立即处理**，可将事件标记为已处理、忽略或删除该事件，详情请参见 **事件状态处理**。

- 已忽略：单击**取消忽略**或**删除**，可将事件变为待处理或删除。

自定义列表管理

1. 在容器逃逸页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

2. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表字段说明

1.事件类型：容器逃逸告警事件类型，包括宿主机文件访问逃逸、MountNamespace 逃逸、程序提权逃逸、特权容器启动逃逸、敏感路径挂载和 Syscall 逃逸。

2.首次生成时间：该逃逸事件首次触发告警的时间。

> **说明：**
>
> 系统默认对未处理的相同逃逸事件进行告警聚合。

3.最近生成时间：聚合的告警事件最近触发告警的时间。可单击右侧"排序"按钮对列表事件按时间正序和时间反序进行排列。

4.事件数量：聚合时间范围内该逃逸事件触发告警的总数量。

5.状态：包括已处理、已忽略、未处理、已加白，支持按状态对列表事件进行快速筛选。

逃逸白名单

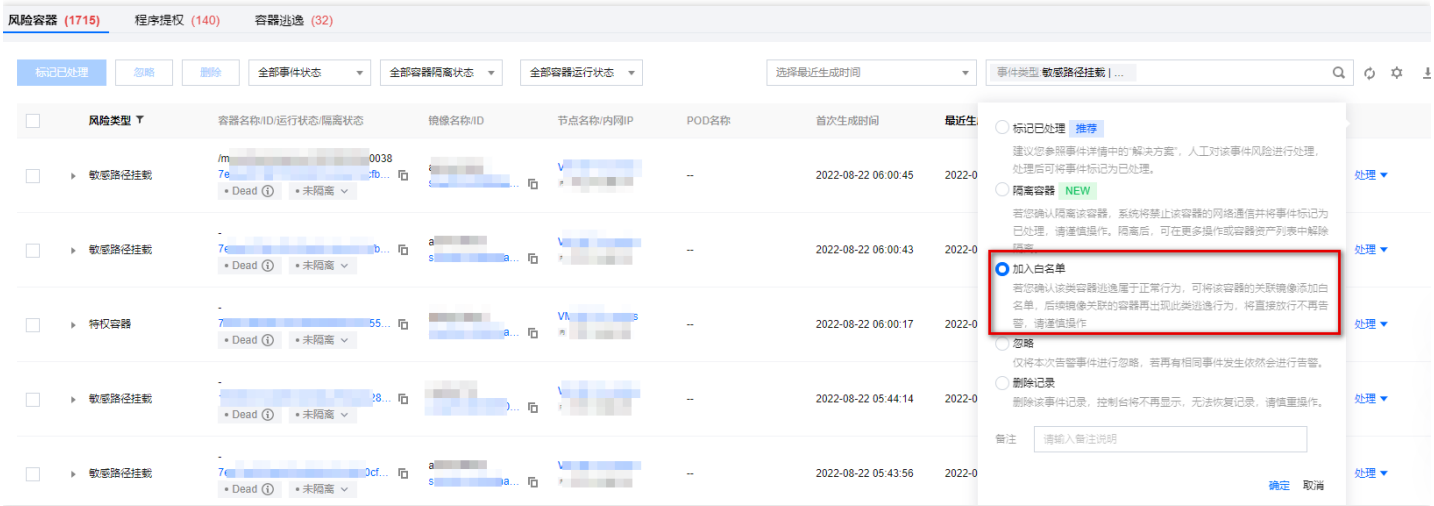
排查容器逃逸告警时，如部分业务容器需以特权模式启动、需挂载敏感路径或其他会导致逃逸告警的配置，可进行加白处理。加白操作分类两类：根据告警事件加白和在白名单管理页面新建白名单。

加白告警事件

1. 在 [容器逃逸页面] ，如需对告警事件进行加白，单击**处理**，选择加入白名单，单击**确定**。

> **注意：**

> 若您确认该类容器逃逸属于正常行为，可将该容器的关联镜像添加白名单，**后续镜像关联的容器再出现此类逃逸行为，将直接放行不再告警，请谨慎操作。**



2. 在添加白名单镜像页面，默认勾选告警事件中关联的逃逸告警类型和来源镜像，您也可以在此基础上增加勾选加白事件类型和需要加白的镜像，单击**确定**即可完成白名单配置。

3. 如需对某种事件类型进行全部镜像加白，您可以单击监控状态右侧的**监控设置**，对开启监控的风险类型进行调整。

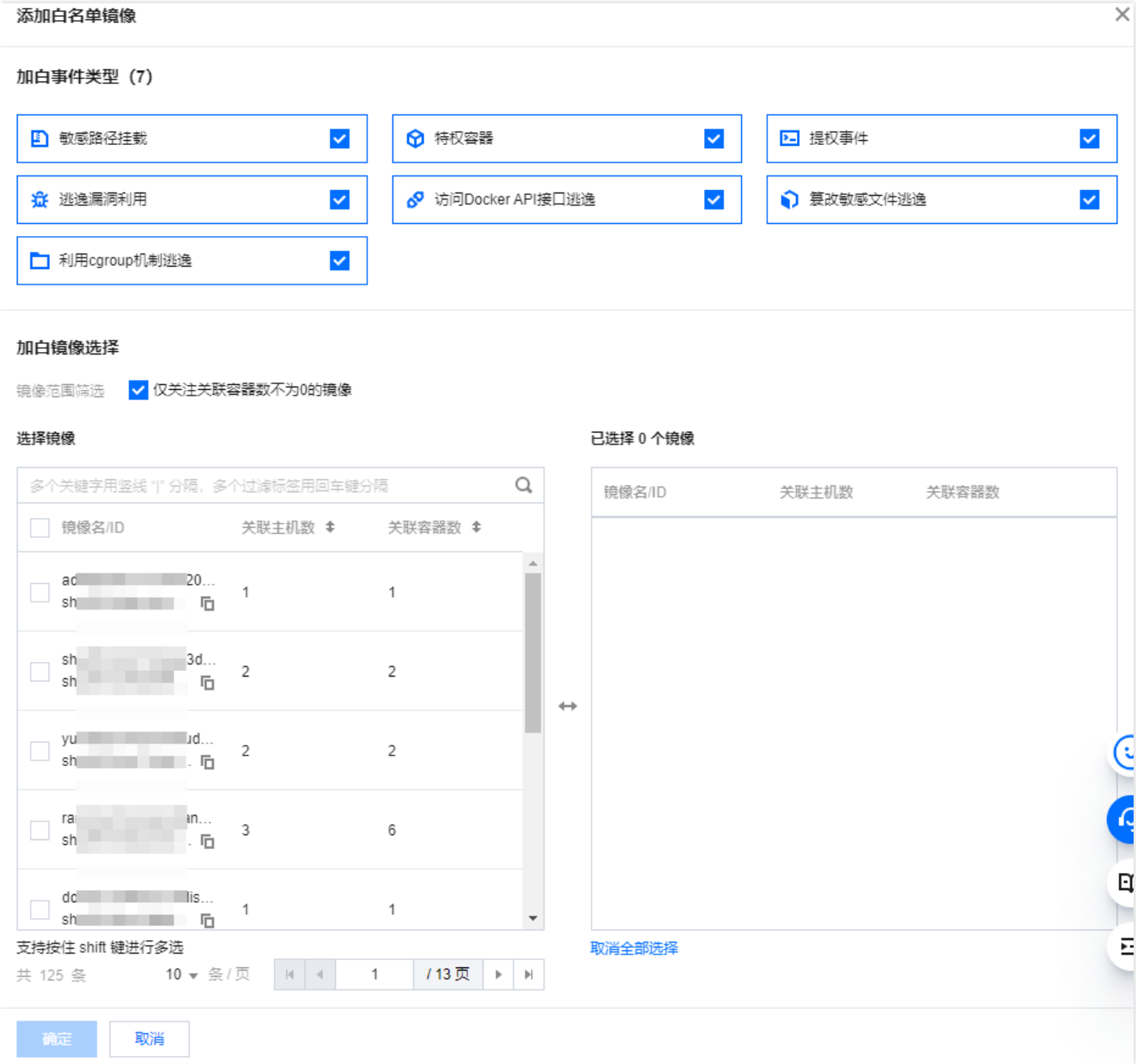
白名单管理

用户也可在白名单管理页面，批量新增白名单，避免后续产生告警。

添加白名单

1. 在 [容器逃逸] > **白名单管理**页面，单击**添加白名单策略**。

2. 在添加白名单镜像页面，选择加白事件类型和生效的镜像，也可批量选择需加白的事件类型和生效的镜像，单击**确定**。



3. 添加白名单完毕后，白名单管理列表以镜像 ID 对白名单进行统一管理，展示每一个镜像已加白的事件类型。例如添加白名单时勾选了3个镜像，那么列表中将更新3条白名单镜像记录。

编辑白名单

- 编辑单个白名单

1. 在 [容器逃逸] > **白名单管理**页面，单击目标镜像操作列的**编辑加白类型**。

2. 在编辑加白事件类型对话框中，修改加白事件类型，单击**保存**。

- 批量编辑白名单 如需批量对多个镜像进行加白事件类型变更、**且这些镜像需加白的类型一致**，按照如下操作修改：

  -在 [容器逃逸] > **白名单管理**页面，选择一个或多个镜像，单击左上角的**编辑加白类型**。

-在编辑加白事件类型对话框中，修改加白事件类型，单击**保存**。

> **注意：**
>
> 对所选镜像进行事件类型编辑后，原先已设置的事件类型内容将被清空。

删除白名单

1. 在 [容器逃逸] > **白名单管理**页面，可删除单个白名单或批量删除白名单。

- 删除单个白名单： 选择所需镜像，单击操作列的**删除**。

- 批量删除白名单：选择一个或多个镜像，单击左上角的**删除**。

2. 在确认删除对话框中，单击**确认**，即可删除目标白名单。

> **注意：**
>
> 确认删除后将无法恢复，该白名单镜像在触发此类逃逸时将再次产生告警。

反弹shell
事件列表

最近更新时间: 2024-08-23 15:08:00

本文档介绍反弹 Shell 功能的事件列表。

筛选刷新事件列表

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**运行时安全** > **反弹 Shell** > **事件列表**，进入事件列表页面。

2. 在事件列表页面，单击搜索框，可通过"进程名称、父进程名称"等关键词对反弹 Shell 事件进行查询。

3. 在事件列表页面，单击操作栏右侧刷新图标，即可刷新反弹 Shell 事件列表。

导出事件列表

在事件列表页面，单击勾选所需的反弹 Shell 事件后，单击导出图标即可导出反弹 Shell 事件。

> **说明：**
>
> 可单击 图标勾选多个反弹 Shell 事件后，单击 图标可进行批量导出。

事件状态处理

在事件列表页面，可对反弹 Shell 事件列表进行标记已处理、忽略和删除处理。

- 标记已处理：单击勾选反弹 Shell 事件后，单击**标记已处理** > **确定**，即可将选中事件标记已处理。

> **说明：**
>
> 建议您参照事件详情中的“解决方案”，人工对该事件风险进行处理，可将事件标记为已处理。

- 忽略：单击勾选所需的反弹 Shell 事件后，单击**忽略** > **确定**，即可将选中事件忽略。

> **说明：**
>
> 仅将已选事件进行忽略，若再有相同事件发生依然会进行告警。

- 删除：单击勾选所需的反弹 Shell 事件后，单击**删除** > **确定**，即可将选中事件删除。

> **注意：**
>
> 删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

查看列表详情

1. 在事件列表页面，单击事件类型左侧展开图标，可查看事件描述。

2. 在事件列表页面，单击“容器名称/ID ”或“镜像名称/ID”，可跳转至对应的资产管理列表。

3. 在事件列表页面，单击**查看详情**，右侧抽屉展示事件详细信息，包括告警事件详情、进程信息、父进程信息和事件描述。

4. 在事件列表页面，事件状态包含已处理、已忽略、待处理。可对不同状态的事件进行以下操作：

- 已处理/已加白：单击**删除**，并在弹窗中进行二次确认删除，可将事件删除。

> **说明：**
>
> 删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

- 待处理：单击**立即处理**，可将事件标记为已处理、忽略、删除和添加白名单，详情请参见 事件状态处理。
- 已忽略：单击**取消忽略**或**删除**，可将事件变为待处理或删除。

自定义列表管理

1. 在事件列表页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

2. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 首次生成时间：该 Shell 反向连接事件首次触发告警的时间。

> **说明：**
>
> 系统默认对未处理的相同告警事件进行聚合。

2. 最近生成时间：聚合的告警事件最近触发告警的时间。可单击右侧排序按钮对列表事件按时间正序和时间反序进行排列。

3. 事件数量：聚合时间范围内该 Shell 反向连接事件触发告警的总数量。

4. 状态：包括已处理、已忽略、未处理、已加白，支持按状态对列表事件进行快速筛选。

配置白名单

最近更新时间: 2024-08-23 15:08:00

本文档为您介绍如何配置白名单管理。

筛选刷新白名单

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**运行时安全** > **反弹 Shell** > **白名单管理**，进入白名单管理页面。

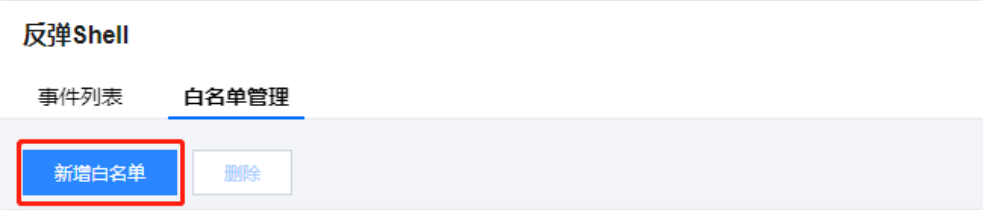
2. 在白名单管理页面，单击搜索框，可通过"连接进程"关键词对白名单事件进行查询。

3. 在白名单管理页面，单击操作栏右侧刷新图标，即可刷新白名单管理列表。

新增白名单

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**运行时安全** > **反弹 Shell** > **白名单管理**，进入白名单管理页面。

2. 在白名单管理页面，单击**新增白名单**，右侧弹出新增白名单设置页面。



3. 在新增白名单设置页面，需配置白名单生效的目标地址、连接进程和选择白名单生效范围。

- 单击目标地址左侧勾选图标，输入目标地址的 IP 和端口。

> **说明：**
>
> - IP 不能为空
> - IP 地址格式：单个 IP (127.0.0.1)；IP 范围 (127.0.0.1-127.0.0.254)；IP网段 (127.0.0.1/24)
> - 端口格式：80,8080 (支持多个，用英文逗号分隔。不限端口请留空）

- 单击连接进程左侧勾选图标，输入支持命令行通配符。

- 白名单生效范围为全部镜像或自选镜像。其中单击所需的自选镜像勾选或删除图标，即可选中或删除自选镜像。

> **说明：**
>
> 支持按住 shift 键进行多选。

4. 选择所需内容后，单击**确定**或**取消**，即可完成或取消新增白名单。

5. 配置完成后，满足条件的目标地址和连接进程将直接放行不再告警。

编辑白名单

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**运行时安全** > **反弹 Shell** > **白名单管理**，进入白名单管理页面。

2. 在白名单管理页面，单击右侧**编辑**，右侧弹出编辑白名单设置页面。

3. 在编辑白名单设置页面，可修改白名单生效的目标地址、连接进程和白名单生效范围。

4. 选择所需内容后，单击**确定**或**取消**，即可完成或取消修改白名单。

删除白名单

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**运行时安全** > **反弹 Shell** > **白名单管理**，进入白名单管理页面。

2. 在白名单管理页面，单击右侧**删除**，弹出"确认删除"弹窗。

3. 在"确认删除"弹窗中，单击**删除**或**取消**，即可删除或取消删除白名单。

> **说明：**
>
> 删除后，白名单将无法恢复，该白名单的关联镜像触发系统策略时将再次产生告警。

自定义列表管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**运行时安全** > **反弹 Shell** > **白名单管理**，进入白名单管理页面。

2. 在白名单管理页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 镜像数：白名单生效的镜像。

2. 连接进程：白名单生效的连接进程。

3. 目标主机：白名单生效的主机 IP 及端口。

文件查杀

最近更新时间: 2024-08-23 15:08:00

文件查杀提供实时检测和定期扫描容器内木马病毒文件功能。

查看风险趋势

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**运行时安全** > **文件查杀**。

2. 在文件查杀页面，可以查看待处理风险、影响容器的数量和趋势。

- 待处理风险：展示近7天待处理风险趋势图和较昨日新增风险数据。将鼠标悬停在趋势图上，展示某一天的待处理风险数据。
- 影响容器：展示近7天影响容器趋势图和较昨天新增影响容器数据。将鼠标悬停在趋势图上，展示某一天的影响容器数据。

设置风险检测

在 [文件查杀页面] 的风险检测模块，支持对定时检测和实时监控功能进行设置。

> **说明：**
> - 实时监控是客户配置的路径的增量文件实时检测。
> - 定时检测是客户配置的路径全部文件检测。

设置定时检测

1. 在风险检测模块，单击定时检测右侧的编辑图标，进入定时检测设置页面。

2. 在定时检测设置页面，单击开启开关，开启定时检测，并依次设置检测时间、检测路径、检测范围。

参数说明：

- 实时检测开关：支持通过单击“开关”，可开启或关闭实时检测功能。
- 检测时间
  - 检测周期：包括每天、每隔三天、每隔七天。
  - 开始检测时间：配置定时任务何时开始扫描。
  - 超时时长：当检测时长达到超时设置时间时，检测任务将终止。默认时间为5小时。
- 检测路径

- 全部路径：检测容器内全部文件路径。
- 自选路径：按自选的配置路径检测容器内文件。

- 检测范围
  - 主机节点：选择主机节点时，可选择扫描全部节点或自选节点。自选节点时，支持按节点名称和 IP 筛选需定时扫描的节点。
  - 容器：选择容器时，可选择全部容器或自选容器。自选容器时，支持按容器名称和容器 ID 筛选需定时扫描的容器。

3. 单击**保存设置**，即可完成定时检测设置。

设置实时监控

1. 在风险检测模块，单击实时监控右侧的编辑图标，进入实时监控设置页面。

2. 在实时监控设置页面，单击开启，开启实时监控，配置相关参数，

参数说明：

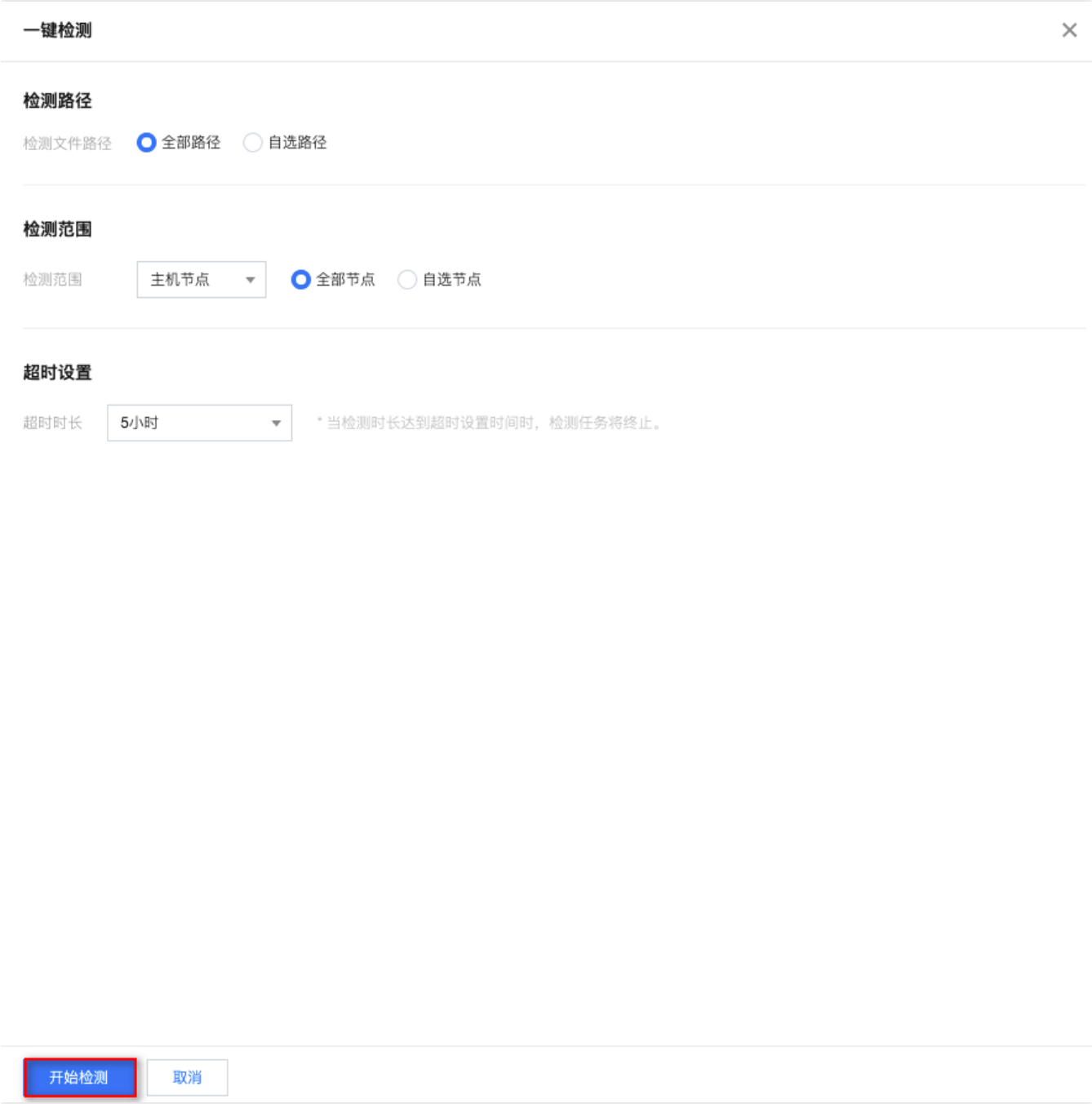
- 实时监控开关：支持通过单击开启或关闭实时监控功能。
- 检测路径
  - 全部路径：检测容器内全部文件路径。
  - 自选路径：按自选的配置路径检测容器内文件。
- 选择路径：根据实际需求选择**检测以下文件路径**或**检测除以下文件路径外的其他路径**。单击 可添加多个路径，最多为30个。

3. 单击**保存设置**，即可完成实时监控设置。

设置一键检测

1. 在风险检测模块，单击**一键检测**，进入一键检测页面。

2. 在一键检测页面，选择检测路径、检测范围，并设置超时时间。



参数说明：

- 检测路径：
  - 全部路径：检测容器内全部文件路径。
  - 自选路径：按自选的配置路径检测容器内文件。
- 检测范围：
  - 主机节点：选择主机节点时，可选择扫描全部节点或自选节点。自选节点时，支持按节点名称和 IP 筛选需定时扫描的节点。
  - 容器：选择容器时，可选择全部容器或自选容器。自选容器时，支持按容器名称和容器 ID 筛选需定时扫描的容器。

- 超时设置：当检测时长达到超时设置时间时，检测任务将终止。默认时间为5小时。

3. 单击**开始检测**，即按配置条件开始扫描容器内文件。

查看最近一次检测结果

在风险检测模块，单击**最近一次检测结果**，可查看近一次扫描任务详情。

检测详情展示内容：

- **检测详情概览**
  - 近一次扫描任务是否发现风险文件，如有发现，将展示风险文件数量、风险容器数量和扫描容器数量。
  - 近一次扫描任务开始检测和结束检测时间。
- **检测详情列表**：展示近一次扫描任务扫描出的风险文件概况，按容器资产进行聚合。
  - 列表字段包括：容器名称/ID、镜像名称/ID、主机节点名称/IP、检测状态、检测用时、风险数和操作项。
  - 支持对扫描任务进行重新检测，或停止正在检测中的任务。
  - 支持按主机名称、主机 IP、容器名称、容器 ID、镜像名称、镜像 ID 进行检索。
  - 单击左侧展开图标可查看风险文件的文件名称、文件路径、病毒名称和查看详情按钮；单击**查看详情**，可查看恶意文件详情。

查看事件列表

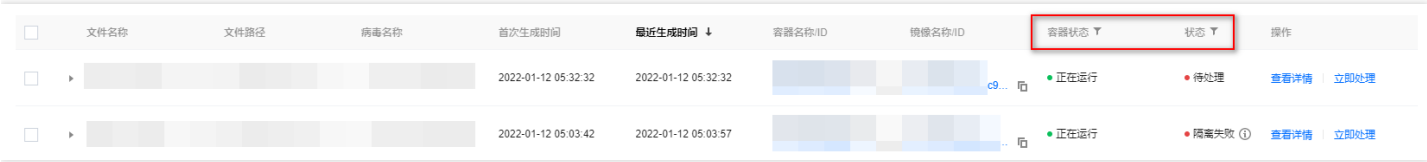
在 [文件查杀页面]的事件列表模块中，展示模块中提供容器木马病毒检测结果。

筛选事件

在事件列表模块中，支持通过如下两种方法对事件进行筛选。

- 单击搜索框通过"文件名称、文件路径、病毒名称、容器名称"等关键词查询木马病毒事件。

- 单击容器状态或状态右侧的筛选图标，可以通过容器状态和事件状态对木马病毒事件进行查询。

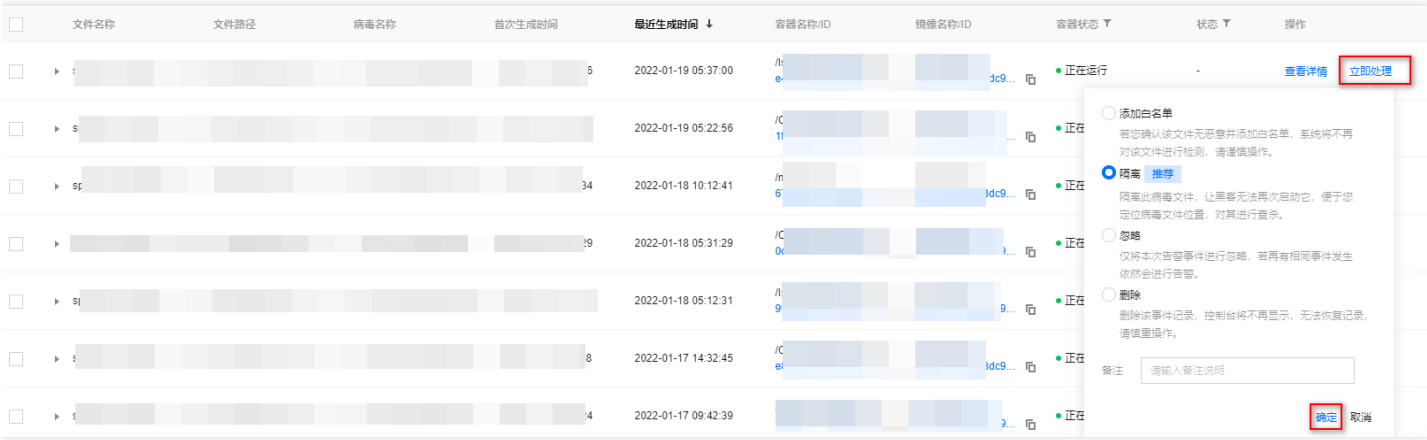


查看详情

在事件列表模块中，单击**查看详情**，右侧抽屉展示事件详情信息，包括病毒文件基本信息、事件详情、事件描述和进程信息。仅实时监控上报的事件详情中展示进程信息。

处理事件

在事件列表模块中，单击**立即处理**，可以选择对事件进行添加白名单、隔离（推荐）、忽略、删除，单击**确定**，即可对事件进行上述处理。



参数说明：

- 添加白名单：若您确认该文件无恶意并添加白名单，**系统将不再对该文件进行检测，请谨慎操作。**
- 隔离（推荐）：隔离此病毒文件，让黑客无法再次启动它，便于您定位病毒文件位置，对其进行查杀。
- 忽略：仅将本次告警事件进行忽略，若再有相同事件发生依然会进行告警。
- 删除：删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

自动隔离文件

容器安全服务新增木马自动隔离功能，支持自动隔离检测出的系统黑名单文件，以及用户自定义的恶意文件。

系统自动隔离文件

容器安全将自动隔离检测出的系统黑名单文件，部分恶意文件仍需用户手动确认隔离，建议您检查文件查杀列表中所有安全事件，确保已全部处理。若出现误隔离，请在已隔离列表中对文件进行恢复。

1. 登录 [容器安全服务控制台] ，在左侧导航中，单击**运行时安全** > **文件查杀**。

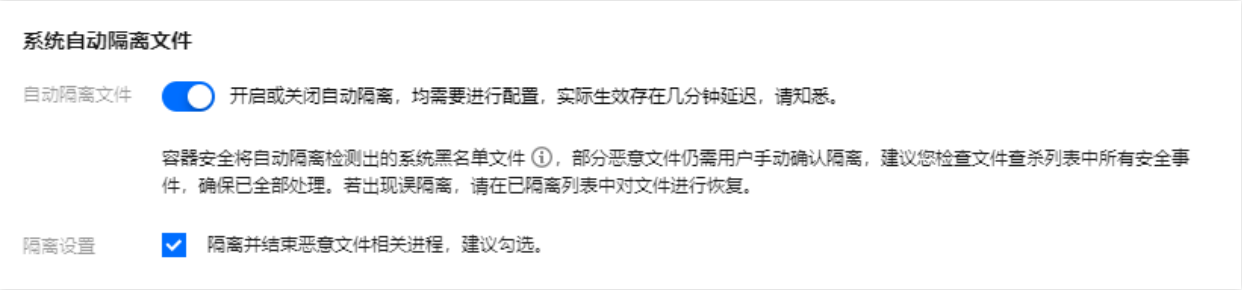
2. 在文件查杀页面，单击右上角的**查杀设置**。

3. 在查杀设置窗口中，单击**自动隔离文件**。

4. 在系统自动隔离文件模块，可单击开启或关闭自动隔离，同时，支持隔离并结束恶意文件相关进程。

> **说明：**

- 系统黑名单文件：腾讯云容器安全运营专家与算法专家经过沉淀的文件名单，此名单中的文件可进行自动隔离。
- 自动隔离开关默认关闭，客户可根据需求进行开启。启动自动隔离时，客户可自定义勾选是否隔离并结束恶意文件相关进程。
- 自动隔离开启时，系统黑名单和用户自定义黑名单均生效，支持对黑名单中的文件进行自动隔离。 自动隔离关闭时，系统黑名单和用户自定义黑名单均不对告警关联的恶意文件进行自动隔离。



用户自定义隔离文件

支持查看用户自定义隔离文件列表，自定义开启或关闭该文件的自动隔离开关。

1. 登录 [容器安全服务控制台] ，在左侧导航中，单击**运行时安全** > **文件查杀**。

2. 在文件查杀页面，单击右上角的**查杀设置**。

3. 在查杀设置窗口中，单击**自动隔离文件**。

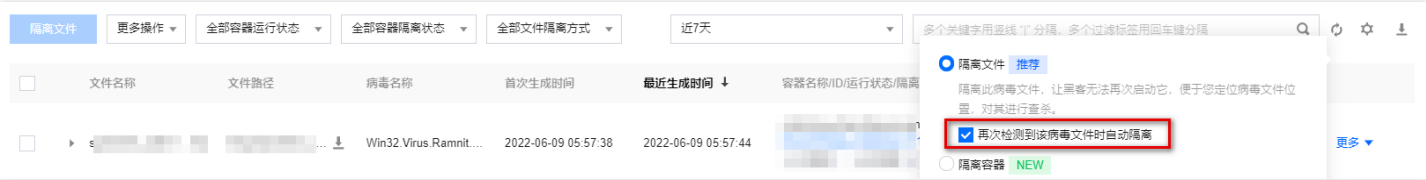
4. 在用户自定义隔离文件模块，支持控制自动隔离开关、查看详情和下载文件。

操作说明：

- 单击**自动隔离开关**，可开启或关闭自动隔离。
- 单击**详情**查看恶意文件的基本信息、危害描述和修复建议。
- 单击**下载**，可下载该恶意文件。

隔离文件列表

- 在 [文件查杀页面]的事件列表中，手动隔离恶意文件时，如勾选“再次检测到该病毒文件时自动隔离”，该恶意文件的 MD5值将记录在用户自定义隔离文件列表，自动隔离开关状态为开启。系统将对后续检出的同样文件进行自动隔离。当事件列表中手动隔离的恶意文件取消隔离后，用户自定义隔离文件列表中将删除该条记录，自动隔离配置也不再生效。



- [文件查杀页面]的事件列表中，手动隔离恶意文件时，不勾选“再次检测到该病毒文件时自动隔离”，该恶意文件的MD5值将记录在用户自定义隔离文件列表，自动隔离开关状态为关闭。

> **说明：**
>
> 用户自定义隔离文件自动隔离生效，需开启系统自动隔离开关；否则，即使处理安全事件时勾选“再次检测到该病毒文件时自动隔离”，系统也不会对自定义黑名单进行隔离。

恶意外连

最近更新时间: 2024-08-23 15:08:00

当容器向恶意域名或 IP 发起外连请求时，容器安全服务将检测此类行为，为您提供实时告警。当发现容器存在访问恶意域名/IP 的行为时，您的容器可能已经失陷，因为恶意域名/IP 可能是黑客的远控服务器、恶意软件下载源、矿池地址等。您需要及时进行如下排查：

1. 检查容器内的恶意进程及非法端口，删除可疑的启动项和定时任务。

2. 对容器存在的风险进行排查，如进行漏洞扫描、木马扫描等。

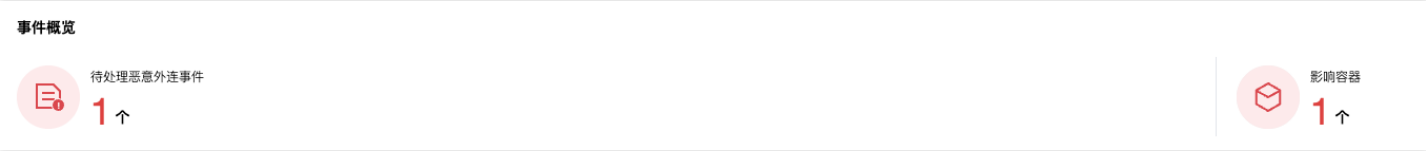
3. 对容器所使用的镜像进行加固，并替换运行中的容器。

事件列表

事件概览

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**运行时安全** > **恶意外连**，默认进入事件列表页面。

2. 在事件列表页面的事件概览中，将根据系统上报的安全事件，实时统计待处理的恶意外连事件及其影响的容器数量。



事件列表

在事件列表中，默认展示近7天的恶意外连事件，如需查看更多事件，可调整查询时长。列表展示字段如下表所示。

字段名称	字段详情
事件类型	恶意域名请求。
请求域名	触发安全事件的域名详情。
容器名称/ID/运行状态/隔离状态	展示容器资产相关的名称、ID、运行状态等信息；如客户认为该条安全事件属实，即容器可能已经失陷，可点击隔离容器避免风险在内网扩散。
镜像名称/ID	触发安全事件的容器的来源镜像，可通过单击**镜像 ID** 查看镜像详情，例如镜像安全风险、组件信息、构建历史等。
主机名称/IP	触发安全事件的容器所在的云服务器节点。展示该节点的名称和内外网 IP 信息。
首次生成时间	该条安全事件首次发生的时间。
最近生成时间	该条安全事件最近发生的时间。

字段名称	字段详情
请求次数	系统按容器 ID、域名、进程路径、进程启动用户等对待处理安全事件进行聚合展示，聚合周期为当天。
状态	包括待处理、已处理、已忽略、已加白。
操作	- 单击**详情**查看事件详情。详情包括事件详情，关联容器、镜像、主机等资产信息，风险描述，解决方案，请求域名详情和三层进程信息。 - 单击**处理**对安全事件进行处理。包括添加白名单、标记已处理、隔离容器、忽略和删除记录。

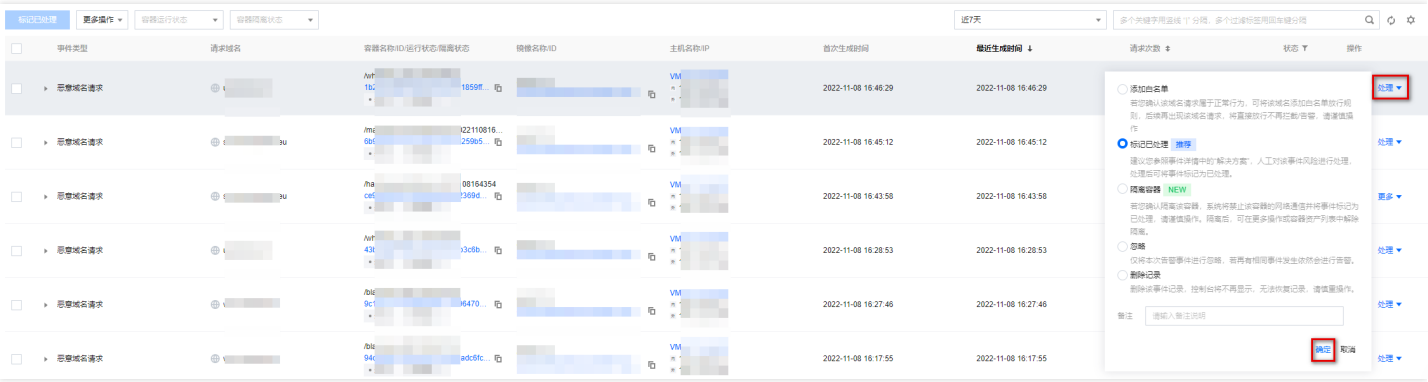
查看详情

在事件列表中，单击**详情**，进入事件详情，展示事件详情，关联容器、镜像、主机等资产信息，风险描述，解决方案，请求域名详情和三层进程信息。

事件详情
待处理
标记已处理
隔离容器
更多操作
事件详情
事件类型
恶意域名请求
事件数量
1 个
首次生成时间 2022-11-02 15:20:15
最近生成时间 2022-11-02 15:20:15
容器名称/ID
未隔离
镜像名称/ID
主机节点名称/IP
POD名称
风险描述
事件描述
发现容器存在访问恶意IP/域名的行为，您的容器可能已经失陷。
恶意IP/域名可能是黑客的远控服务器、恶意软件下载源、矿池地址等。
解决方案
建议方案
1.检查容器内的恶意进程及非法端口，删除可疑的启动项和定时任务；
2.对容器存在的风险进行排查，如进行漏洞扫描、木马扫描等；
3.对容器所使用的的镜像进行加固，并替换运行中的容器。
事件详情
恶意请求域名
命中规则
用户自定义
标签特征
-
进程信息
进程权限
-rwxrwxrwx
进程MD5
进程用户
root:root
进程路径
/normal_test
进程树
进程命令行参数
-
父进程信息

处理事件

1. 在事件列表中，单击**处理**，可以选择对事件进行添加白名单、标记已处理、隔离容器、忽略和删除记录，单击**确定**。



2. 在二次确认窗口中，进行如下操作：

- 添加白名单：输入白名单域名和备注，单击**确认**。添加白名单时，系统会根据加白的来源事件自动填入请求的域名，如有需要可手动调整为母域名。同时可勾选“批量处理相同事件（将相同域名触发的待处理事件批量加白）”，勾选并确认后，系统将批量对相同域名产生的安全事件批量加白处理。

> **注意：**
>
> 若您确认该域名请求属于正常行为，可将该域名添加白名单放行规则，后续再出现该域名请求，**将直接放行不再拦截/告警，请谨慎操作。**

- 标记已处理：建议您参照事件详情中的“解决方案”，人工对该事件风险进行处理，单击**确定**，处理后可将事件标记为已处理。
- 隔离容器：若您确认隔离该容器，系统将禁止该容器的网络通信并将事件标记为已处理，请谨慎操作。单击**确定**隔离后，可在更多操作或容器资产列表中解除隔离。
- 忽略：单击**确定**，仅将本次告警事件进行忽略，若再有相同事件发生依然会进行告警。
- 删除：单击**删除**，删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

黑白名单管理

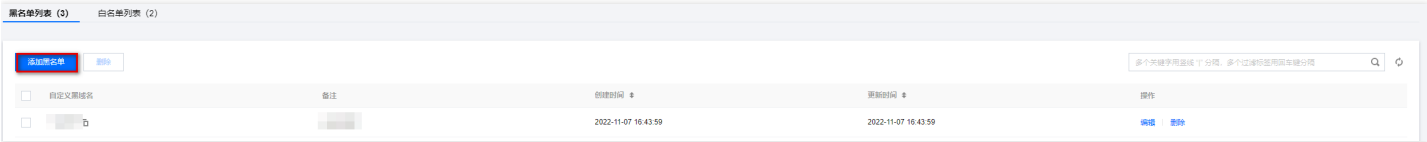
除容器安全服务产品提供的系统黑名单，客户也可自定义域名黑名单和域名白名单。黑白名单生效优先级为：**白名单 > 黑名单。**

- 黑名单：当容器向名单中的域名发起外连请求时，系统将判定为恶意外联行为，为您产生实时告警，可前往 [事件列表]查看。
- 白名单：当容器向白名单中的域名发起外连请求时，系统将直接放行，不再进行告警。

黑名单管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**运行时安全** > **黑白名单管理**，默认进入黑名单列表页签。

2. 在黑名单列表页签，单击**添加黑名单**。



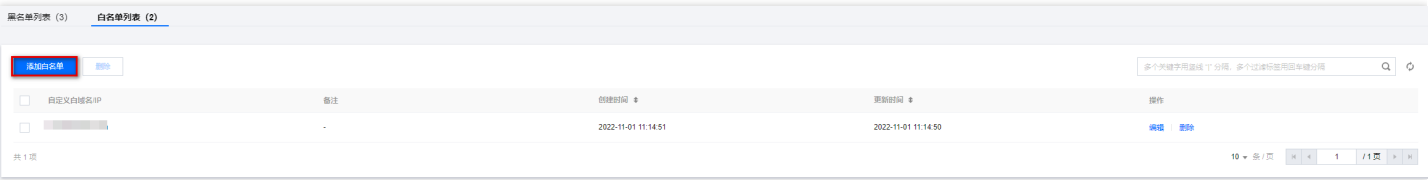
3. 在添加黑名单窗口中，可支持批量新增多个自定义黑域名；输入域名时，支持前缀置空的泛域名，例如 `*.tencent.com`；泛域名下的子域名均会告警。

4. 单击**确认**，列表将根据实际输入的域名生成记录；当输入多个域名时，将生成多条记录。

白名单管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**运行时安全** > **黑白名单管理** > **白名单列表**。

2. 在白名单列表页签，单击**添加白名单**。



3. 在添加白名单窗口中，可支持批量新增多个自定义白域名；输入域名时，支持前缀置空的泛域名，例如 `*.tencent.com`；泛域名下的子域名均会被放行，不产生告警。

4. 单击**确认**，列表将根据实际输入的域名生成记录；当输入多个域名时，将生成多条记录。

高级防御
概述

最近更新时间: 2024-08-23 15:08:00

高级防御支持自适应识别黑客攻击，实时监控和防护容器运行时安全，提供异常进程、文件篡改和高危系统调用安全功能。

- 异常进程：通过系统规则和用户自定义检测规则，实时监控进程异常启动行为，并告警通知或拦截。系统监控策略包括代理软件、横向渗透、恶意命令、反弹 Shell、无文件程序执行、高危命令、敏感服务异常子进程启动等。
- 文件篡改：通过系统规则和用户自定义检测规则，实时监控核心文件被修改的文件异常访问行为，并告警通知或拦截。系统监控策略包括篡改计划任务、篡改系统程序、篡改用户配置等。
- 高危系统调用：基于腾讯云安全自适应学习技术，实时审计容器内发起的可能引起安全风险的 Linux 系统调用行为。

异常进程
事件列表

最近更新时间: 2024-08-23 15:08:00

异常进程是基于自适应学习技术，通过系统规则和用户自定义检测规则，实时监控进程异常启动行为，并实时告警通知或拦截。异常进程包含事件列表和规则配置两大模块。本文档介绍高级防御的事件列表功能。

筛选刷新事件列表

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **异常进程** > **事件列表**，进入事件列表页面。

2. 在事件列表页面，单击搜索框，可通过"连接进程"关键词对白名单事件进行查询。

3. 在事件列表页面，单击操作栏右侧刷新图标，即可刷新事件列表。

导出事件列表

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **异常进程** > **事件列表**，进入事件列表页面。

2. 在事件列表页面，单击勾选所需的异常进程事件后，单击导出图标即可导出异常进程事件。

> **说明：**
>
> 单击操作栏处 图标，可进行批量勾选。

事件状态处理

登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **异常进程** > **事件列表**，进入事件列表页面。

方式1

在事件列表页面，可对异常进程事件进行标记已处理、忽略和删除处理。

- 标记已处理：单击勾选所需的异常进程事件后，单击**标记已处理**>**确定**，即可将选中事件标记已处理。

> **说明：**
>
> 建议您参照事件详情中的“解决方案”，人工对该事件风险进行处理，可将事件标记为已处理。

- 忽略：单击勾选所需的异常进程事件后，单击**忽略**>**确定**，即可将选中事件忽略。

> **说明：**
>
> 仅将已选事件进行忽略，若再有相同事件发生依然会进行告警。

- 删除：单击勾选所需的异常进程事件后，单击**删除**>**确定**，即可将选中事件删除。

> **注意：**
>
> 删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

方式2

1. 在事件列表页面，事件状态为待处理时，单击**立即处理**，可选择将事件状态设置为添加白名单、标记已处理和忽略等。

2. 单击**确定**或**取消**，即可完成或取消事件状态更改。

3. 在事件列表页面，事件状态为已忽略时，可单击**取消忽略**或**删除**，可将事件取消忽略或删除。

> **说明：**
>
> - 取消忽略后，该事件状态将变更为待处理，需单击**确定**进行二次确认。
> - 删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

4. 在事件列表页面，事件状态为已处理时，可单击**删除**，删除该事件。

> **说明：**
>
> 删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

查看事件详情

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **异常进程** > **事件列表**，进入事件列表页面。

2. 在事件列表页面，单击进程路径左侧展开图标，可查看事件描述。

3. 在事件列表页面，单击**查看详情**，右侧弹出事件详情页面。

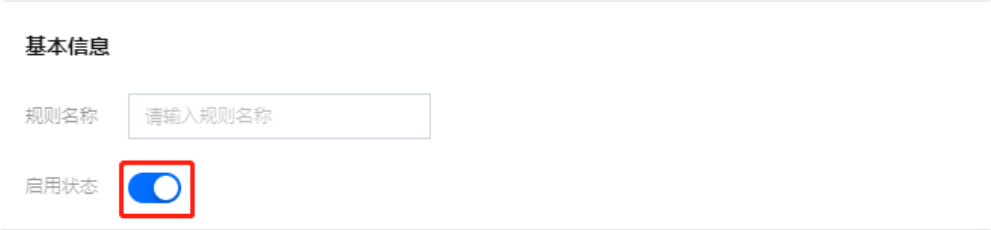
4. 在事件详情页面，展示了事件详情、进程信息、父进程信息和事件描述。并可对该事件进行标记已处理、忽略和加白等操作。

> **说明：**
>
> 标记已处理、忽略和删除：相应操作处理请参考事件状态处理。

5. 在事件详情页面，单击**加白**进入复制规则页面，需配置基本信息、配置规则和镜像生效范围。

- 基本信息：输入事件的规则名称，单击开启或关闭规则检查。

> **说明：**
>
> 关闭后，将不再进行该规则检测！



- 配置规则：需输入进程路径和执行动作。单击**添加**或**删除**，可进行添加或删除规则。
- 镜像范围：全部镜像和自选镜像。其中单击所需的自选镜像勾选或删除图标，即可选中或删除自选镜像。

> **说明：**
>
> 支持按住 shift 键进行多选。

6. 选择所需内容后，单击**设置**或**取消**，即可完成或取消设置。

自定义列表管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **异常进程** > **事件列表**，进入事件列表页面。

2. 在事件列表页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 首次生成时间：该异常进程事件首次触发告警的时间。系统默认对未处理的相同告警事件进行聚合。

2. 最近生成时间：聚合的告警事件最近触发告警的时间。可单击右侧排序按钮对列表事件按时间正序和时间反序进行排列。

3. 事件数量：聚合时间范围内该异常进程事件触发告警的总数量。

4. 动作执行结果：包括拦截成功、拦截失败、放行、告警，支持按动作执行结果对列表事件进行快速筛选。

5. 状态：包括已处理、已忽略、未处理、已加白，支持按状态对列表事件进行快速筛选。

规则配置

最近更新时间: 2024-08-23 15:08:00

异常进程是基于自适应学习技术，通过系统规则和用户自定义检测规则，实时监控进程异常启动行为，并实时告警通知或拦截。异常进程包含事件列表和规则配置两大模块。本文档介绍高级防御的规则配置功能。

筛选刷新规则

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **异常进程** > **规则配置**，进入规则配置页面。

2. 在规则配置页面，单击搜索框，可通过"规则名称"关键词对配置规则进行查询。

3. 在规则配置页面，单击操作栏右侧 图标，即可刷新规则列表。

新增规则

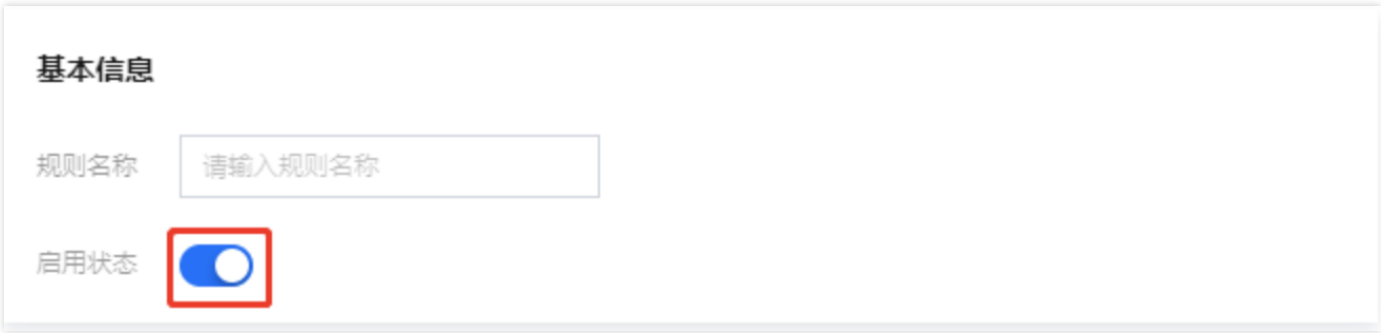
1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **异常进程** > **规则配置**，进入规则配置页面。

2. 在规则配置页面，单击**创建规则**，右侧抽屉弹出新增规则页面。

3. 在新增规则页面，需配置基本信息、配置规则和镜像生效范围。

- 基本信息：输入事件的规则名称，单击开启或关闭规则检查。

> **说明：**
>
> 关闭后，将不再进行该规则检测！



- 配置规则：需输入进程路径和执行动作。单击**添加**或**删除**，可进行添加或删除规则。

> **说明：**
>
> - 配置规则最多可添加30条。
> - 执行动作有：
> - 拦截：命中规则条件时，将自动拦截进程运行，记录事件详情。
> - 告警：命中规则条件时，仅自动告警事件，不拦截进程运行，记录事件详情。
> - 放行：命中规则条件时，将自动放行进程运行，不产生事件记录。

- 镜像范围：全部镜像和自选镜像。其中单击所需的自选镜像 或 图标，即可选中或删除自选镜像。

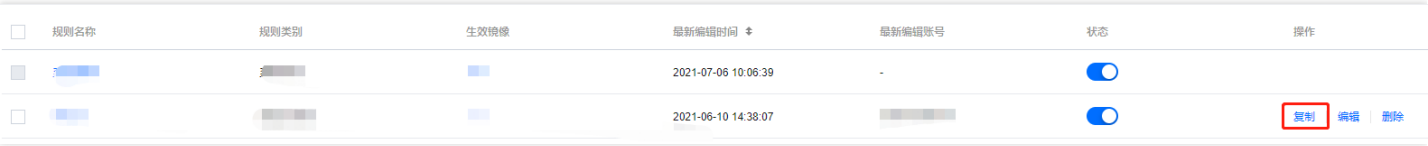
> **说明：**
>
> 支持按住 shift 键进行多选。

4. 选择所需内容后，单击**设置**或**取消**，即可完成或取消设置。

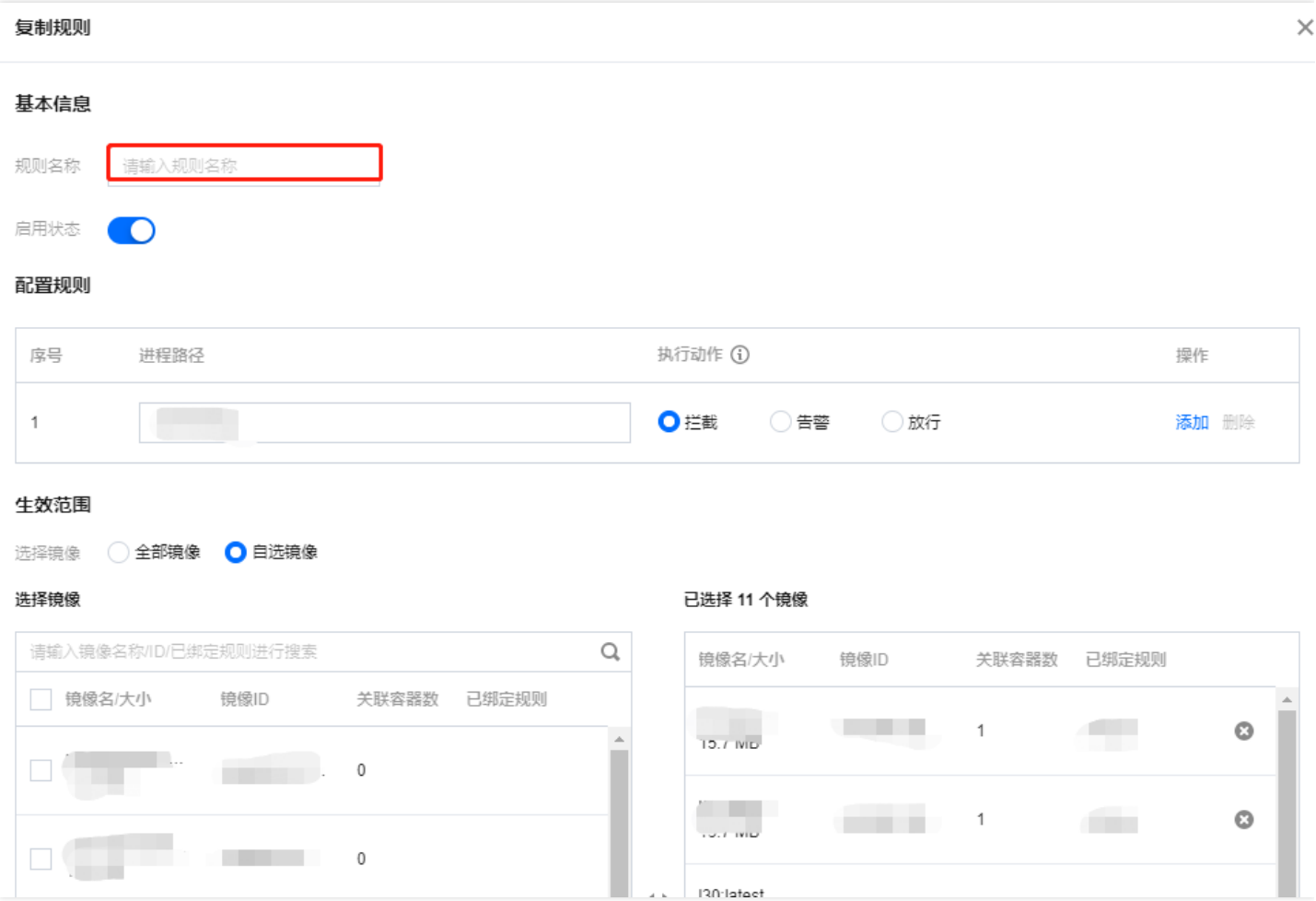
复制规则

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **异常进程** > **规则配置**，进入规则配置页面。

2. 在规则配置页面，单击右侧**复制**，右侧弹出复制规则页面。



3. 在复制规则页面，需输入规则名称，可修改启用状态、配置规则和镜像生效范围。

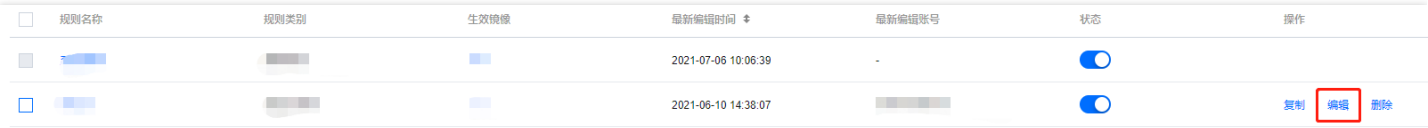


4. 选择所需内容后，单击**确定**或**取消**，即可完成或取消复制规则。

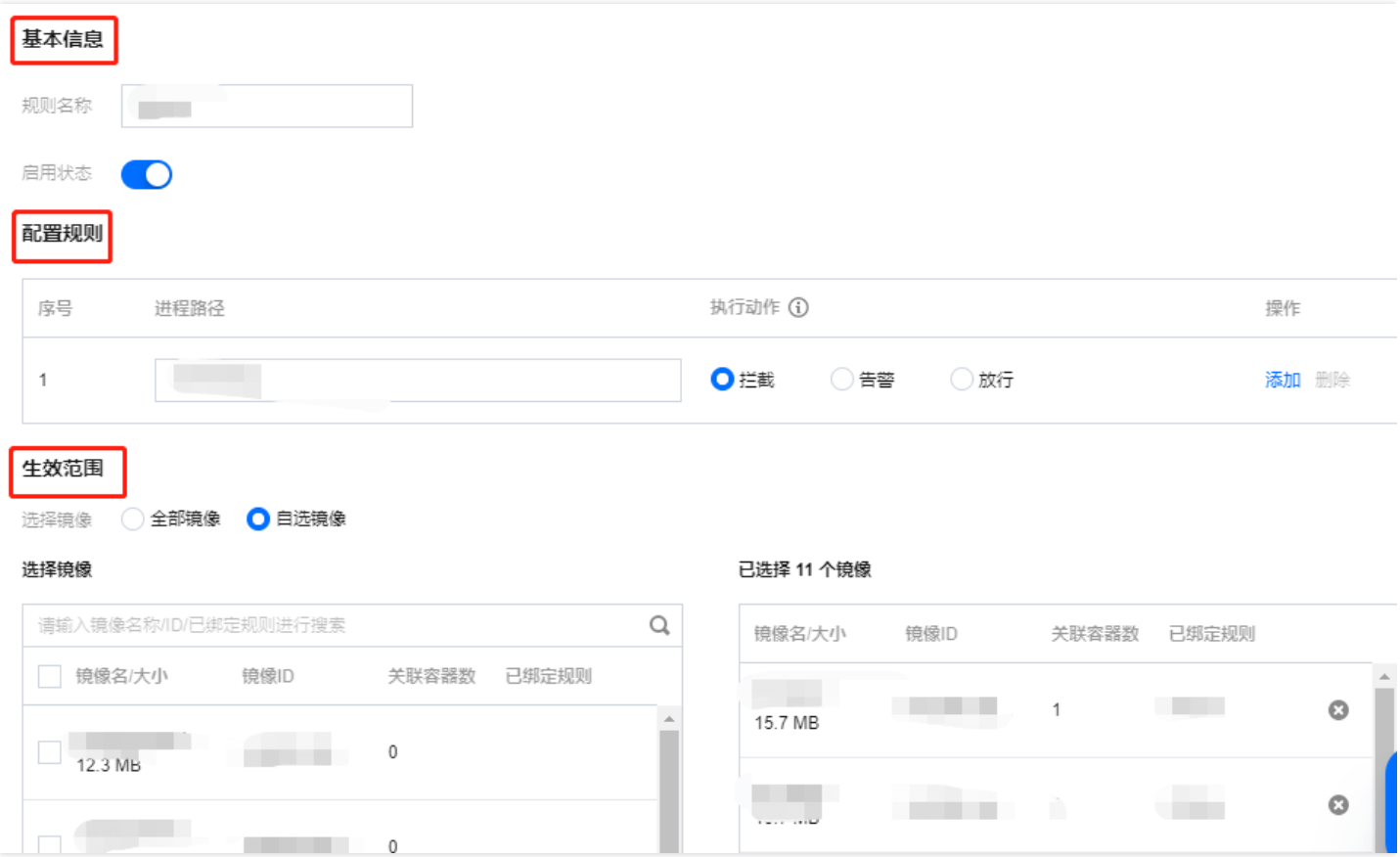
编辑规则

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **异常进程** > **规则配置**，进入规则配置页面。

2. 在规则配置页面，单击右侧**编辑**，右侧弹出编辑规则设置页面。



3. 在编辑规则设置页面，可修改规则的基本信息、配置规则和镜像生效范围。



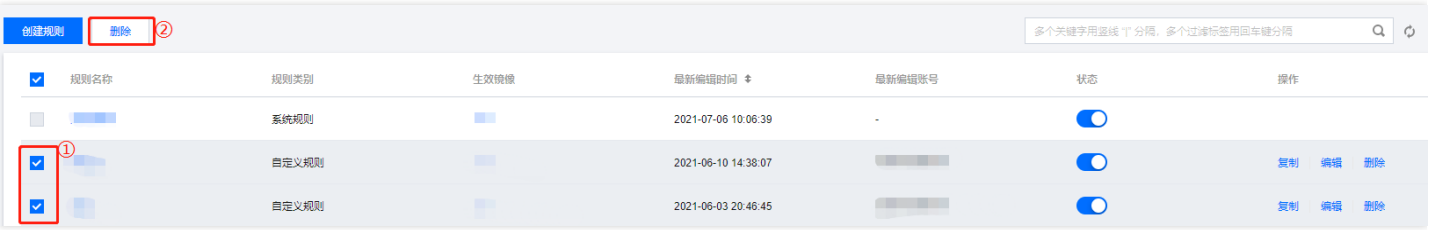
4. 选择所需内容后，单击**确定**或**取消**，即可完成或取消修改规则。

删除规则

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **异常进程** > **规则配置**，进入规则配置页面。

2. 在规则配置页面，可选择如下两种方式删除规则：

- 选择所需的规则单击勾选图标，后单击操作栏左侧**删除**，弹出“确认删除”弹窗。



- 选择所需规则的所作行，单击右侧**删除**，弹出“确认删除”弹窗。

3. 在“确认删除”弹窗中，单击**删除**或**取消**，即可删除或取消删除规则。

> **说明：**
>
> 删除后，规则将无法恢复，该规则的关联镜像将自动关联系统默认规则。

导出规则

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **异常进程** > **规则配置**，进入规则配置页面。

2. 在规则配置页面，单击勾选所需的异常进程规则后，单击导出图标即可导出异常进程规则。

> **说明：**
>
> 单击操作栏处 图标，可进行批量勾选。

自定义列表管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **异常进程** > **规则配置**，进入规则配置页面。

2. 在规则配置页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 规则类别：系统规则或自定义规则。

2. 生效镜像：规则生效的镜像数量。单击生效镜像“数字”，右侧抽屉展示规则详情。

3. 状态：启用/禁用。

4. 操作：系统策略操作栏仅复制规则，用户自定义规则支持复制、编辑和删除。

文件篡改
事件列表

最近更新时间: 2024-08-23 15:08:00

文件篡改功能提供文件篡改监测事件列表和规则配置列表。事件列表展示模块中提供文件篡改检测结果。

筛选刷新事件列表

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **文件篡改** > **事件列表**，进入事件列表页面。

2. 在事件列表页面，单击搜索框，可通过"文件名称、进程路径和命中规则"等关键词对文件篡改检测结果进行查询。

3. 在事件列表页面，单击操作栏右侧刷新图标，即可刷新事件列表。

导出检测结果

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **文件篡改** > **事件列表**，进入事件列表页面。

2. 在事件列表页面，单击勾选所需的文件篡改检测事件后，单击导出图标即可导出文件篡改检测事件。

> **说明：**
>
> 单击操作栏处 图标，可进行批量勾选。

更改事件状态

登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **文件篡改** > **事件列表**，进入事件列表页面。

方式1

在事件列表页面，可对文件篡改检测事件进行标记已处理、忽略和删除处理。

- 标记已处理：单击勾选所需的文件篡改检测事件后，单击**标记已处理**>**确定**，即可将选中事件标记已处理。

> **说明：**
>
> 建议您参照事件详情中的“解决方案”，人工对该事件风险进行处理，可将事件标记为已处理。

- 忽略：单击勾选所需的文件篡改检测事件后，单击**忽略**>**确定**，即可将选中事件忽略。

> **说明：**
>
> 仅将已选事件进行忽略，若再有相同事件发生依然会进行告警。

- 删除：单击勾选所需的文件篡改检测事件后，单击**删除**>**确定**，即可将选中事件删除。

> **注意：**
>
> 删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

方式2

1. 在事件列表页面，事件状态为待处理时，单击**立即处理**，可选择将事件状态设置为添加白名单、标记已处理和忽略等。

2. 单击**确定**或**取消**，即可完成或取消事件状态更改。

3. 在事件列表页面，事件状态为已忽略时，可单击**取消忽略**或**删除**，可将事件取消忽略或删除。

> **说明：**
>
> - 取消忽略后，该事件状态将变更为待处理，需单击**确定**进行二次确认。
> - 删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

4. 在事件列表页面，事件状态为已处理时，可单击**删除**，删除该事件。

> **说明：**
>
> 删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

查看事件详情

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **文件篡改** > **事件列表**，进入事件列表页面。

2. 在事件列表页面，单击进程路径左侧展开图标，可查看事件描述。

3. 在事件列表页面，单击**查看详情**，右侧弹出事件详情页面。

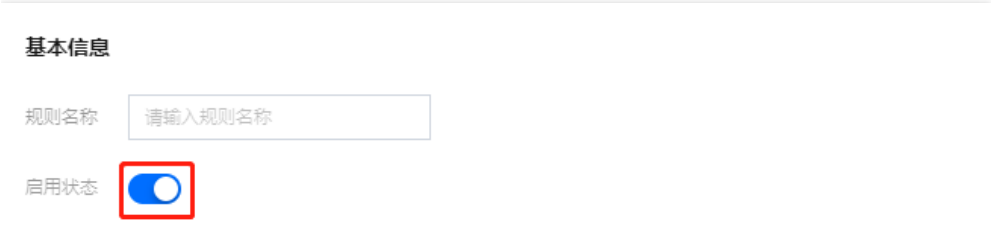
4. 在事件详情页面，展示了事件详情、进程信息、父进程信息和事件描述。并可对该事件进行标记已处理、忽略和加白等操作。

> **说明：**
>
> 标记已处理、忽略和删除：相应操作处理请参考更改事件状态。

5. 在事件详情页面，单击**加白**进入复制规则页面，需配置基本信息、配置规则和镜像生效范围。

- 基本信息：输入事件的规则名称，单击开启或关闭规则检查。

> **说明：**
>
> 关闭后，将不再进行该规则检测！



- 配置规则：输入需放行的进程路径和被访问文件路径，选择执行动作。单击**添加**或**删除**，可进行添加或删除规则。

> **说明：**
>
> - 配置规则最多可添加30条。
> - 执行动作有：
> - 拦截：命中规则条件时，将自动拦截进程运行，记录事件详情。
> - 告警：命中规则条件时，仅自动告警事件，不拦截进程运行，记录事件详情。
> - 放行：命中规则条件时，将自动放行进程运行，不产生事件记录。

- 镜像范围：全部镜像和自选镜像。其中单击所需的自选镜像 或 图标，即可选中或删除自选镜像。

> **说明：**
>
> 支持按住 shift 键进行多选。

6. 选择所需内容后，单击**设置**或**取消**，即可完成或取消设置。

自定义列表管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **文件篡改** > **事件列表**，进入事件列表页面。

2. 在事件列表页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 首次生成时间：该文件篡改事件首次触发告警的时间。系统默认对未处理的相同告警事件进行聚合。

2. 最近生成时间：聚合的告警事件最近触发告警的时间。可单击右侧排序按钮对列表事件按时间正序和时间反序进行排列。

3. 事件数量：聚合时间范围内该文件篡改事件触发告警的总数量。

4. 动作执行结果：包括拦截成功、拦截失败、放行、告警，支持按动作执行结果对列表事件进行快速筛选。

5. 状态：包括已处理、已忽略、未处理、已加白，支持按状态对列表事件进行快速筛选。

规则配置

最近更新时间: 2024-08-23 15:08:00

文件篡改功能提供文件篡改监测事件列表和规则配置列表。规则配置展示模块中提供配置规则列表。

筛选刷新规则

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **文件篡改** > **规则配置**，进入规则配置页面。

2. 在规则配置页面，单击搜索框，可通过"规则名称"关键词对配置规则进行查询。

3. 在规则配置页面，单击操作栏右侧刷新图标，即可刷新规则列表。

新增规则

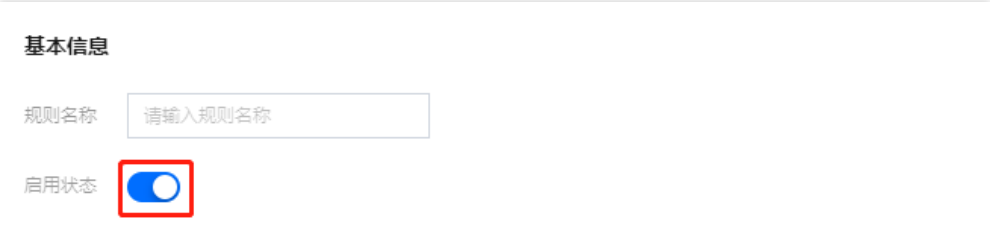
1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **文件篡改** > **规则配置**，进入规则配置页面。

2. 在规则配置页面，单击**创建规则**，右侧抽屉弹出新增规则页面。

3. 在新增规则页面，需配置基本信息、配置规则和镜像生效范围。

- 基本信息：输入事件的规则名称，单击开启或关闭规则检查。

> **说明：**
>
> 关闭后，将不再进行该规则检测！



- 配置规则：需输入进程路径和被访问文件路径，并选择执行动作，单击**添加**或**删除**，可进行添加或删除规则。

> **说明：**
>
> - 配置规则最多可添加30条。
> - 执行动作有：
> - 拦截：命中规则条件时，将自动拦截进程运行，记录事件详情。
> - 告警：命中规则条件时，仅自动告警事件，不拦截进程运行，记录事件详情。
> - 放行：命中规则条件时，将自动放行进程运行，不产生事件记录。

- 镜像范围：全部镜像和自选镜像。其中单击所需的自选镜像勾选或删除图标，即可选中或删除自选镜像。

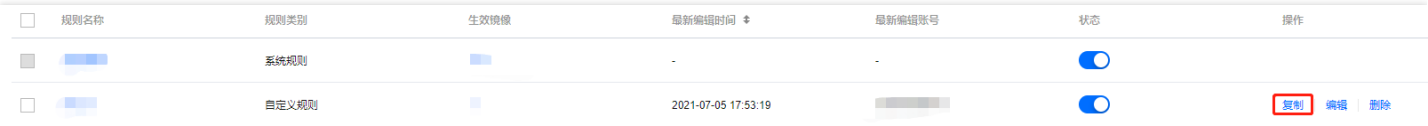
> **说明：**
>
> 支持按住 shift 键进行多选。

4. 选择所需内容后，单击**设置**或**取消**，即可完成或取消设置。

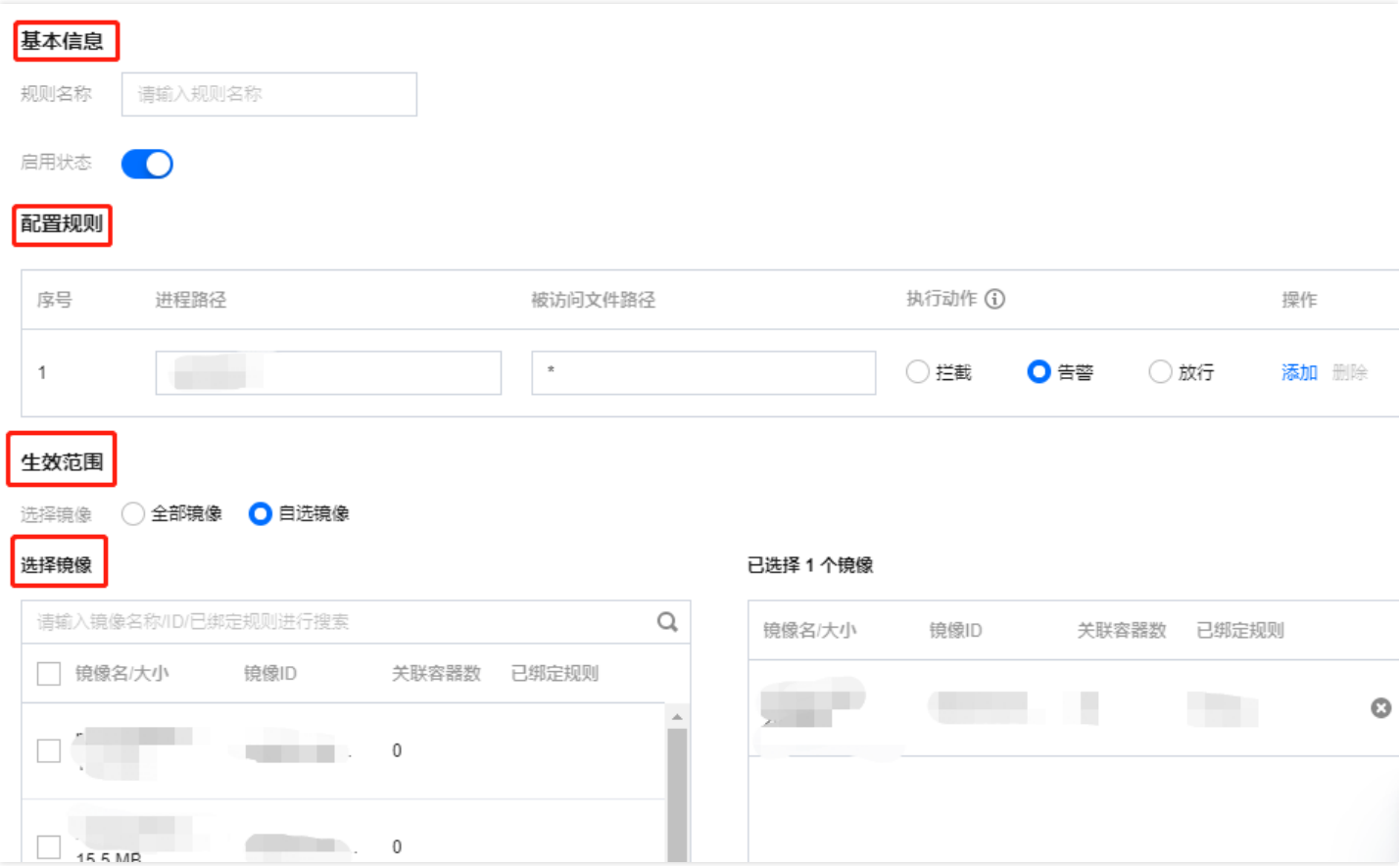
复制规则

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **文件篡改** > **规则配置**，进入规则配置页面。

2. 在规则配置页面，单击右侧**复制**，右侧弹出编复制规则页面。



3. 在复制规则页面，需输入规则名称，可修改启用状态、配置规则和镜像生效范围。

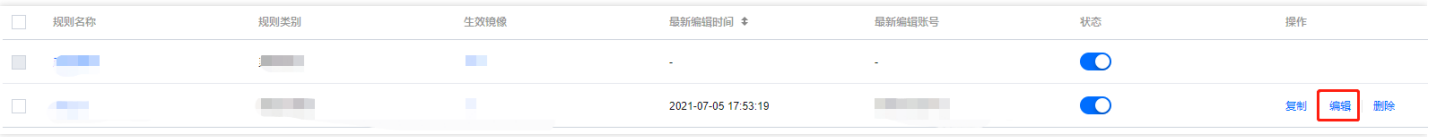


4. 选择所需内容后，单击**确定**或**取消**，即可完成或取消复制规则。

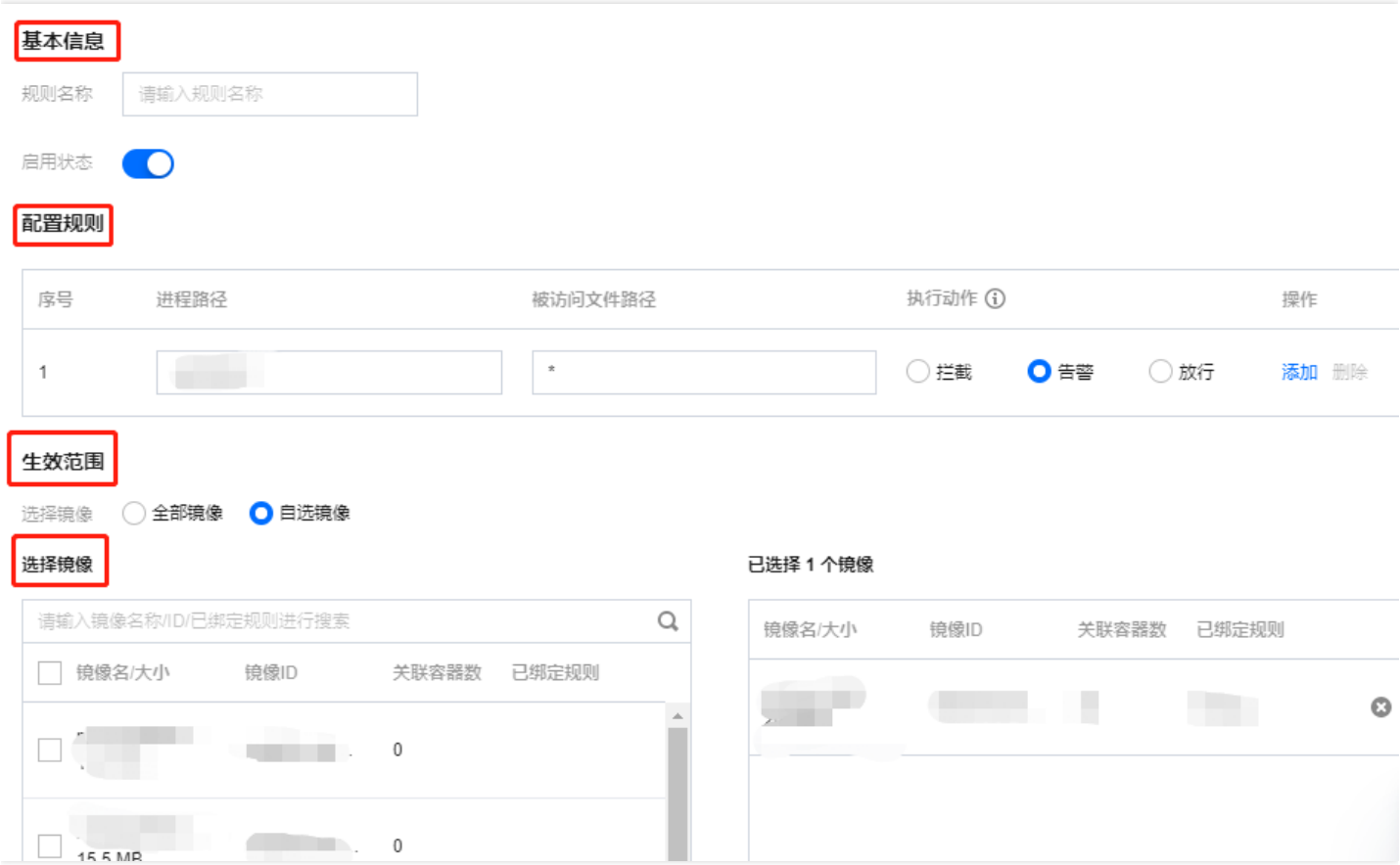
编辑规则

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **文件篡改** > **规则配置**，进入规则配置页面。

2. 在规则配置页面，单击右侧**编辑**，右侧弹出编辑规则设置页面。



3. 在编辑规则设置页面，可修改规则的基本信息、配置规则和镜像生效范围。



4. 选择所需内容后，单击**确定**或**取消**，即可完成或取消修改规则。

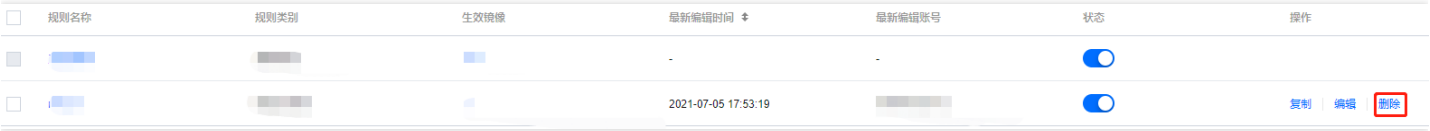
删除规则

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御**>**文件篡改**>**规则配置**，进入规则配置页面。

2. 在规则配置页面，可选择如下两种方式删除规则：

- 选择所需的规则单击勾选图标，后单击操作栏左侧**删除**，弹出“确认删除”弹窗。

- 在规则配置页面，选择所需规则的所作行，单击右侧**删除**，弹出“确认删除”弹窗。



3. 在“确认删除”弹窗中，单击**删除**或**取消**，即可删除或取消删除规则。

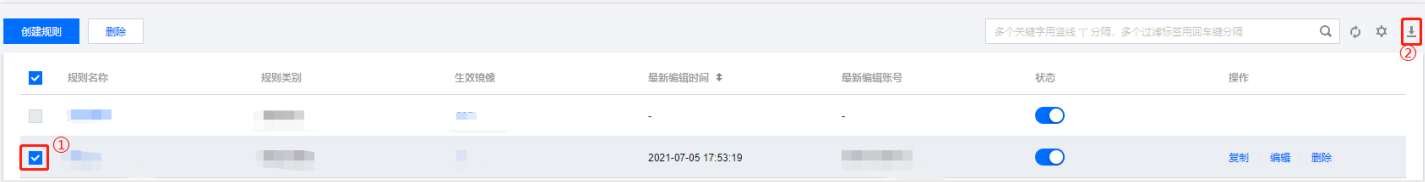
> **说明：**
>
> 删除后，规则将无法恢复，该规则的关联镜像将自动关联系统默认规则。

导出规则

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **文件篡改** > **规则配置**，进入规则配置页面。

2. 在规则配置页面，单击勾选所需的文件篡改规则后，单击导出图标即可导出文件篡改规则。

> **说明：**
>
> 单击操作栏处 图标，可进行批量勾选。



自定义列表管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **文件篡改** > **规则配置**，进入规则配置页面。

2. 在规则配置页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 规则类别：系统规则或自定义规则。

2. 生效镜像：规则生效的镜像数量。单击生效镜像“数字”，右侧抽屉展示规则详情。

3. 状态：启用/禁用

4. 操作：系统策略操作栏仅复制规则；用户自定义规则支持复制、编辑和删除。

高危系统调用
事件列表

最近更新时间: 2024-08-23 15:08:00

高危系统调用提供可能存在风险的系统调用行为检测事件列表和白名单管理列表。事件列表展示模块中提供高危系统调用检测结果。

筛选刷新事件列表

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **高危系统调用** > **事件列表**，进入事件列表页面。

2. 在事件列表页面，单击搜索框，可通过"进程路径、系统调用名称和容器名称"等关键词对高危系统调用检测事件进行查询。

3. 在事件列表页面，单击操作栏右侧刷新图标，即可刷新事件列表。

导出事件列表

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **高危系统调用** > **事件列表**，进入事件列表页面。

2. 在事件列表页面，单击勾选所需的文件篡改检测事件后，单击导出图标即可导出高危系统调用事件。

> **说明：**
>
> 单击操作栏处 图标，可进行批量勾选。

更改事件状态

登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **高危系统调用** > **事件列表**，进入事件列表页面。

方式1

在事件列表页面，可对高危系统调用事件进行标记已处理、忽略和删除处理。

- 标记已处理：单击勾选所需的高危系统调用事件后，单击**标记已处理**>**确定**，即可将选中事件标记已处理。

> **说明：**
>
> 建议您参照事件详情中的"解决方案"，人工对该事件风险进行处理，可将事件标记为已处理。

- 忽略：单击勾选所需的高危系统调用事件后，单击**忽略**>**确定**，即可将选中事件忽略。

> **说明：**
>
> 仅将已选事件进行忽略，若再有相同事件发生依然会进行告警。

- 删除：单击勾选所需的高危系统调用事件后，单击**删除**>**确定**，即可将选中事件删除。

> **注意：**
>
> 删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

方式2

1. 在事件列表页面，事件状态为待处理时，单击**立即处理**，可选择将事件状态设置为添加白名单、标记已处理和忽略等。

2. 单击**确定**或**取消**，即可完成或取消事件状态更改。

3. 在事件列表页面，事件状态为已忽略时，可单击**取消忽略**或**删除**，可将事件取消忽略或删除。

> **说明：**
>
> - 取消忽略后，该事件状态将变更为待处理，需单击**确定**进行二次确认。
> - 删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

4. 在事件列表页面，事件状态为已处理时，可单击**删除**，删除该事件。

> **说明：**
>
> 删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

查看事件详情

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **高危系统调用** > **事件列表**，进入事件列表页面。

2. 在事件列表页面，单击进程路径左侧展开图标，可查看事件描述。

3. 在事件列表页面，单击**查看详情**，右侧弹出事件详情页面。

4. 在事件详情页面，展示了事件详情、进程信息、父进程信息和事件描述。并可对该事件进行标记已处理、忽略和加白等操作。

> **说明：**
>
> 标记已处理、忽略和删除：相应操作处理请参考更改事件状态。

5. 在事件详情页面，单击**加白**进入新增白名单页面，需确认满足条件（进程路径、系统调用名称）和镜像生效范围。

- 满足条件：进程路径和系统调用名称，不可更改内容。

- 镜像生效范围：全部镜像和自选镜像。其中单击所需的自选镜像 或 图标，即可选中或删除自选镜像。

> **说明：**
>
> 支持按住 shift 键进行多选。

6. 选择所需内容后，单击**设置**或**取消**，即可完成或取消新增白名单。

自定义列表管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **高危系统调用** > **事件列表**，进入事件列表页面。

2. 在事件列表页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。

列表重点字段说明

1. 首次生成时间：该系统调用事件首次触发告警的时间。系统默认对未处理的相同告警事件进行聚合。

2. 最近生成时间：聚合的告警事件最近触发告警的时间。可单击右侧排序按钮对列表事件按时间正序和时间反序进行排列。

3. 事件数量：聚合时间范围内该系统调用事件触发告警的总数量。

4. 事件数量：聚合时间范围内该系统调用事件触发告警的总数量。

5. 状态：包括已处理、已忽略、未处理、已加白，支持按状态对列表事件进行快速筛选。

白名单管理

最近更新时间: 2024-08-23 15:08:00

白名单管理展示模块中提供配置白名单接口和白名单展示列表。

筛选刷新白名单

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **高危系统调用** > **白名单管理**，进入白名单管理页面。

2. 在白名单管理页面，单击搜索框，可通过"进程路径、系统调用名称"关键词对配置的白名单进行查询。

3. 在白名单管理页面，单击操作栏右侧刷新图标，即可刷新白名单管理列表。

新增白名单

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **高危系统调用** > **白名单管理**，进入白名单管理页面。

2. 在白名单管理页面，单击**新增白名单**，右侧弹出新增白名单设置页面。

3. 在新增白名单设置页面，需配置白名单生效的进程路径、系统调用名称和生效范围。

- 单击进程路径和系统调用名称左侧勾选图标，输入进程路径，并选择系统调用名称。

> **说明：**
>
> 进程路径不能为空。

- 白名单生效范围为全部镜像或自选镜像。其中单击所需的自选镜像勾选或删除图标，即可选中或删除自选镜像。

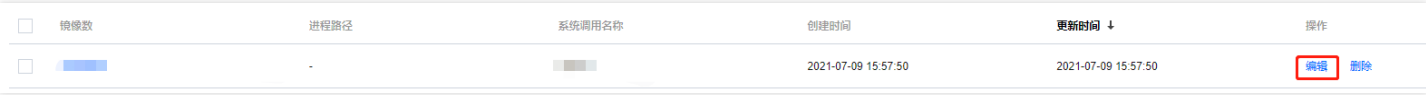
> **说明：**
>
> 支持按住 shift 键进行多选。

4. 选择所需内容后，单击**确定**或**取消**，即可完成或取消新增白名单。

编辑白名单

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **高危系统调用** > **白名单管理**，进入白名单管理页面。

2. 在白名单管理页面，单击右侧**编辑**，右侧弹出编辑白名单设置页面。



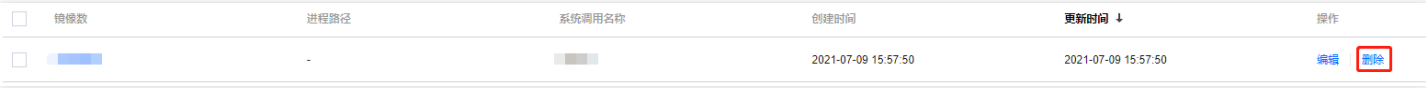
3. 在编辑白名单设置页面，可修改白名单生效的进程路径、系统调用名称和生效范围。

4. 选择所需内容后，单击**确定**或**取消**，即可完成或取消修改白名单。

删除白名单

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **高危系统调用** > **白名单管理**，进入白名单管理页面。

2. 在白名单管理页面，单击右侧**删除**，弹出“确认删除”弹窗。



3. 在“确认删除”弹窗中，单击**删除**或**取消**，即可删除或取消删除白名单。

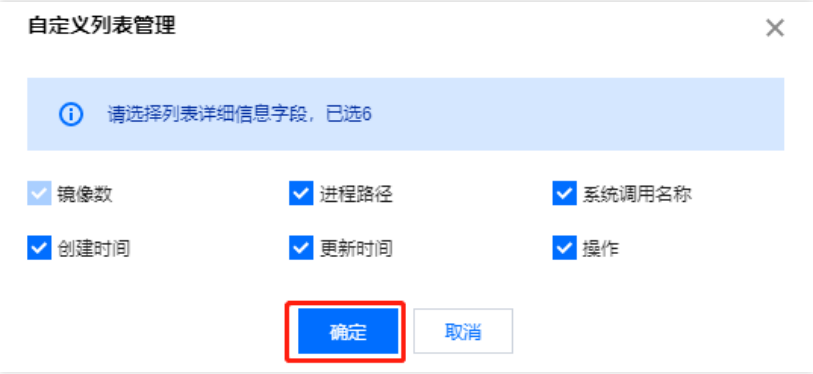
> **说明：**
>
> 删除后，白名单将无法恢复，该白名单的关联镜像触发系统策略时将再次产生告警。

自定义列表管理

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **高危系统调用** > **白名单管理**，进入白名单管理页面。

2. 在白名单管理页面，单击设置图标，弹出自定义列表管理弹窗，在弹窗中可以自定义设定列表管理。

3. 在自定义列表管理弹窗，选择所需的类型后，单击**确定**，即可完成设置自定义列表管理。



列表重点字段说明

1. 镜像数：白名单生效的镜像。

2. 进程路径：白名单生效的进程路径。

3. 系统调用名称：白名单生效的系统调用名称。

4. 操作：用户可编辑、删除白名单。

K8s API异常请求

最近更新时间: 2024-08-23 15:08:00

支持实时监控集群 API 异常请求行为，包括系统策略和用户自定义规则两部分。

- 系统策略：基于腾讯云安全技术及多维度多种手段，通过匿名访问、异常 UA 请求、匿名用户权限变动、凭据信息获取、敏感路径挂载、命令执行、异常定时任务、静态 pod 创建、可疑容器创建等共9个规则类型，对集群 API 异常请求行为进行监测。
- 用户自定义规则：支持自定义 K8s API 异常请求字段，及具体生效范围，更加灵活贴近实际业务需求。

事件列表

登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **K8s API 异常请求**，默认进入事件列表页面。

安全状态和事件趋势

- 安全状态将根据系统上报的安全事件，实时统计待处理的 K8s API 异常请求事件，以及按高危、中危、低危、提示来统计安全事件数量。

- 事件趋势将根据系统上报的安全事件，按命中的系统规则和自定义规则来统计近七天安全事件趋势。

事件列表

您可以选择"最近生成时间"来查看安全事件，或通过集群名称或集群 ID 来检索关联的安全事件。事件列表字段包括：

字段名称	字段详情
命中规则	匿名访问、异常 UA 请求、匿名用户权限变动、凭据信息获取、敏感路径挂载、命令执行、异常定时任务、静态 pod 创建、可疑容器创建等9个系统规则和用户自定义规则。
规则类型	系统规则、用户自定义规则。

字段名称	字段详情
威胁等级	高危、中危、低危和提示。
受影响集群名称/ID/运行状态	展示安全事件影响的集群名称、集群 ID 以及集群运行状态。
首次生成时间	该条安全事件首次发生的时间。
最近生成时间	该条安全事件最近发生的时间。
告警数量	系统按集群名称、集群 ID、命中规则、请求日志等对待处理安全事件进行聚合展示，聚合周期为当天。
状态	待处理、已处理、已忽略、已加白。
操作	单击**详情**，查看事件详情。

查看详情

在事件列表中，单击**详情**，查看事件详情。详情包括事件详情，集群名称/ID，集群运行时组件，风险描述，建议方案，异常请求信息和 json 日志。

事件详情
待处理
标记已处理
加白
更多操作
事件详情
事件类型
规则详情
静态Pod创建
系统规则
告警数量
356
威胁等级
低危
首次生成时间
2022-11-29 00:0...
最近生成时间
2022-11-29 15:4...
集群名称/ID
运行中
集群Master-IP
Kubernetes版本
运行时组件
风险描述
事件描述
检测到您的K8s API Server创建了静态pod，静态pod无法通过kube-apiserver进行管理，通常攻击者可利用创建静态pod的方式，运行指定的镜像。
解决方案
建议方案
请及时排查该创建静态pod的yaml文件是否为业务所需，非必要请勿使用静态pod。
如需删除静态pod，请直接删除静态pod的yaml文件，该文件通常与 API Server的yaml文件处于同一目录，
如：/etc/kubernetes/manifests。
异常请求信息
json日志
已为您自动高亮事件关联的异常请求信息：
操作类型verb
patch
日志ID
Pod名称/IP
来源IPsourceIPs
用户代理User agent
请求资源requestURI
发起请求用户User

处理事件

1. 在事件列表中，单击**处理**，可以选择对事件进行标记已处理、添加白名单、忽略和删除记录，单击**确定**。

2. 在二次确认窗口中，进行如下操作：

- 标记已处理：建议您参照事件详情中的“解决方案”，人工对该事件风险进行处理，单击**确定**，处理后可将事件标记为已处理。
- 添加白名单：配置相关参数，单击**确定**。

> **说明：**
>
> - 若您确认该 K8S API 请求属于正常行为，可添加白名单放行规则，后续再出现该请求，将直接放行不再告登，请谨慎操作。
> - 添加白名单时，系统会根据加白的来源事件自动填入触发告警的字段和集群。如有需要，可手动调整白名单的生效字段和生效集群范围。

- 忽略：单击**确定**，仅将已选事件进行忽略，若再有相同事件发生依然会进行告警。
- 删除记录：单击**确定**，删除已选事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

规则配置

登录 [容器安全服务控制台]，在左侧导航中，单击**高级防御** > **K8s API 异常请求** > **规则配置**，进入规则配置页面。

系统规则

在规则配置页面，开启或关闭系统规则和自定义规则。单击系统**规则名称**，可查看全部系统规则类型，如下图所示。用户也可以通过此页面，关闭部分系统规则类型。

规则详情

基本信息

规则名称 系统规则

启用状态 已开启

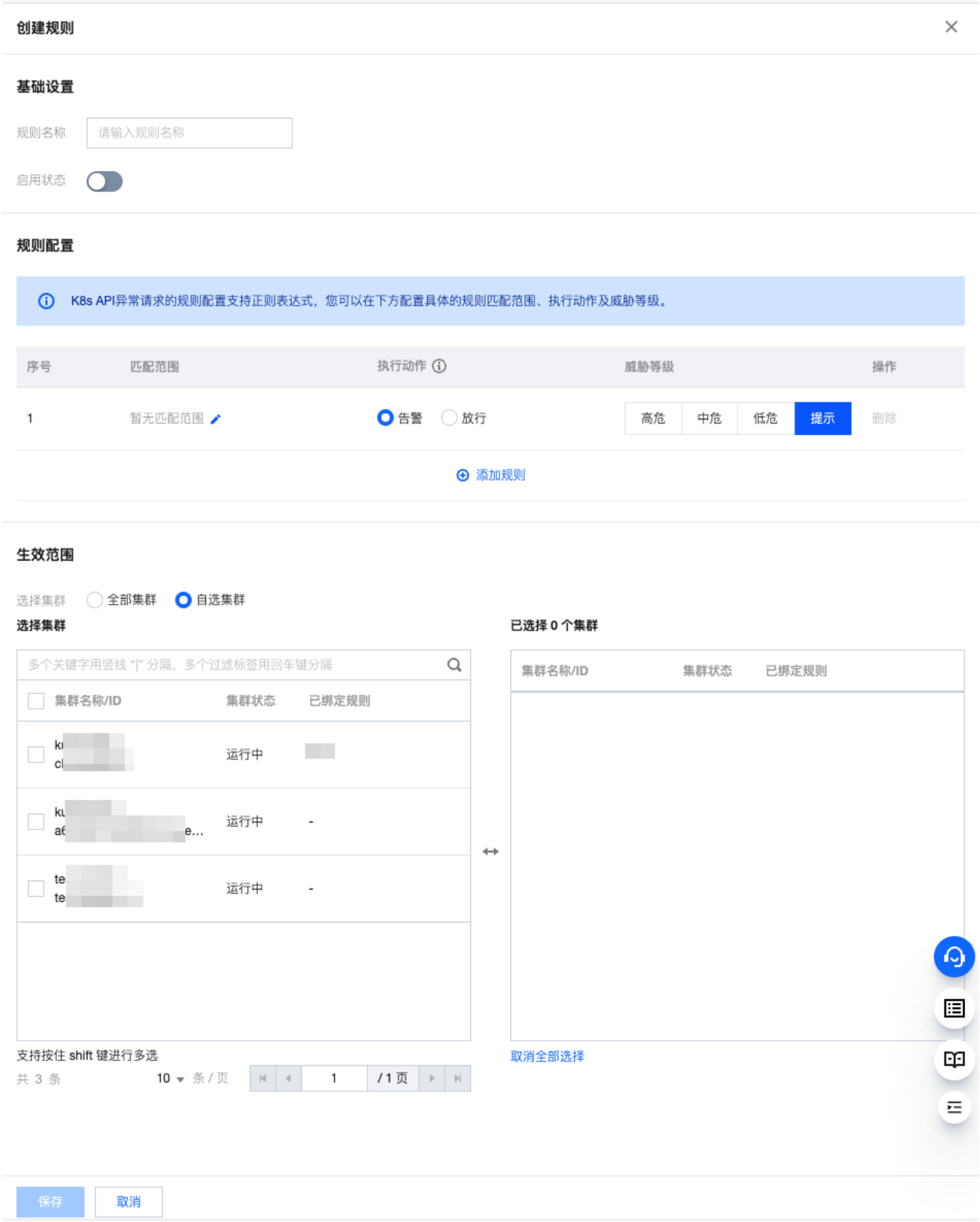
配置规则详情

序号	事件类型	执行动作	启用状态
1	匿名访问	告警	
2	异常UA请求	告警	
3	匿名用户权限异动	告警	
4	凭据信息获取	告警	
5	敏感路径挂载	告警	
6	命令执行	告警	
7	异常定时任务	告警	
8	静态Pod创建	告警	
9	异常Pod创建	告警	

共 9 项 10 条 / 页 1 / 1 页

自定义规则

除容器安全服务产品提供的系统规则，用户也可以自定义创建规则。 在规则配置页面，单击**创建规则**，配置相关参数，单击**保存**。


创建规则
基础设置
规则名称
请输入规则名称
启用状态
规则配置
K8s API异常请求的规则配置支持正则表达式，您可以在下方配置具体的规则匹配范围、执行动作及威胁等级。
序号
匹配范围
执行动作
威胁等级
操作
1
暂无匹配范围
告警
放行
高危
中危
低危
提示
删除
添加规则
生效范围
选择集群
全部集群
自选集群
选择集群
已选择 0 个集群
多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔
集群名称/ID
集群状态
已绑定规则
运行中
运行中
运行中
支持按住 shift 键进行多选
取消全部选择
共 3 条
10 条 / 页
1
/ 1 页
保存
取消

字段名称	字段详情

字段名称	字段详情
基础设置	包括自定义规则的名称，以及是否启用规则的开关。
规则设置	- 在此部分配置告警和放行的字段，配置告警字段时需同步配置规则的威胁等级。 - 当配置内容多条时，单击下方的**添加规则**即可。 - 配置规则的具体内容时，单击匹配范围列的**编辑**，规则配置支持正则表达式。
生效范围	用户可自定义选择配置规则的生效集群范围。 注意：**同一个集群只能绑定一个自定义规则**，如需对一个集群配置多条检测规则，建议在同一条规则中编辑添加。

策略管理
镜像拦截策略

最近更新时间: 2024-08-23 15:08:00

用户可在 **镜像拦截策略页面** 配置告警和拦截策略。镜像拦截策略支持您对存在严重安全问题的镜像进行容器启动拦截，避免恶意镜像运行容器业务。

- 创建并生效拦截策略后，约3-5分钟左右生效。生效后，如命中的风险镜像存在启动容器行为，系统将按照策略配置的告警、拦截要求，对镜像启动行为进行告警、或拦截容器启动并上报拦截记录。
- 目前支持拦截的镜像类型：存在严重&高危漏洞、木马病毒、敏感信息风险的镜像，特权模式启动镜像。
- 拦截特权模式镜像仅支持配置一条规则，如需修改拦截镜像的范围，可编辑调整已配置规则。

查看策略概览

用户配置告警和拦截策略后，系统将统计开启的策略总数，以及其包含的已生效拦截策略和观察期策略数量。

查看事件概览

用户配置镜像启动拦截策略后，如策略立即生效，则目标风险镜像启动容器时，将实时拦截镜像启动行为并上报事件记录；如策略配置了观察期，观察期仅告警不拦截，则目标风险镜像启动容器时，将实时上报镜像启动行为记录。两种情况均会产生事件记录。

在事件概览中，将对每日镜像启动拦截事件和仅告警的事件进行统计，展示近7日两类事件的趋势图和当前的事件总数。单击**查看事件详情**，跳转**镜像风险管理** > **镜像拦截事件**页面查看镜像拦截事件详情。

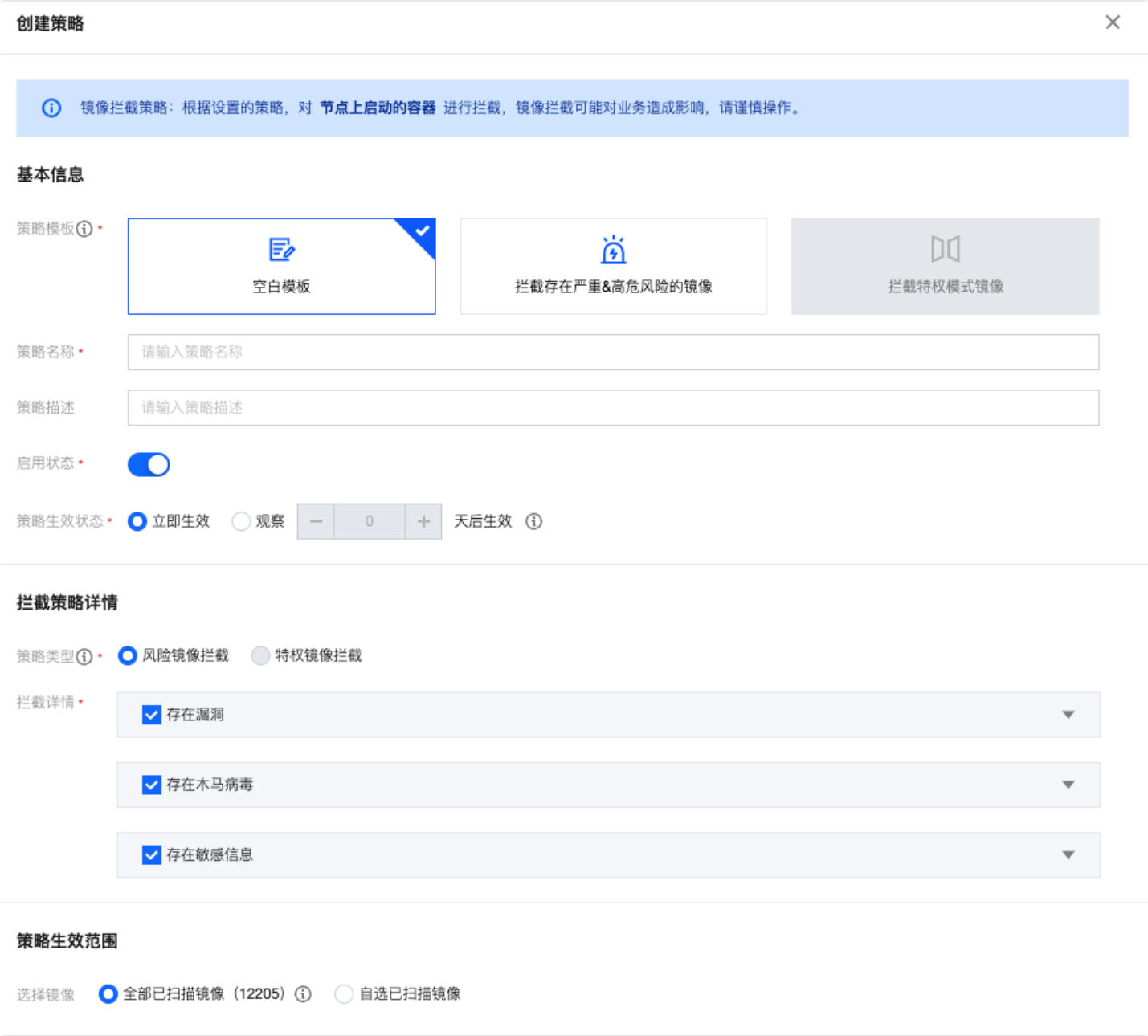
创建策略

1. 登录 [容器安全服务控制台]，在左侧导航中，选择**策略管理** > **镜像拦截策略**。

2. 在镜像拦截策略页面，单击**创建策略**，配置相关参数，单击**确定**。

> **注意：**
>
> 根据设置的策略，对节点上启动的容器进行拦截，镜像拦截可能对业务造成影响，请谨慎操作。

- 新建风险镜像拦截策略



参数类别	参数名称	参数详情
基本信息	策略模板	必选，选择“拦截存在严重&高危风险的镜像”。
	策略名称	必填，不超过128字符。
	策略描述	非必填，不超过256字符。
	启用状态	- 开启：开始执行镜像拦截动作，或观察期开始倒计时。 - 关闭：策略不生效。
	策略生效状态	- 立即生效：即策略下发完成后，命中目标镜像时，立即执行拦截动作。 - 观察 n 天生效：即观察期仅告警不拦截，观察期结束立即执行拦截动作。
拦截策略详情	策略类型	策略模板选择“拦截存在严重&高危风险的镜像”，策略类型为风险镜像拦截； 如需修改策略类型，需调整策略模板。

参数类别	参数名称	参数详情
	拦截详情	存在漏洞、存在木马病毒、存在敏感信息这三类至少需配置一项。 - 配置“存在漏洞”，可按CVE编号、组件名称及版本号、或按漏洞分类进行配置。 - 配置“存在木马病毒”，可按文件 MD5、或按木马病毒类型进行配置。 - 配置“存在敏感信息”，可按威胁等级和敏感信息的类型进行配置。
策略生效范围	选择镜像	配置风险镜像拦截时，策略生效的范围需为已扫描镜像，未扫描镜像系统无法判断是否存在漏洞、木马病毒或敏感信息风险。

- 新建特权模式镜像拦截策略新建特权模式镜像拦截策略时，如已创建过特权镜像拦截策略，则无法新建，需对已创建策略进行编辑新增；未新建时，可单击创建策略直接配置。

参数类别	参数名称	参数详情
基本信息	策略模板	必选，选择“拦截存在严重&高危风险的镜像”。
	策略名称	必填，不超过128字符。
	策略描述	非必填，不超过256字符。
	启用状态	- 开启：开始执行镜像拦截动作，或观察期开始倒计时。 - 关闭：策略不生效。

参数类别	参数名称	参数详情
	策略生效状态	- 立即生效：即策略下发完成后，命中目标镜像时，立即执行拦截动作。 - 观察 n 天生效：即观察期仅告警不拦截，观察期结束立即执行拦截动作。
拦截策略详情	策略类型	策略模板选择“拦截存在严重&高危风险的镜像”，策略类型为风险镜像拦截； 如需修改策略类型，需调整策略模板。
	拦截详情	用户可对特权启动参数进行勾选，默认选择全部。系统将特权参数类型分为5大类，基础权限、文件操作权限、系统操作、网络操作和高危权限。用户可对大类，或某种大类中的具体分类进行调整。
策略生效范围	生效方式	配置特权镜像拦截策略时，生效方式包括“选中的镜像不允许以特权模式运行”，或“仅选中的镜像允许以特权模式运行（其他镜像特权启动将阻止运行）”。
	选择镜像	用户可选择全部镜像或自选镜像。

管理策略

- 查看：在镜像拦截策略页面，单击**镜像拦截策略名称**，查看拦截策略详情，
- 开启或关闭：通过开启或关闭启动状态列的按钮调整策略是否生效。
- 开启后，开始执行镜像拦截动作，或观察期开始倒计时。
- 关闭时，策略不生效。
- 编辑：单击**编辑**，对策略的名称、描述、启动状态、策略生效状态、拦截策略详情、策略生效范围进行调整；策略模板不可调整。

告警设置

最近更新时间: 2024-08-23 15:08:00

本文档将指导您如何为镜像安全事件和运行时安全事件配置告警策略。

前提条件

请确认消息订阅中“安全消息-安全事件通知”已打开，单击 [进入设置]。

事件类型

告警设置中事件类型、默认告警时间和告警如列表所示：

事件类型	默认告警时间	默认告警项
安全漏洞	全天	严重
木马病毒	全天	严重、高危、中危、低危
敏感信息	全天	严重、高危、中危、低危
容器逃逸	全天	-
异常进程	全天	拦截失败、告警
文件篡改	全天	拦截失败、告警
反弹 Shell	全天	-
文件查杀	全天	-

操作步骤

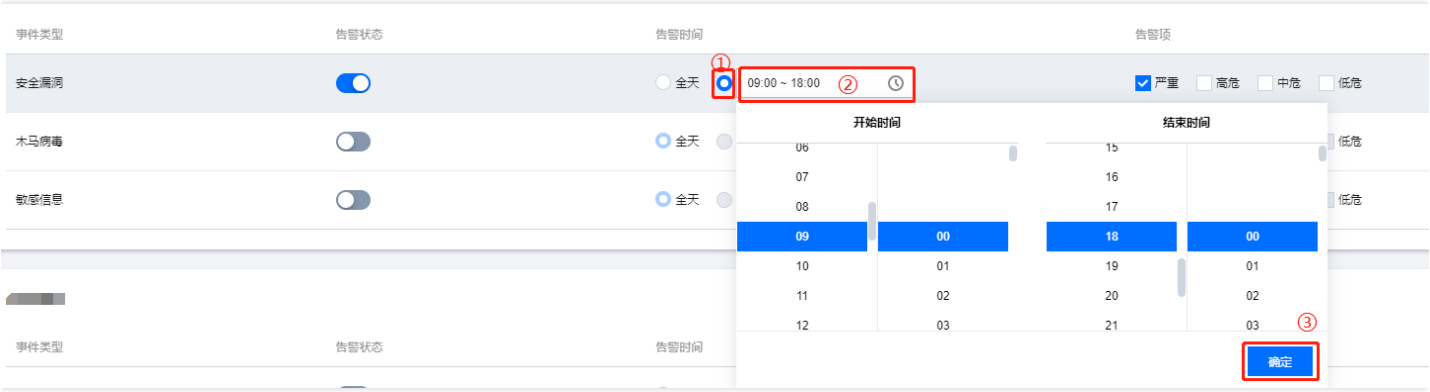
1. 登录 [容器安全服务控制台]，在左侧导航中，单击**告警设置**。

2. 在告警设置页面，单击开启“告警状态”，开启告警设置模式。

3. 开启告警设置模式后，告警时间可以单击选择全体或自定义时间。

- 单击全天左侧图标，即可完成全天告警通知设置。

- 单击自定义时间框左侧图标，按需选择开始时间和结束时间后，单击**确定**，即可完成自定义时间通知设置。



日志分析

概述

最近更新时间: 2024-08-23 15:08:00

本文档将为您介绍如何使用日志分析功能，查看容器 bash 日志、容器启动审计日志和 Kubernetes API 审计日志，以及相关日志配置和日志投递操作。

背景信息

日志分析提供容器 bash 日志、容器启动审计日志和 Kubernetes API 审计日志等多维度日志，支持语句检索和查询，并提供可视化报表、统计分析和导出功能，帮助用户能够快速的查询容器相关业务日志、溯源容器安全事件，提升运营效率。

- 容器 bash 日志：提供 bash 日志审计，帮助用户溯源异常进程。
- 容器启动审计日志：提供容器启动日志审计，帮助用户记录容器启动行为。
- Kubernetes API 审计日志：帮助用户记录 k8s API 调用的日志。

根据《中华人民共和国网络安全法》、《信息安全等级保护管理办法》规定，日志存储时长不少于6个月，建议用户对核心资产开启日志审计功能，根据实际所需购买存储，以便采集和留存日志数据。

容器安全服务专业版提供日志采集功能，建议用户购买专业版后再购买日志存储。若已购买日志存储，但出现容量不够的情况，此时日志分析服务将会对历史日志数据进行清理，建议用户及时升级扩容。

前提条件

日志分析存储为容器安全服务的增值服务，需进入 [容器安全服务购买页] 独立购买。

查询日志

最近更新时间: 2024-08-23 15:08:00

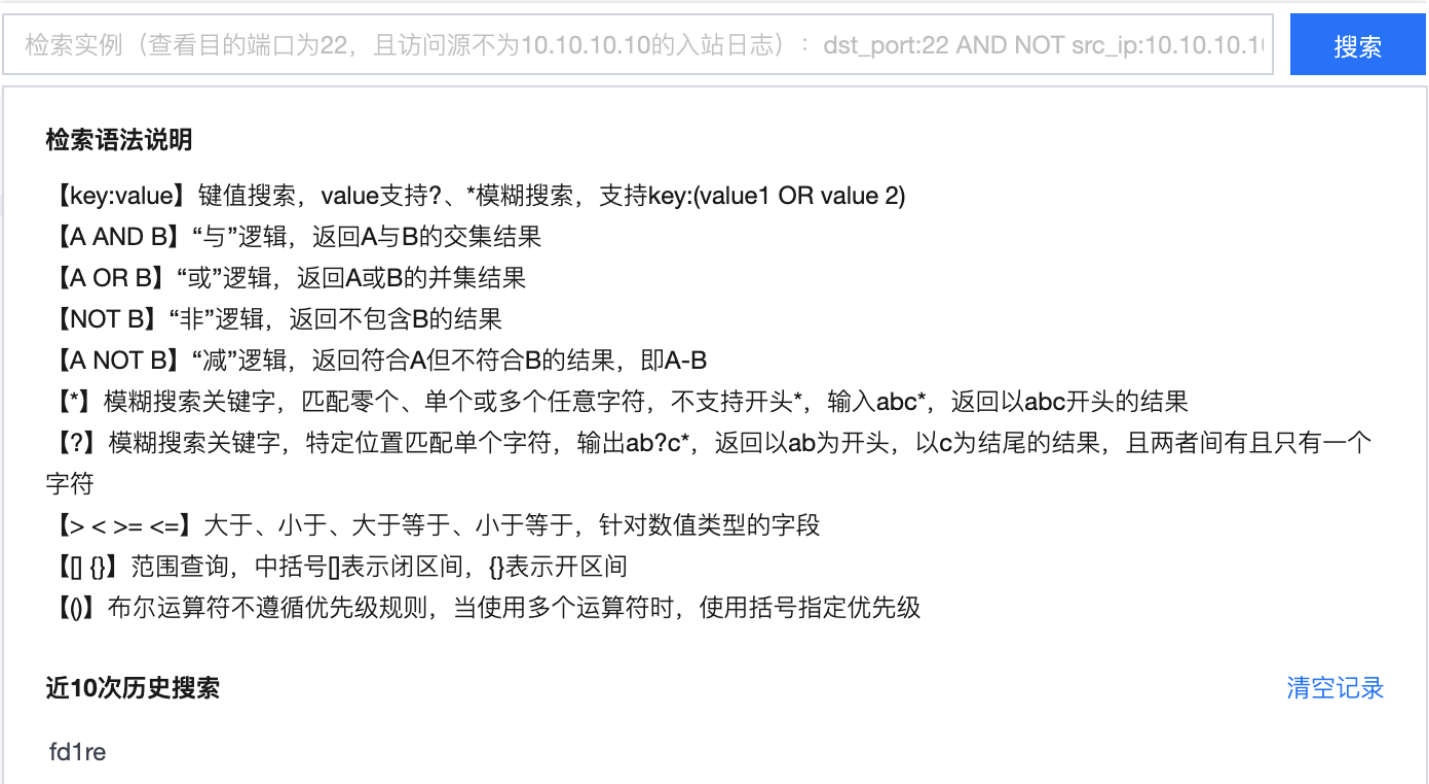
1. 登录 [容器安全服务控制台]，在左侧导航中，单击**安全运营** > **日志分析**。

2. 在日志分析页面，检索日志分析结果并进行相关操作。

- 按时间类型筛选日志：在日志分析页面上方，支持按时间（近15分钟、近60分钟、近12小时、近24小时、今天、近7天、近14天、近30天、近90天及自定义日期）、日志类型筛选日志分析结果，选择需要查看的时间和日志类型，单击**确定**即可。

- 按纪录字段筛选日志：在日志分析页面上方，支持按日志记录字段筛选，提供手动输入字段、自动输入字段两种方式。

  -手动输入字段：在输入框内以字段名和字段值成对的形式输入需要筛选的字段，单击**搜索**即可。可参考下图检索语法说明。



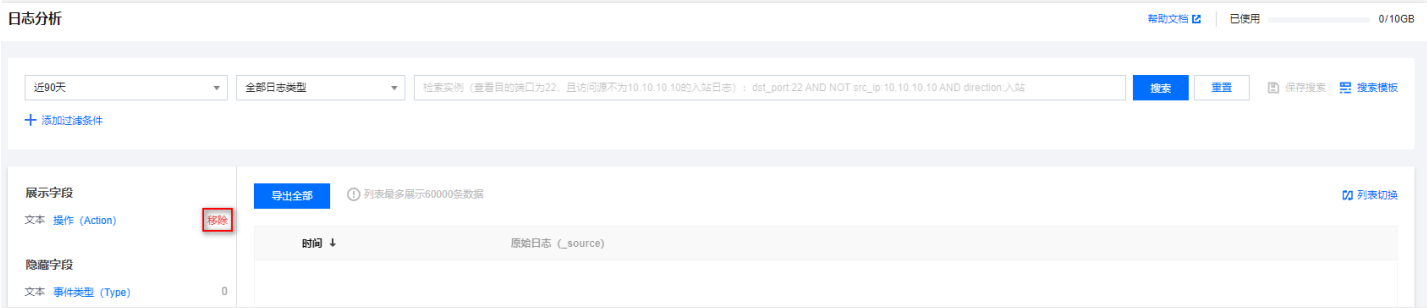
-自动输入字段：单击**搜索模板**，选中需要复用的查询模板名称即可。或单击筛选输入框中的**历史纪录**，如上图所示。复用查询模板，需用户在手动输入查询语句时，单击**保存搜索**以达到保存当前配置（日志类型、检索语句）的目的。

- 快速检索查看日志趋势图：
- 方式1：为了方便对指定时间范围内的日志量进行查看，您可以滑动鼠标快速查看日志趋势图上的"蓝色柱形图"，查看日志统计时间和日志量。
- 方式2：单击日志趋势图"蓝色柱形图"，可进一步对日志进行放大检索。

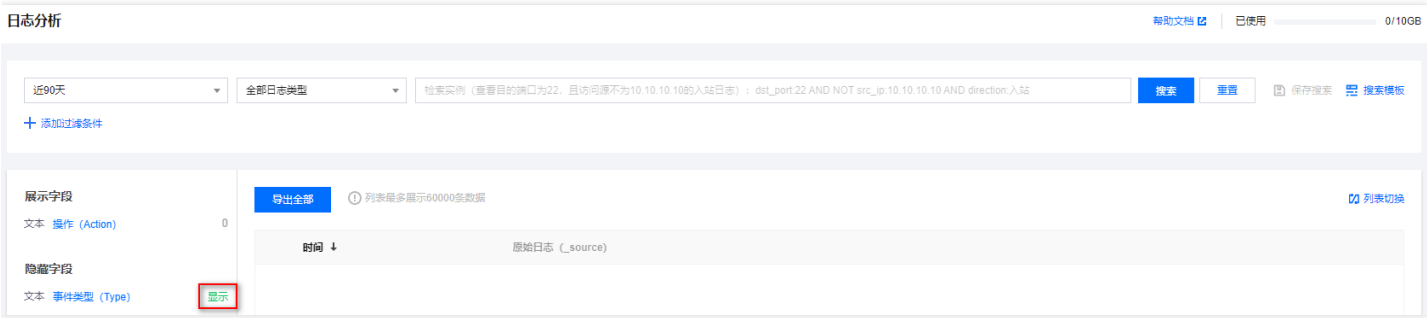
3. 在日志分析页面的日志列表中，根据"展示字段"模块内容，在列表中展示并查看相关字段详情。展示字段中为"原始日志（_source）"时，列表中展示所有日志字段。列表最多展示60000条数据。

- 自定义需要展示或隐藏的字段：

  -显示：将鼠标移动至隐藏字段上方，在隐藏字段右侧，单击**显示**，该隐藏字段将出现在展示字段中，列表中仅展示选定显示的字段，其他隐藏字段不展示。



-隐藏：将鼠标移动至展示字段上方，在展示字段右侧，单击**移出**，该隐藏字段将在展示字段中删除，对应右侧日志列表将不再展示该字段内容。



- 导出：在字段详情左上角，单击**导出全部**，日志分析会将满足检索条件的60000条日志导出为文件，并通过浏览器下载到本地。

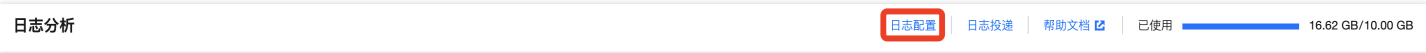
- 切换表格列展示：在字段详情右上角，单击**列表切换**，可将展示字段切换为表格列展示。

配置日志

最近更新时间: 2024-08-23 15:08:00

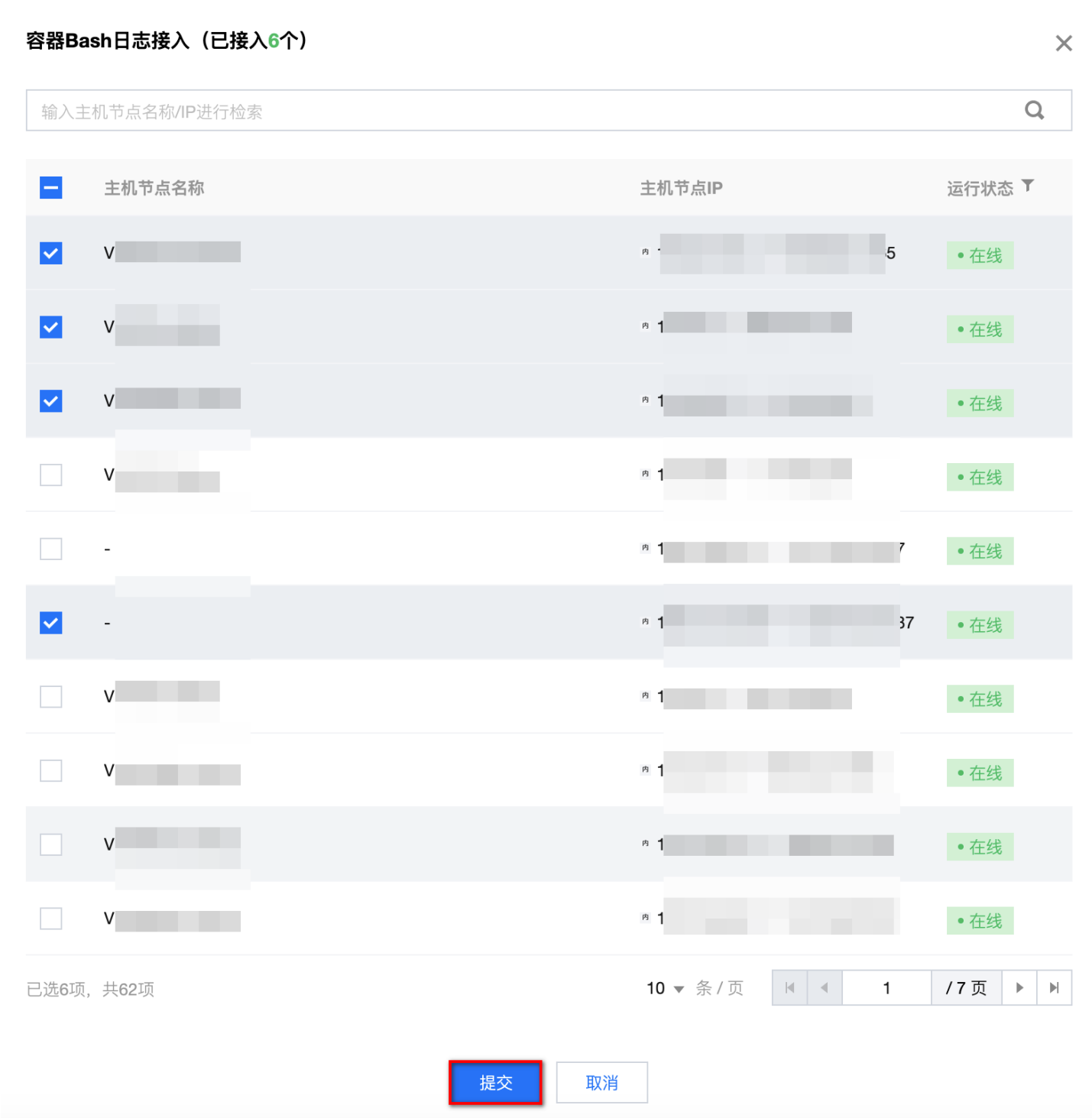
日志接入

1. 在 [日志分析页面]，单击页面上方的**日志配置** > **日志接入**。



2. 在日志接入页面，支持对容器 bash 日志、容器启动审计日志和 Kubernetes API 审计日志是否开启采集进行配置。在“是否接入日志”列开启开关，即可对该类日志进行采集。关闭按钮，即不对该类日志进行采集。

3. 在日志接入页面，单击已接入资产列的**编辑**，即可配置采集日志的节点范围。勾选需要采集日志的主机节点，单击**提交**后，配置生效。



日志清理

1. 在 [日志分析页面]，单击页面上方的**日志配置** > **日志清理**。

2. 在日志清理页面，支持用户按百分比或存储天数清理日志。

- 按百分比清理日志：当日志存储量达到用户配置百分比时，开始清理历史日志，清理到用户配置的清理百分比。
- 按存储天数清理日志：当日志存储天数达到用户配置数值时，开始清理历史日志，仅保留用户配置天数的日志。

> **说明：**
>
> 两种日志清理方式同时生效，当任一情况满足时即开始日志清理。

混合云安装指引
概述

最近更新时间: 2024-08-23 15:08:00

背景信息

随着企业上云率提升，更多中大型企业选择公有云+私有云的混合云模式，兼具公有云成本低、敏捷、灵活、使用方便及私有云可控、安全、高可用部署的优点。而混合云管理功能的上新能够支持客户接入非腾讯云机器，帮助更好地用户统一管理和监控容器安全。

功能概述

- 支持腾讯云的边缘计算机器、轻量应用服务器自动接入容器安全。
- 支持非腾讯云服务器，如：私有云、阿里云、华为云、青云、亚马逊云、UCloud 等云服务器手动接入容器安全。

客户端支持版本说明

Linux 系统支持版本：

- RHEL: Versions 6 and 7(64 bit)。
- Ubuntu: 9.10 - 18.04(64 bit)。
- Debian: 6, 7, 8, 9(64 bit)。
- CentOS: Versions 6 (64 bit)及以上。

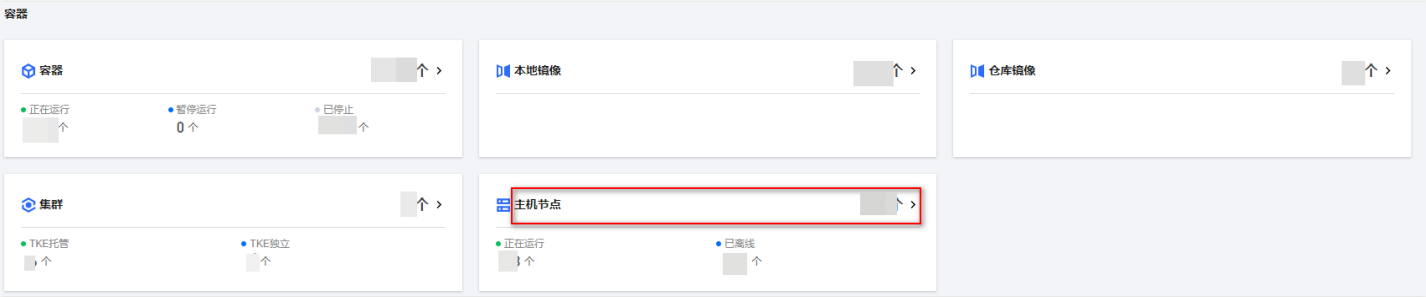
配置非腾讯云机器

最近更新时间: 2024-08-23 15:08:00

步骤1：安装容器安全服务客户端

1. 登录 [容器安全服务控制台]，在左侧导航中单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击容器的**主机节点** > **安装容器安全服务 Agent**，在右侧弹窗中查看安装指引详情。



3. 在安装指引中选择服务器类型、服务器产品及推荐安装方式。如果是通过专线打通云上云外的话，选择专线安装方式，否则选择公网的安装方式。

- 通过公网接入：单击复制图标并执行相应命令，即可安装容器安全服务客户端，需注意命令有效期。

- 通过专线接入：选择已连专线的 VPC，单击复制图标并执行相应命令，即可安装容器安全服务客户端，**需注意命令有效期**。

> **说明：**
>
> - 如需了解专线相关，可单击**了解专线**跳转专线接入控制台。
> - 如防火墙需开放目标 IP，参考图片对命令中 IP 开放访问权限。

步骤2：确认是否安装成功

1. 按照安装指引判断是否安装成功的命令执行，打开任务管理器确认 YDLive 进程有运行，即安装成功。

- 执行命令： `ps -ef | grep YD` 查看 YDService，YDLive 进程是否有运行。
- 进程无运行，root 用户可手动启动程序，执行命令： `/usr/local/qcloud/YunJing/YDEyes/YDService` 。

```
[root@VM_90_131_centos conf]# ps -ef|grep YD
root     16216 21992  0 14:33 pts/3    00:00:00 grep --color=auto YD
root     32707     1  0 11:23 ?        00:00:09 /usr/local/qcloud/YunJing/YDEyes/YDService
root     32724     1  0 11:23 ?        00:00:01 /usr/local/qcloud/YunJing/YDLive/YDLive
[root@VM_90_131_centos conf]# ps -ef|grep YD
```

2. 安装成功后在 [主机节点]页面，单击选择**主机来源** > **非腾讯云服务器**，即可查看对应服务器。

3. 当 Agent 状态显示为**在线**状态，即已安装成功服务已上线。

> **说明：**
>
> 如未正常上线，请 联系我们 获得支持。

主机名称/IP	业务组	主机来源	Agent状态	Docker版本	Containerd版本	文件系统类型	容器数	镜像数	操作
- 外	-	非腾讯云服务器	在线	未安装	-	-	0	0	卸载Agent
	-	非腾讯云服务器	在线	20.10.11	-	overlay2	4	1	卸载Agent

连接专线VPC

最近更新时间: 2024-08-23 15:08:00

背景信息

目前 VPC 专线接入暂时只支持华南地区（广州）、华北地区（北京）、华东地区（上海、上海金融、南京）， 西南地区（成都），已经支持公有云与客户机房网络在 VPC 内互通，可以直接安装客户端。

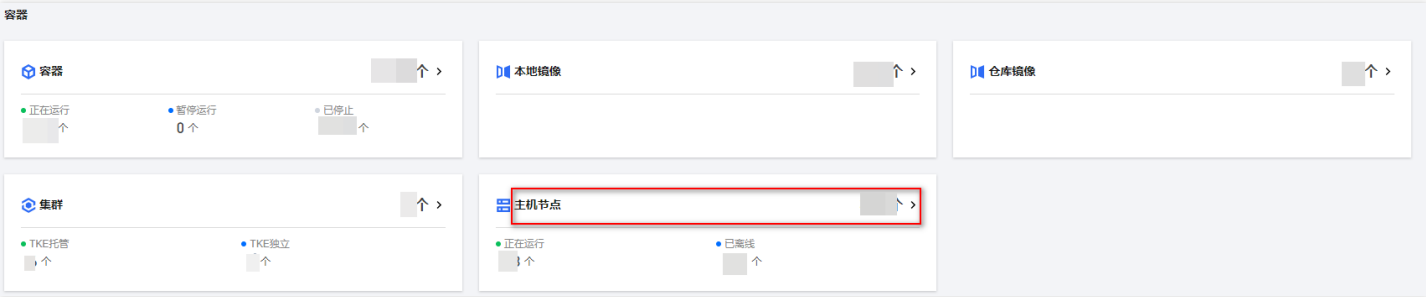
若需要接入的地区不在 VPC 专线接入的范围之内，需要通过云联网，将专线网关（VPN）与 VPC 打通。专线网关需要客户另行购买和搭建完成对 VPC 专线接入的工作。

操作指南

步骤1：确认是否需要通过云联网进行接入

1. 登录 [容器安全服务控制台]，在左侧导航中单击**资产管理**，进入资产管理页面。

2. 在资产管理页面，单击容器的**主机节点** > **安装容器安全服务 Agent**，在右侧弹窗中查看安装指引详情。



3. 在安装指引中，服务器类型单击选择**非腾讯云**，推荐安装方式单击选择**专线**。

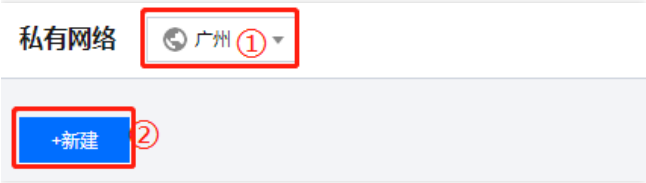
4. 如您在华南地区（广州）、华北地区（北京）、华东地区（上海）、华东地区（上海金融）、华东地区（南京）和西南地区（成都）地区：

- 已有和非腾讯云机房网络互联的 VPC，则选择已连接专线的 VPC 网络，直接使用安装命令安装。
- 没有找到相应的 VPC 网络与您的非腾讯云机房网络进行互联，可参考步骤2云联网。

步骤2：确认用于连接专线的私有网络

1. 如您在当前华南地区（广州）、华北地区（北京）、华东地区（上海）、华东地区（上海金融）、华东地区（南京）和西南地区（成都）地区没有 VPC 网络，则登录私有网络控制台，单击**私有网络**进入私有网络页面。

2. 在私有网络页面中，单击"下拉框"选择所需区域，单击 **+新建**，弹出新建 VPC 弹窗。



3. 在新建 VPC 弹窗中，输入所需参数单击**确定**，即可完成新建 VPC。

步骤3：通过云联网实现 VPC 和已连专线的非腾讯云机房网络互通

1. 如已存在和非腾讯云机房通信的云联网，则将步骤2中选择的 VPC 实例添加到云联网中。 a. 登录私有网络控制台，在左侧导航栏，单击**云联网**，进入云联网页面。
   b. 在云联网页面，单击右侧**管理实例** > **关联实例**，进入关联实例页面。 c. 在关联实例页面，单击**新增实例**，将步骤2中选择的 VPC 实例添加到云联网中，单击**确定**即完成关联实例。

2. 如尚未配置云联网，则需要新建。 a. 登录私有网络控制台，在左侧导航栏，单击**云联网**，进入云联网页面。
   b. 在云联网页面中，单击**+新建**，弹出新建云联网实例弹窗。 c. 在新建云联网实例弹窗，输入所需参数单击**确定**，即可完成新建云联网实例。

> **说明：**
>
> - 专线网关：请选择您和非腾讯云机房通信连接的专线网关。
> - 私有网络：请选择 步骤2 中选择的 VPC 实例。
> - 如出现 IP 地址段冲突，请返回 步骤2 重新选择或新建一个不会冲突的 VPC 实例。

3. 回到 [容器安全服务控制台]，参考步骤1获取安装命令进行安装。您的非腾讯云机房需要放通对步骤1中描述的 IP 的5574、8080、80、9080共4个端口的访问。

热点问题

最近更新时间: 2024-08-23 15:08:00

专线连接到云端，目标地址和开放端口是多少？

请参考下图的目标地址和开放端口，放通防火墙权限。

> **说明：**
>
> 地址和开放端口是不会变化。

常见问题排查

防火墙拦截

建议防火墙策略放过容器安全服务后台服务器访问地址

基础网络域名	s.yd.qcloud.com, l.yd.qcloud.com, u.yd.qcloud.com	基础网络端口	5574, 8080, 80, 9080
VPC网络域名	s.yd.tencentyun.com, l.yd.tencentyun.com, u.yd.tencentyun.c...	VPC网络端口	5574, 8080, 80, 9080
公网域名	sp.yd.qcloud.com, lp.yd.qcloud.com, up.yd.qcloud.com	公网端口	5574, 8080, 80, 443, 9080

国外的 IDC 是否支持安装 Agent?

支持的，目前只要机器能够联网，系统满足要求，就可以安装容器安全服务 Agent。

安装 Agent 后，控制台目前多久会展示非腾讯云机器？

整点自动开启新增机器的服务。

非腾讯云机器，需要另外购买控制台吗？

不需要的，统一在公有云控制台进行管理、计费。

需要开 IDC 到云上的网络端口访问权限，目标 IP 和端口是什么？

目标 IP 是安装命令内的 IP，端口5574 80 8080 9080。

内网机器，无法访问公网或者没有专线的情况下是不是无法使用云镜？

目前是的。

混合云的客户端会和 Zabbix 进程冲突吗？

我们没有对 Zabbix 做特殊处理，也没有注入等，可以关注下机器上是否有其他的客户端安装驱动。

失陷容器隔离说明

最近更新时间: 2024-08-23 15:08:00

当用户业务环境中的容器遭遇攻击，例如发生容器逃逸、容器中了木马病毒或传播性较强的蠕虫病毒、容器失陷后对内发起横向探测或横向攻击、攻击者利用集群和节点等的漏洞或配置不当风险拉起恶意容器时，急需对相应的风险容器进行网络隔离。

> **说明：**
>
> 隔离容器网络的操作可能会影响业务正常运行，建议您排查确认为风险容器、且需要隔离来避免入侵行为进一步恶化时使用该功能。

隔离容器网络

用户可在 [运行时安全]、[高级防御] 或 [资产管理] 使用隔离容器网络功能。在不同模块使用该功能的效果有所不同，具体如下表所示：

模块名称	功能详情
容器逃逸	在某个安全事件处隔离容器成功后，系统将禁止该容器的网络通信，并将该安全事件标记为已处理。
反弹Shell	
异常进程	
文件篡改	
高危漏洞系统	
文件查杀	由于仅隔离容器并不能清除容器木马病毒风险，所以在某个安全事件处隔窝容器成功后，系统将禁止该容器的网络通信，但并不会将该安全事件标记为已处理，用户仍需对容器内的木马病寿进行自动隔离或手动隔离来更改事件状态。

运行时安全或高级防御

1. 登录 [容器安全服务控制台]，在左侧导航中，单击**运行时安全** > **容器逃逸**。

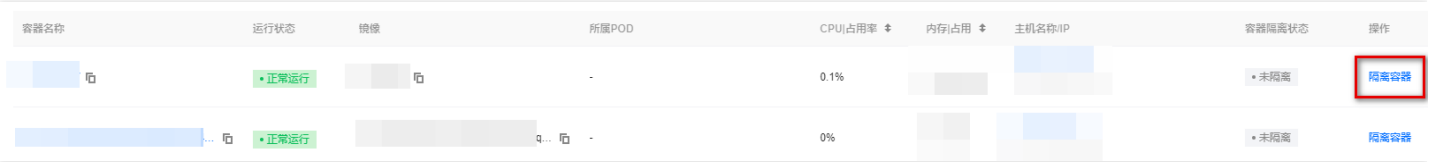
2. 在容器逃逸页面，选择所需容器，单击操作列的**处理**。

3. 选择**容器隔离**，并填写备注，单击**确定**。

资产管理

1. 在 [资产管理页面]，单击**容器**。

2. 在容器页面，选择所需容器，单击**隔离容器**。

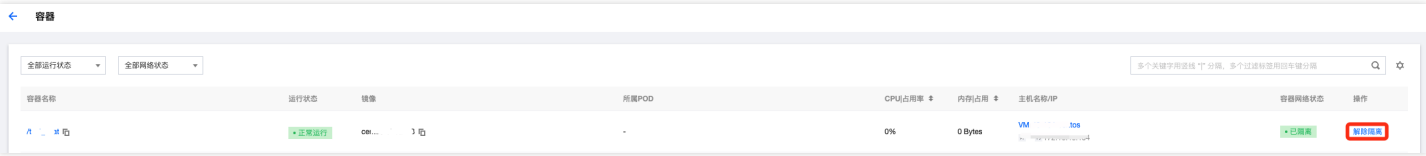


3. 在确认隔离弹窗中，单击**确定**，即可隔离该容器。

> **注意：**
>
> 确认后，将隔离此容器，系统将禁止该容器的网络通信，请谨慎操作。

解除容器网络隔离

当用户对容器存在的风险处理完毕、需恢复容器网络通信时，可在 [运行时安全] 或 [高级防御] 的安全事件列表中，单击**更多**，选择**解除隔离**；或者在 [资产管理]> **容器**，选择所需容器，单击**解除隔离**。



查看容器隔离状态

不论在 [运行时安全]、[高级防御] 或 [资产管理] 中隔离容器，容器隔离状态会作为容器资产属性之一进行刷新。例如在**运行时安全** > **容器逃逸**事件列表中对某一个容器进行网络隔离，隔离成功后，在**资产管理** > **容器**列表中查看该容器时，容器为已隔离。同理，在**资产管理** > **容器**列表中隔离容器网络，也会同步刷新运行时安全或高级防御的安全事件中的容器隔离状态。

用户可通过列表上方的全部容器隔离状态筛选框，对不同隔离状态的容器事件进行筛选。

最佳实践-新
容器安全等保测评解读

最近更新时间: 2024-08-23 15:08:00

容器安全服务（Tencent Container Security Service, TCSS）产品符合等级保护2.0标准体系主要标准。在一般测评实施过程中能够帮助企业满足**容器、镜像、主机、Kubernetes 资产层面**的杀毒、主动入侵防御、定期漏洞扫描等方面要求。

根据《网络安全等级保护基本要求》（GB/T 22239-2019），容器安全服务满足第三级及以下安全要求：

序号	等保标准章节	等保标准序号	等保标准内容	对应功能描述
1	安全区域边界—入侵防范	8.1.3.3 b）	应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。	容器安全可实时监控容器内的攻击行为，对恶意命令、横向渗透、反弹 Shell 等类型的异常进程进行实时告警及拦截。
2	安全区域边界—入侵防范	8.1.3.3 c）	应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。	容器安全可对容器、镜像、kubernetes 资产环境进行实时检测，对容器逃逸、集群漏洞、挖矿病毒等新型攻击行为和新型样本进行检测告警。
3	安全计算环境—安全审计	8.1.4.3 a）	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。	容器安全支持对高危命令、高危操作进行审计，并支持对容器 bash 日志、容器启动日志和 k8s api 请求日志进行审计和记录（灰度中）。
4	安全计算环境—入侵防范	8.1.4.4 e）	应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。	容器安全支持检测镜像及集群中存在的安全漏洞，评估风险级别并提供修复建议。
5	安全计算环境—入侵防范	8.1.4.4 f）	应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	容器安全支持检测容器内的入侵行为，主要包括容器逃逸，反弹 Shell，恶意文件，异常进程启动，文件篡改，高危系统调用等，提高告警及部分主动拦截能力。
6	安全计算环境—恶意代码防范	8.1.4.5	应采用免受恶意代码攻击的技术措施或采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	容器安全支持恶意文件查杀功能，实时监测容器内木马病毒并支持隔离恶意文件。

镜像漏洞扫描和漏洞管理

最近更新时间: 2024-08-23 15:08:00

镜像安全是容器稳定运行的必备条件，当镜像存在安全风险时，风险镜像运行的容器随时可能遭受攻击、影响线上运行业务稳定性。因此在业务上线之前，需对即将应用到的镜像进行安全风险评估，确认无风险后再投入使用。

镜像安全风险主要涉及漏洞、木马和敏感信息泄漏，其中涉及到的镜像漏洞及漏洞管理问题尤其重要。在对镜像漏洞进行扫描和管理时，主要分为两个阶段进行管理：上线前、上线后。

- 上线前：镜像存储在仓库，客户需要对仓库镜像的安全性进行保障。
- 上线后：拉取到云服务器的镜像称为本地镜像，业务方需及时评估最新漏洞、应急漏洞等是否影响到运行业务的镜像。

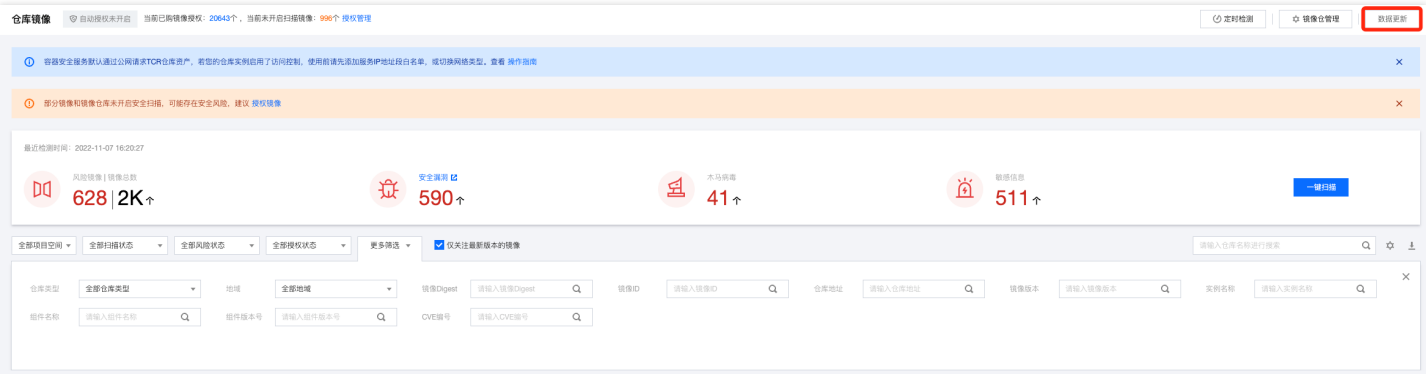
仓库存储阶段

镜像上线之前，客户将打包或下载好的镜像存储在仓库，入仓时需对新入仓的镜像进行整体安全评估，**如存在安全问题，建议修复后再入仓管理。**

拉取仓库镜像

容器安全服务支持的仓库类型包括：腾讯云 TCR 镜像、腾讯云 CCR 镜像、Harbor 镜像。

- TCR 和 CCR 镜像默认自动拉取，当有新镜像入仓时，在 [仓库镜像页面]，单页右上角的**数据更新**即可更新资产。



- 当客户镜像存储在 Harbor 仓库时，客户**需手动接入仓库再拉取镜像资产**。在[仓库镜像页面]，单页右上角的**镜像仓管理** > **新增镜像仓**，按要求验证仓库基本信息、连接地址等即可。

扫描与查看仓库镜像漏洞

在[仓库镜像页面]，勾选新增的待评估镜像进行授权并扫描镜像。扫描完成，进入 [漏洞管理页面]查看扫描出的漏洞。

如需查看全部漏洞，依次单击**系统漏洞**和**应用漏洞**，导出所有漏洞列表，在列表中查看影响仓库镜像的漏洞即可。一般情况下，镜像扫描的漏洞数据较多，全部修复工作量较大，建议区分优先级依次修复，例如：按应急漏洞，按具有 EXP、POC、远程利用、在野利用等标签等。

- POC（Proof of Concept）：可通过一段描述或样例来证明漏洞确实存在。
- EXP（Exploit）：一段对漏洞如何利用的详细说明或者一个演示的漏洞攻击代码，可以使得读者完全了解漏洞的机理以及利用的方法。
- 远程利用漏洞：指攻击者可以直接通过网络发起攻击并利用的软件漏洞。例如这类软件漏洞中的 RCE（远程代码执行）漏洞危害极大，攻击者能随心所欲地通过此漏洞对远端计算机进行远程控制，此类漏洞也是蠕虫病毒主要利用的漏洞。
- 本地利用漏洞：指攻击者必须在本机具有访问权限的前提下才能攻击并利用的软件漏洞。比较典型的是没有网络服务功能的本地软件漏洞，以及本地权限提升漏洞。例如本地提权漏洞能让普通用户获得最高管理员权限甚至系统内核的权限。
- 在野利用：该类漏洞存在在野利用或云平台上存在在野攻击（数据来源：we-detect 和 cisa）。

按应急漏洞

建议优先修复应急漏洞。对所有应急漏洞进行扫描之后，扫描完成单击导出图标，在列表中查看影响仓库镜像的漏洞，对存在应急漏洞的仓库镜像进行修复。

按具有 EXP、POC、远程利用、在野利用等标签

应急漏洞修复完成后，客户可优先挑选具有 EXP、POC、远程利用、在野利用等标签的系统漏洞和应用漏洞进行修复。对风险标签进行筛选，单击导出图标，选择**仅导出筛选结果**，在列表中查看影响仓库镜像的漏洞，对存在这些标签的仓库镜像进行修复。

除了上述标签，客户在筛选仓库镜像漏洞时，也可利用“仅展示影响最新版本的镜像”、“威胁等级”、“CVSS”评分等条件进行综合筛选。

本地应用阶段

镜像安全风险问题在仓库存储阶段得到监控和修复后，在本地应用阶段则仅需关注新增漏洞的问题。本地镜像如存在严重的漏洞问题，可能直接影响线上业务。

授权与扫描本地镜像

容器安全服务会在每天的资产自动更新时，默认更新云服务器上存在的镜像，无需客户手动拉取。客户如需关注重点业务镜像的安全风险，可按如下步骤操作：

步骤1：授权镜像

1. 在仓库镜像，单击页面上方的**授权管理**。

2. 在授权管理页面中，镜像范围筛选选择**仅关注关联容器数不为0的镜像**，并搜索所需内网 IP，配置相关参数，单击**确认授权**。

授权管理
购买授权
批量授权
自动授权
授权记录
本地镜像授权
已选择： 0 个
仓库镜像授权
已选择： 0 个
本地镜像授权
选择镜像
自选未授权镜像
全部未授权镜像（93）
镜像范围筛选
仅关注关联容器数不为0的镜像
选择镜像
选择全部
已选择 0 个镜像
取消全部选择
内网IP:
镜像名/ID
关联主...
关联容...
镜像名/ID
关联主机数
关联容器数
支持按住 shift 键进行多选
共 41 条
10 条 / 页
1
/ 5 页
仓库镜像授权
选择镜像
自选未授权镜像
全部未授权镜像（786）
仓库类型
全部仓库类型
项目空间
全部项目空间
镜像范围筛选
仅关注最新版本的镜像
确认授权
取消

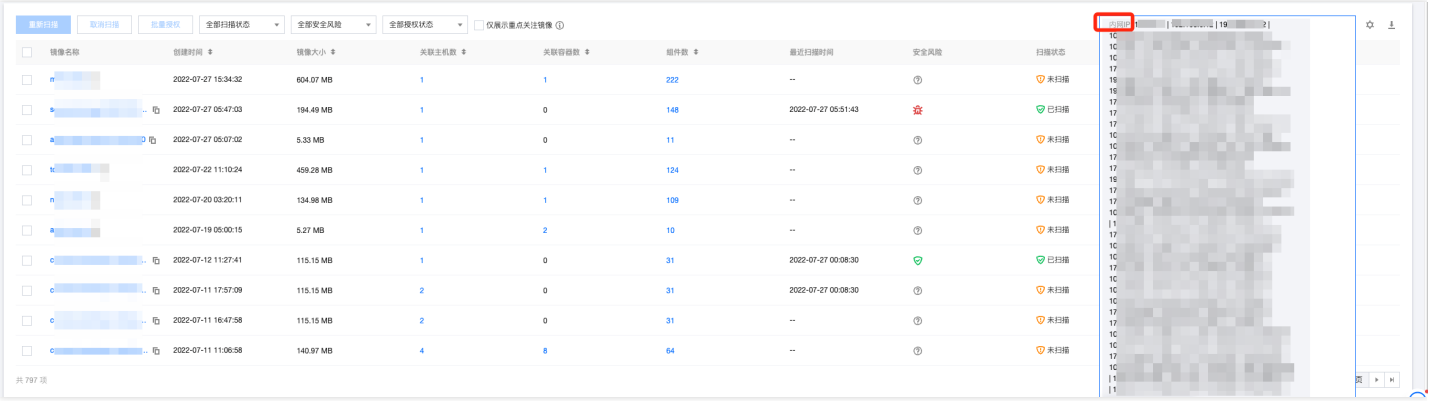
说明：

授权镜像时，可支持多内网 IP 进行检索，筛选关注节点、且运行有容器的镜像：多内网 IP 检索时，使用英文“|”对 IP 进行分隔，可使用文档替换工具，批量将列表中的换行符替换为“|”。目前前端限制多 IP 检索的数量为200个，建议不要超过这个量，否则数据量大的时候容易检索超时。

步骤2：扫描镜像

在完成授权操作后，可保证授权的镜像仅为筛选的节点上的镜像，且镜像有容器在运行。在实际业务运行中，节点上镜像是否运行容器、是否新增，可通过在本地镜像列表进行筛选。

客户可在 [本地镜像页面] ，通过内网多 IP 检索、以及选择已授权镜像的方式，选择需要扫描漏洞风险的本地镜像。



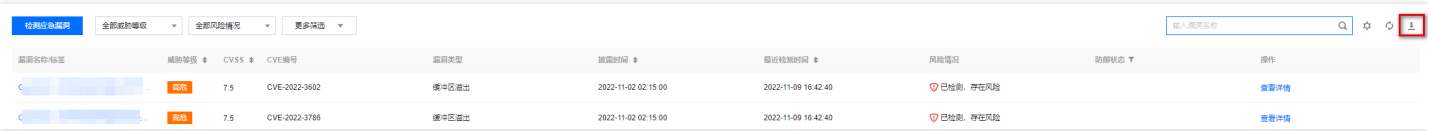
查看本地镜像漏洞

扫描漏洞任务完成后，进入 [漏洞管理页面] 查看扫描出的漏洞。

如需查看全部漏洞，依次单击**系统漏洞**和**应用漏洞**，导出所有漏洞列表，在列表中查看影响本地镜像的漏洞即可。一般情况下，镜像扫描的漏洞数据较多，全部修复工作量较大，建议区分优先级依次修复，例如：按应急漏洞，按具有 EXP、POC、远程利用、在野利用等标签等。

按应急漏洞

建议优先修复应急漏洞。对所有应急漏洞进行扫描之后，扫描完成单击导出图标，在列表中查看影响本地镜像的漏洞，对存在应急漏洞的本地镜像进行修复。



按具有 EXP、POC、远程利用、在野利用等标签

应急漏洞修复完成后，客户可优先挑选具有 EXP、POC、远程利用、在野利用等标签的系统漏洞和应用漏洞进行修复。对风险标签进行筛选，单击导出图标，选择**仅导出筛选结果**，在列表中查看影响本地镜像的漏洞，对存在这些标签的本地镜像进行修复。

除了上述标签，客户在筛选本地镜像漏洞时，如只需查看运行容器的本地镜像漏洞时，可打开“仅展示影响容器的漏洞”开关，或在导出的漏洞列表中筛选关联容器大于0的镜像。同时也可以利用“威胁等级”、“CVSS”评分等条件进行综合筛选。

常见问题-新
常见问题

最近更新时间: 2024-08-23 15:08:00

如何防护容器安全？

容器安全服务能通过对镜像及镜像仓库提供一键检测，支持对漏洞、木马病毒及敏感信息等多维度安全扫描，帮助用户解决防护镜像安全。同时容器安全提供容器逃逸、进程黑白名单、文件访问控制等安全功能，保护容器运行时安全，并提供安全运营日志，帮助企业实现容器安全可视化。

如何监控容器的健康状况？

通过容器安全服务的安全运营功能，可帮助企业实现容器安全可视化，并提供安全策略等功能，提高企业安全运营质量及效率。

容器安全服务和其他安全产品是否冲突？

不冲突，传统的主机安全产品仅仅对 OS（操作系统） 一层有效，无法深入识别容器内的安全问题。传统防火墙主要是为了南北向业务模型所设计，无法细粒度管理到容器环境如此海量和复杂的业务。

容器安全服务的漏洞库多久更新一次？

容器安全服务的漏洞库，每天更新一次，容器安全服务会实时获取官方发布的漏洞信息，会在每天固定时刻将漏洞更新至漏洞库中。

容器安全服务支持线下及跨平台部署吗？

支持。详情请参见操作指南-混合云安装指引。

镜像与容器之间有什么关系？

- 镜像是一个包含程序运行必要依赖的环境和代码的只读文件，镜像是容器运行的基础。容器在启动或者创建时，依赖于镜像。不同的镜像可以构造出不同的容器，同一个镜像，我们也可以通过配置不同参数来构造出不同的容器。
- 容器是用镜像创建的运行实例。每个容器都可以被启动、开始、停止及删除，同时容器之间相互隔离，保证应用运行期间的安全。

API文档
容器安全服务（tcss）
版本（2020-11-01）
API概览

最近更新时间: 2024-09-03 18:49:46

API版本

V3

告警设置相关接口

接口名称	接口功能
AddEditWarningRules	添加编辑告警策略
DescribeWarningRules	获取告警策略列表

安全合规相关接口

接口名称	接口功能
AddComplianceAssetPolicySetToWhitelist	安全合规忽略资产+检测项列表
AddCompliancePolicyAssetSetToWhitelist	安全合规忽略检测项+资产列表
AddCompliancePolicyItemToWhitelist	安全合规忽略检测项列表
CreateComplianceTask	安全合规创建合规检查任务
CreateExportComplianceStatusListJob	创建一个导出安全合规信息的任务
DeleteComplianceAssetPolicySetFromWhitelist	删除安全合规忽略项， 资产+检测项列表
DeleteCompliancePolicyAssetSetFromWhitelist	删除检测项+资产列表的白名单策略
DeleteCompliancePolicyItemFromWhitelist	安全合规取消忽略检测项列表
DescribeComplianceAssetDetailInfo	安全合规查询某个资产的详情
DescribeComplianceAssetList	安全合规查询某类资产的列表
DescribeComplianceAssetPolicyItemList	安全合规查询某资产下的检测项列表
DescribeCompliancePeriodTaskList	安全合规查询定时任务列表
DescribeCompliancePolicyItemAffectedAssetList	安全合规查询检测项影响的资产列表
DescribeCompliancePolicyItemAffectedSummary	安全合规查询某检测项影响的信息
DescribeComplianceScanFailedAssetList	安全合规查询上次检测失败的资产的列表

接口名称	接口功能
DescribeComplianceTaskAssetSummary	安全合规查询上次任务的资产通过率汇总信息
DescribeComplianceTaskPolicyItemSummaryList	安全合规查询上次任务的检测项的汇总信息列表
DescribeComplianceWhitelistItemList	安全合规查询白名单列表
InitializeUserComplianceEnvironment	安全合规初始化用户的合规基线检测环境
ModifyCompliancePeriodTask	安全合规编辑定时任务
ScanComplianceAssets	安全合规重新检测选定的资产
ScanComplianceAssetsByPolicyItem	安全合规用指定的检测项重新检测选定的资产
ScanCompliancePolicyItems	安全合规重新检测选定的检测项
ScanComplianceScanFailedAssets	安全合规重新检测上次检测失败的资产

安全运营-日志分析 相关接口

接口名称	接口功能
CreateSearchTemplate	添加检索模板
DeleteSearchTemplate	删除检索模板
DescribeESAggregations	获取ES字段聚合结果
DescribeESHits	获取ES查询文档列表
DescribeIndexList	获取索引列表
DescribeLogStorageStatistic	获取日志检索容量使用统计
DescribePublicKey	获取公钥
DescribeSearchExportList	导出ES查询文档列表
DescribeSearchLogs	获取历史搜索记录
DescribeSearchTemplates	获取快速检索列表
DescribeSecLogAlertMsg	查询安全日志告警信息
DescribeSecLogCleanSettingInfo	查询安全日志清理设置详情
DescribeSecLogDeliveryClsOptions	查询安全日志投递cls可选项
DescribeSecLogDeliveryClsSetting	查询安全日志投递Cls配置
DescribeSecLogDeliveryKafkaOptions	查询安全日志投递kafka可选项
DescribeSecLogDeliveryKafkaSetting	查询安全日志投递kafka配置
DescribeSecLogJoinObjectList	查询安全日志接入对象列表
DescribeSecLogJoinTypeList	查询安全日志接入列表
DescribeSecLogKafkaUIN	查询安全日志KafkaUIN

接口名称	接口功能
ModifySecLogCleanSettingInfo	修改安全日志清理设置信息
ModifySecLogDeliveryClsSetting	更新安全日志-日志投递cls配置
ModifySecLogDeliveryKafkaSetting	更新安全日志投递kafka设置
ModifySecLogJoinObjects	修改安全日志接入对象
ModifySecLogJoinState	修改安全日志接入状态
ModifySecLogKafkaUIN	修改安全日志kafkaUIN
ResetSecLogTopicConfig	重置安全日志主题设置

网络安全相关接口

接口名称	接口功能
AddAndPublishNetworkFirewallPolicyDetail	容器网络创建网络策略添加并发布任务
AddAndPublishNetworkFirewallPolicyYamlDetail	容器网络创建Yaml网络策略并发布任务
AddNetworkFirewallPolicyDetail	容器网络创建网络策略添加任务
AddNetworkFirewallPolicyYamlDetail	容器网络创建Yaml网络策略添加任务
CheckNetworkFirewallPolicyYaml	容器网络创建检查Yaml网络策略任务
ConfirmNetworkFirewallPolicy	容器网络创建网络策略确认任务
CreateNetworkFirewallClusterRefresh	容器网络集群下发刷新任务
CreateNetworkFirewallPolicyDiscover	容器网络集群网络策略创建自动发现任务
CreateNetworkFirewallPublish	容器网络创建网络策略发布任务
CreateNetworkFirewallUndoPublish	容器网络创建网络策略撤销任务
DeleteNetworkFirewallPolicyDetail	容器网络创建网络策略删除任务
DescribeNetworkFirewallAuditRecord	查询集群策略审计列表
DescribeNetworkFirewallClusterList	查询集群策略列表
DescribeNetworkFirewallClusterRefreshStatus	容器网络查询资产任务进度
DescribeNetworkFirewallNamespaceLabelList	查询集群网络空间标签列表
DescribeNetworkFirewallNamespaceList	查询集群网络空间列表
DescribeNetworkFirewallPodLabelsList	查询集群网络pod标签
DescribeNetworkFirewallPolicyDetail	容器网络集群查看策略详情
DescribeNetworkFirewallPolicyDiscover	容器网络查询网络策略自动发现任务进度
DescribeNetworkFirewallPolicyList	查询集群网络策略列表
DescribeNetworkFirewallPolicyStatus	容器网络查询网络策略策略执行状态

接口名称	接口功能
DescribeNetworkFirewallPolicyYamlDetail	容器网络集群查看Yaml网络策略详情
UpdateAndPublishNetworkFirewallPolicyDetail	容器网络创建网络策略更新并发布任务
UpdateAndPublishNetworkFirewallPolicyYamlDetail	容器网络更新Yaml网络策略并发布任务
UpdateNetworkFirewallPolicyDetail	容器网络创建网络策略更新任务
UpdateNetworkFirewallPolicyYamlDetail	容器网络更新Yaml网络策略任务

计费相关接口

接口名称	接口功能
DescribeImageAuthorizedInfo	查询镜像授权信息
DescribeProVersionInfo	查询专业版需购买信息
DescribePurchaseStateInfo	查询容器安全服务已购买信息
DescribeSecLogVasInfo	查询安全日志商品信息

资产管理相关接口

接口名称	接口功能
CreateAssetImageScanSetting	添加容器安全镜像扫描设置
CreateAssetImageVirusExportJob	创建本地镜像木马列表导出任务
CreateHostExportJob	创建主机列表导出任务
DeleteMachine	卸载Agent客户端
DescribeABTestConfig	获取用户当前灰度配置
DescribeAgentDaemonSetCmd	查询平行容器安装命令
DescribeAgentInstallCommand	查询agent安装命令
DescribeAssetSyncLastTime	查询资产同步最近时间
DescribeExportJobDownloadURL	查询导出任务下载URL
DescribeExportJobManageList	查询导出任务管理列表
DescribeInspectionReport	查询检查报告
DescribePromotionActivity	查询促销活动
DescribeTcssSummary	查询容器安全概览信息
DescribeUnauthorizedCoresTendency	查询当天未授权核数趋势
ModifyContainerNetStatus	隔离容器网络状态

运行时安全-反弹Shell相关接口

接口名称	接口功能
AddEditReverseShellWhiteList	添加编辑反弹shell白名单
DeleteReverseShellEvents	删除运行时反弹shell事件
DeleteReverseShellWhiteLists	删除运行时反弹shell白名单
DescribeReverseShellDetail	运行时反弹shell事件详细信息
DescribeReverseShellEvents	运行时反弹shell列表
DescribeReverseShellEventsExport	运行时反弹shell列表导出
DescribeReverseShellWhiteListDetail	运行时反弹shell白名单详细信息
DescribeReverseShellWhiteLists	运行时反弹shell白名单列表
ModifyReverseShellStatus	修改反弹shell事件状态

运行时安全-容器逃逸相关接口

接口名称	接口功能
AddEscapeWhiteList	新增逃逸白名单
CreateEscapeEventsExportJob	创建逃逸事件导出异步任务
CreateEscapeWhiteListExportJob	创建逃逸白名单导出任务
DeleteEscapeWhiteList	删除逃逸白名单
DescribeEscapeEventDetail	查询容器逃逸事件详情
DescribeEscapeEventInfo	查询容器逃逸事件列表
DescribeEscapeEventTendency	查询待处理逃逸事件趋势
DescribeEscapeEventTypeSummary	统计容器逃逸各事件类型和待处理事件数
DescribeEscapeEventsExport	查询容器逃逸事件列表导出
DescribeEscapeRuleInfo	查询容器逃逸扫描规则信息
DescribeEscapeSafeState	查询容器逃逸安全状态
DescribeEscapeWhiteList	查询逃逸白名单
ModifyEscapeEventStatus	修改容器逃逸扫描事件状态
ModifyEscapeRule	修改容器逃逸扫描规则信息
ModifyEscapeWhiteList	修改逃逸白名单

运行时安全-木马调用相关接口

接口名称	接口功能

接口名称	接口功能
CreateVirusScanAgain	运行时文件查杀重新检测
CreateVirusScanTask	运行时文件查杀一键扫描
DescribeExportJobResult	查询导出任务的结果
DescribeVirusAutoIsolateSampleDetail	查询木马自动隔离样本详情
DescribeVirusAutoIsolateSampleDownloadURL	查询木马自动隔离样本下载链接
DescribeVirusAutoIsolateSampleList	查询木马自动隔离样本列表
DescribeVirusAutoIsolateSetting	查询木马自动隔离设置
DescribeVirusDetail	运行时查询木马文件信息
DescribeVirusEventTendency	查询木马事件趋势
DescribeVirusList	查询运行时文件查杀事件列表
DescribeVirusManualScanEstimateTimeout	查询木马一键检测预估超时时间
DescribeVirusMonitorSetting	运行时查询文件查杀实时监控设置
DescribeVirusSampleDownloadUrl	查询木马样本下载url
DescribeVirusScanSetting	运行时查询文件查杀设置
DescribeVirusScanTaskStatus	运行时查询文件查杀任务状态
DescribeVirusScanTimeoutSetting	运行时文件扫描超时设置查询
DescribeVirusSummary	运行时查询木马概览信息
DescribeVirusTaskList	运行时查询文件查杀任务列表
ExportVirusList	运行时文件查杀事件列表导出
ModifyVirusAutoIsolateExampleSwitch	修改木马自动隔离样本开关
ModifyVirusAutoIsolateSetting	修改木马自动隔离设置
ModifyVirusFileStatus	运行时更新木马文件事件状态
ModifyVirusMonitorSetting	运行时更新文件查杀实时监控设置
ModifyVirusScanSetting	运行时更新文件查杀设置
ModifyVirusScanTimeoutSetting	运行时文件扫描超时设置
StopVirusScanTask	运行时停止木马查杀任务

运行时安全-高危系统调用相关接口

接口名称	接口功能
CreateAbnormalProcessRulesExportJob	创建异常进程规则导出任务
DeleteRiskSyscallEvents	删除运行时高危系统调用事件

接口名称	接口功能
DeleteRiskSyscallWhiteLists	删除运行时高危系统调用白名单
DescribeRiskSyscallEvents	运行时高危系统调用列表
DescribeRiskSyscallEventsExport	运行时高危系统调用列表导出
DescribeRiskSyscallNames	运行时高危系统调用系统名称列表
DescribeRiskSyscallWhiteListDetail	运行时高危系统调用白名单详细信息
DescribeRiskSyscallWhiteLists	运行时高危系统调用白名单列表
ModifyRiskSyscallStatus	修改高危系统调用事件状态

运行时安全相关接口

接口名称	接口功能
AddEditAbnormalProcessRule	添加编辑异常进程策略
AddEditAccessControlRule	添加编辑运行访问控制策略
AddEditRiskSyscallWhiteList	添加编辑高危系统调用白名单
CreateDefenceVulExportJob	创建支持防御的漏洞导出任务
CreateEmergencyVulExportJob	创建应急漏洞导出任务
CreateProcessEventsExportJob	创建异常进程事件导出异步任务
CreateRiskDnsEventExportJob	创建恶意请求事件导出任务
CreateSystemVulExportJob	创建系统漏洞导出任务
CreateVulContainerExportJob	创建受漏洞影响的容器导出任务
CreateVulImageExportJob	创建导出受漏洞影响的镜像任务
CreateVulScanTask	创建漏洞扫描任务
CreateWebVulExportJob	创建web漏洞导出任务
DeleteAbnormalProcessRules	删除运行时异常进程策略
DeleteAccessControlRules	删除运行时访问控制策略
DescribeAbnormalProcessDetail	运行时异常进程事件详细信息
DescribeAbnormalProcessEventTendency	查询待处理异常进程事件趋势
DescribeAbnormalProcessEvents	运行时异常进程列表
DescribeAbnormalProcessEventsExport	运行时异常进程列表导出
DescribeAbnormalProcessLevelSummary	统计异常进程各威胁等级待处理事件数
DescribeAbnormalProcessRuleDetail	查询运行时异常进程策略详细信息
DescribeAbnormalProcessRules	运行时异常进程策略列表

接口名称	接口功能
DescribeAbnormalProcessRulesExport	运行时异常进程策略列表导出
DescribeAccessControlDetail	运行时访问控制事件详细信息
DescribeAccessControlEvents	运行时访问控制事件列表
DescribeAccessControlEventsExport	运行时访问控制事件列表导出
DescribeAccessControlRuleDetail	查询运行时访问控制策略详细信息
DescribeAccessControlRules	运行时访问控制策略列表
DescribeAccessControlRulesExport	运行时访问控制策略列表导出
DescribeAssetImageBindRuleInfo	镜像绑定规则列表
DescribeEmergencyVulList	查询应急漏洞列表
DescribeRiskDnsEventDetail	查询恶意请求事件详情
DescribeRiskDnsList	查询恶意请求事件列表
DescribeRiskSyscallDetail	运行时高危系统调用事件详细信息
DescribeSupportDefenceVul	查询支持防御的漏洞列表
DescribeVulContainerList	查询受漏洞的容器列表
DescribeVulDetail	查询漏洞详情
DescribeVulImageList	查询漏洞影响的镜像列表
DescribeVulScanInfo	查询漏洞扫描任务信息
DescribeVulScanLocalImageList	查询漏洞扫描任务的本地镜像列表
DescribeWebVulList	查询web应用漏洞列表
ModifyAbnormalProcessRuleStatus	修改运行时异常进程策略状态
ModifyAbnormalProcessStatus	修改异常进程事件状态
ModifyAccessControlRuleStatus	修改运行时访问控制策略状态
ModifyAccessControlStatus	修改运行时访问控制事件状态
OpenTcssTrial	开通容器安全服务试用
StopVulScanTask	停止漏洞扫描任务

镜像安全相关接口

接口名称	接口功能
AddAssetImageRegistryRegistryDetail	新增单个镜像仓库详细信息
AddEditImageAutoAuthorizedRule	新增或编辑本地镜像自动授权规则
AddIgnoreVul	新增漏洞扫描忽略漏洞

接口名称	接口功能
CheckRepeatAssetImageRegistry	检查单个镜像仓库名是否重复
CreateAssetImageRegistryScanTask	镜像仓库创建镜像扫描任务
CreateAssetImageRegistryScanTaskOneKey	镜像仓库创建镜像一键扫描任务
CreateAssetImageScanTask	创建镜像扫描任务
CreateComponentExportJob	查询本地镜像组件列表导出
CreateImageExportJob	创建镜像导出任务
CreateOrModifyPostPayCores	创建或者编辑弹性计费上限
CreateVulDefenceEventExportJob	创建漏洞防御导出任务
CreateVulDefenceHostExportJob	创建漏洞防御主机导出任务
CreateVulExportJob	查询本地镜像漏洞列表导出
DeleteIgnoreVul	取消漏洞扫描忽略漏洞
DescribeAssetAppServiceList	查询app服务列表
DescribeAssetComponentList	查询容器组件列表
DescribeAssetContainerDetail	查询容器信息
DescribeAssetContainerList	查询容器列表
DescribeAssetDBServiceList	查询db服务列表
DescribeAssetHostDetail	查询主机信息
DescribeAssetHostList	查询主机列表
DescribeAssetImageDetail	查询镜像信息
DescribeAssetImageHostList	查询镜像关联主机
DescribeAssetImageList	查询镜像列表
DescribeAssetImageListExport	查询镜像列表导出
DescribeAssetImageRegistryAssetStatus	查看镜像仓库资产更新进度状态
DescribeAssetImageRegistryDetail	镜像仓库查询镜像仓库详情
DescribeAssetImageRegistryList	镜像仓库查询镜像仓库列表
DescribeAssetImageRegistryListExport	镜像仓库镜像列表导出
DescribeAssetImageRegistryRegistryDetail	查看单个镜像仓库详细信息
DescribeAssetImageRegistryRegistryList	镜像仓库仓库列表
DescribeAssetImageRegistryRiskInfoList	镜像仓库查询镜像高危行为列表
DescribeAssetImageRegistryRiskListExport	镜像仓库敏感信息列表导出
DescribeAssetImageRegistryScanStatusOneKey	镜像仓库查询一键镜像扫描状态
DescribeAssetImageRegistrySummary	镜像仓库查询镜像统计信息

接口名称	接口功能
DescribeAssetImageRegistryVirusList	镜像仓库查询木马病毒列表
DescribeAssetImageRegistryVirusListExport	镜像仓库木马信息列表导出
DescribeAssetImageRegistryVulList	镜像仓库查询镜像漏洞列表
DescribeAssetImageRegistryVulListExport	镜像仓库漏洞列表导出
DescribeAssetImageRiskList	查询镜像风险列表
DescribeAssetImageRiskListExport	镜像风险列表导出
DescribeAssetImageScanSetting	获取镜像扫描设置信息
DescribeAssetImageScanStatus	查询镜像扫描状态
DescribeAssetImageScanTask	查询正在一键扫描的镜像扫描taskid
DescribeAssetImageSimpleList	查询镜像简略信息列表
DescribeAssetImageVirusList	查询镜像病毒列表
DescribeAssetImageVirusListExport	镜像木马列表导出
DescribeAssetImageVulList	查询镜像漏洞列表
DescribeAssetImageVulListExport	镜像漏洞列表导出
DescribeAssetPortList	查询端口占用列表
DescribeAssetProcessList	查询进程列表
DescribeAssetSummary	查询账户容器、镜像等统计信息
DescribeAssetWebServiceList	查询web服务列表
DescribeAutoAuthorizedRuleHost	查询自动授权规则授权范围主机信息
DescribeContainerAssetSummary	查询容器安全资产概览
DescribeContainerSecEventSummary	查询容器安全未处理事件概览
DescribeImageAutoAuthorizedLogList	查询镜像自动授权结果列表
DescribeImageAutoAuthorizedRule	查询本地镜像自动授权规则
DescribeImageAutoAuthorizedTaskList	查询镜像自动授权任务列表
DescribeImageComponentList	查询本地镜像组件列表
DescribeImageRegistryNamespaceList	查询用户镜像仓库下的命令空间列表
DescribeImageRegistryTimingScanTask	镜像仓库查看定时任务
DescribeImageRiskSummary	查询本地镜像风险概览
DescribeImageRiskTendency	查询容器安全本地镜像风险趋势
DescribeImageSimpleList	查询全部镜像列表
DescribeNewestVul	查询最新披露漏洞列表
DescribePostPayDetail	查询后付费详情

接口名称	接口功能
DescribeScanIgnoreVulList	查询扫描忽略的漏洞列表
DescribeSecEventsTendency	查询容器运行时安全时间趋势
DescribeSystemVulList	查询系统漏洞列表
DescribeValueAddedSrvInfo	查询增值服务需购买信息
DescribeVulDefenceEvent	查询漏洞防御事件列表
DescribeVulDefenceEventDetail	查询漏洞防御事件详情
DescribeVulDefenceEventTendency	查询漏洞防御攻击事件趋势
DescribeVulDefenceHost	查询漏洞防御的主机列表
DescribeVulDefencePlugin	查询漏洞防御插件列表
DescribeVulDefenceSetting	查询漏洞防御设置信息
DescribeVulIgnoreLocalImageList	查询漏洞扫描忽略的本地镜像列表
DescribeVulIgnoreRegistryImageList	查询漏洞扫描忽略的仓库镜像列表
DescribeVulImageSummary	查询漏洞镜像统计
DescribeVulLevelImageSummary	查询应急漏洞各威胁等级统计镜像数
DescribeVulLevelSummary	查询漏洞各威胁等级统计数
DescribeVulRegistryImageList	查询漏洞影响的仓库镜像列表
DescribeVulScanAuthorizedImageSummary	统计漏洞扫描页已授权和未扫描镜像数
DescribeVulSummary	查询漏洞风险统计概览
DescribeVulTendency	查询漏洞风险趋势
DescribeVulTopRanking	查询漏洞Top排名列表
ModifyAsset	主机资产刷新
ModifyAssetImageRegistryScanStop	镜像仓库停止镜像扫描任务
ModifyAssetImageRegistryScanStopOneKey	镜像仓库停止镜像一键扫描任务
ModifyAssetImageScanStop	停止镜像扫描
ModifyImageAuthorized	批量授权镜像扫描V2.0
ModifyVulDefenceEventStatus	修改漏洞防御事件状态
ModifyVulDefenceSetting	编辑漏洞防御设置
RemoveAssetImageRegistryRegistryDetail	删除单个镜像仓库详细信息
RenewImageAuthorizeState	授权镜像扫描
SwitchImageAutoAuthorizedRule	编辑本地镜像自动授权开关
SyncAssetImageRegistryAsset	镜像仓库资产刷新
UpdateAssetImageRegistryRegistryDetail	更新单个镜像仓库详细信息

接口名称	接口功能
UpdateImageRegistryTimingScanTask	镜像仓库更新定时任务

集群安全相关接口

接口名称	接口功能
CreateCheckComponent	安装检查组件
CreateClusterCheckTask	创建集群检查任务
CreateRefreshTask	下发刷新任务
DescribeAffectedClusterCount	获取受影响的集群数量
DescribeAffectedNodeList	查询节点类型的影响范围
DescribeAffectedWorkloadList	查询workload类型的影响范围
DescribeCheckItemList	查询所有检查项接口
DescribeClusterDetail	查询单个集群的详细信息
DescribeClusterSummary	查询用户集群资产总览
DescribeRefreshTask	查询刷新任务
DescribeRiskList	查询集群风险项列表
DescribeTaskResultSummary	查询检查结果总览
DescribeUnfinishRefreshTask	查询未完成的刷新资产任务信息
DescribeUserCluster	用户集群资产查询
SetCheckMode	设置检测模式和自动检查

高级防御-k8sApi异常请求相关接口

接口名称	接口功能
CreateAccessControlsRuleExportJob	创建文件篡改规则导出任务
CreateK8sApiAbnormalEventExportJob	创建k8s api异常事件导出任务
CreateK8sApiAbnormalRuleExportJob	创建k8sApi异常规则导出任务
CreateK8sApiAbnormalRuleInfo	创建k8sapi异常事件规则
DeleteK8sApiAbnormalRule	删除k8sapi异常事件规则
DescribeAssetClusterList	查询集群列表
DescribeK8sApiAbnormalEventInfo	查询k8s api 异常事件详情
DescribeK8sApiAbnormalEventList	查询k8s api异常事件列表
DescribeK8sApiAbnormalRuleInfo	查询k8sapi异常请求规则详情

接口名称	接口功能
DescribeK8sApiAbnormalRuleList	查询k8sapi异常请求规则列表
DescribeK8sApiAbnormalRuleScopeList	查询k8sapi 异常规则中范围列表
DescribeK8sApiAbnormalSummary	查询k8sapi异常事件统计
DescribeK8sApiAbnormalTendency	查询k8sapi异常事件趋势
ModifyK8sApiAbnormalEventStatus	修改k8sapi异常事件状态
ModifyK8sApiAbnormalRuleInfo	修改k8sapi异常规则信息
ModifyK8sApiAbnormalRuleStatus	修改k8sapi异常事件规则状态

调用方式
接口签名v1

最近更新时间: 2024-09-03 18:49:46

tcecloud API 会对每个访问请求进行身份验证，即每个请求都需要在公共请求参数中包含签名信息（Signature）以验证请求者身份。 签名信息由安全凭证生成，安全凭证包括 SecretId 和 SecretKey；若用户还没有安全凭证，请前往云API密钥页面申请，否则无法调用云API接口。

1. 申请安全凭证

在第一次使用云API之前，请前往云API密钥页面申请安全凭证。 安全凭证包括 SecretId 和 SecretKey：

- SecretId 用于标识 API 调用者身份
- SecretKey 用于加密签名字符串和服务器端验证签名字符串的密钥。
- 用户必须严格保管安全凭证，避免泄露。

申请安全凭证的具体步骤如下：

1. 登录tcecloud管理中心控制台。
2. 前往云API密钥的控制台页面
3. 在云API密钥页面，点击【新建】即可以创建一对SecretId/SecretKey

注意：开发商帐号最多可以拥有两对 SecretId / SecretKey。

2. 生成签名串

有了安全凭证SecretId 和 SecretKey后，就可以生成签名串了。以下是生成签名串的详细过程：

假设用户的 SecretId 和 SecretKey 分别是：

- SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
- SecretKey: Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

注意：这里只是示例，请根据用户实际申请的 SecretId 和 SecretKey 进行后续操作！

以云服务器查看实例列表(DescribeInstances)请求为例，当用户调用这一接口时，其请求参数可能如下:

参数名称	中文	参数值
Action	方法名	DescribeInstances
SecretId	密钥Id	AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
Timestamp	当前时间戳	1465185768
Nonce	随机正整数	11886
Region	实例所在区域	ap-guangzhou
InstanceIds.0	待查询的实例ID	ins-09dx96dg
Offset	偏移量	0
Limit	最大允许输出	20
Version	接口版本号	2017-03-12

2.1. 对参数排序

首先对所有请求参数按参数名的字典序（ ASCII 码）升序排序。注意：1）只按参数名进行排序，参数值保持对应即可，不参与比大小；2）按 ASCII 码比大小，如 InstanceIds.2 要排在 InstanceIds.12 后面，不是按字母表，也不是按数值。用户可以借助编程语言中的相关排序函数来实现这一功能，如 php 中的 ksort 函数。上述示例参数的排序结果如下:

```
{
'Action' : 'DescribeInstances',
'InstanceIds.0' : 'ins-09dx96dg',
'Limit' : 20,
'Nonce' : 11886,
'Offset' : 0,
'Region' : 'ap-guangzhou',
'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE',
'Timestamp' : 1465185768,
'Version': '2017-03-12',
}
```

使用其它程序设计语言开发时，可对上面示例中的参数进行排序，得到的结果一致即可。

2.2. 拼接请求字符串

此步骤生成请求字符串。 将把上一步排序好的请求参数格式化成“参数名称”=“参数值”的形式，如对 Action 参数，其参数名称为 "Action" ，参数值为 "DescribeInstances" ，因此格式化后就为 Action=DescribeInstances 。 **注意：“参数值”为原始值而非url编码后的值。**

然后将格式化后的各个参数用"&"拼接在一起，最终生成的请求字符串为:

```
Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.3. 拼接签名原文字符串

此步骤生成签名原文字符串。 签名原文字符串由以下几个参数构成:

1. 请求方法: 支持 POST 和 GET 方式，这里使用 GET 请求，注意方法为全大写。
2. 请求主机:查看实例列表(DescribeInstances)的请求域名为：cvm.cloud.sunhongs.com。实际的请求域名根据接口所属模块的不同而不同，详见各接口说明。
3. 请求路径: 当前版本云API的请求路径固定为 / 。
4. 请求字符串: 即上一步生成的请求字符串。

签名原文串的拼接规则为: 请求方法 + 请求主机 +请求路径 + ? + 请求字符串

示例的拼接结果为：

```
GETcvm.cloud.sunhongs.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.4. 生成签名串

此步骤生成签名串。 首先使用 HMAC-SHA1 算法对上一步中获得的**签名原文字符串**进行签名，然后将生成的签名串使用 Base64 进行编码，即可获得最终的签名串。

具体代码如下，以 PHP 语言为例:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3EXAMPLE';
$srcStr = 'GETcvm.cloud.sunhongs.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

最终得到的签名串为:

```
EliP9YW3pW28FpsEdkXt/+WcGeI=
```

使用其它程序设计语言开发时，可用上面示例中的原文进行签名验证，得到的签名串与例子中的一致即可。

3. 签名串编码

生成的签名串并不能直接作为请求参数，需要对其进行 URL 编码。

如上一步生成的签名串为 EliP9YW3pW28FpsEdkXt/+WcGeI= ，最终得到的签名串请求参数（Signature）为：EliP9YW3pW28FpsEdkXt%2f%2bWcGeI%3d，它将用于生成最终的请求 URL。

注意：如果用户的请求方法是 GET，或者请求方法为 POST 同时 Content-Type 为 application/x-www-form-urlencoded，则发送请求时所有请求参数的值均需要做 URL 编码，参数键和=符号不需要编码。非 ASCII 字符在 URL 编码前需要先以 UTF-8 进行编码。

注意：有些编程语言的 http 库会自动为所有参数进行 urlencode，在这种情况下，就不需要对签名串进行 URL 编码了，否则两次 URL 编码会导致签名失败。

注意：其他参数值也需要进行编码，编码采用 RFC 3986。使用 %XY 对特殊字符例如汉字进行百分比编码，其中“X”和“Y”为十六进制字符（0-9 和大写字母 A-F），使用小写将引发错误。

4. 签名失败

根据实际情况，存在以下签名失败的错误码，请根据实际情况处理

错误代码	错误描述
AuthFailure.SignatureExpire	签名过期
AuthFailure.SecretIdNotFound	密钥不存在
AuthFailure.SignatureFailure	签名错误
AuthFailure.TokenFailure	token 错误
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）

5. 签名演示

在实际调用 API 3.0 时，推荐使用配套的tcecloud SDK 3.0 ，SDK 封装了签名的过程，开发时只关注产品提供的具体接口即可。详细信息参见 SDK 中心。当前支持的编程语言有：

- Python
- Java
- PHP
- Go
- JavaScript
- .NET

为了更清楚的解释签名过程，下面以实际编程语言为例，将上述的签名过程具体实现。请求的域名、调用的接口和参数的取值都以上述签名过程为准，代码只为解释签名过程，并不具备通用性，实际开发请尽量使用 SDK 。

最终输出的 url 可能为： https://cvm.cloud.sunhongs.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-

guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Signature=EliP9YW3pW28FpsEdkXt%2F%2BWcGeI%3D&Timestamp=1465185768&Version=2017-03-12

注意：由于示例中的密钥是虚构的，时间戳也不是系统当前时间，因此如果将此 url 在浏览器中打开或者用 curl 等命令调用时会返回鉴权错误：签名过期。为了得到一个可以正常返回的 url ，需要修改示例中的 SecretId 和 SecretKey 为真实的密钥，并使用系统当前时间戳作为 Timestamp 。

注意：在下面的示例中，不同编程语言，甚至同一语言每次执行得到的 url 可能都有所不同，表现为参数的顺序不同，但这并不影响正确性。只要所有参数都在，且签名计算正确即可。

注意：以下代码仅适用于 API 3.0，不能直接用于其他的签名流程，即使是旧版的 API ，由于存在细节差异也会导致签名计算错误，请以对应的实际文档为准。

Java

```
import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
import java.util.Random;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class TceCloudAPIDemo {
private final static String CHARSET = "UTF-8";

public static String sign(String s, String key, String method) throws Exception {
Mac mac = Mac.getInstance(method);
SecretKeySpec secretKeySpec = new SecretKeySpec(key.getBytes(CHARSET), mac.getAlgorithm());
mac.init(secretKeySpec);
byte[] hash = mac.doFinal(s.getBytes(CHARSET));
return DatatypeConverter.printBase64Binary(hash);
}

public static String getStringToSign(TreeMap<String, Object> params) {
StringBuilder s2s = new StringBuilder("GETcvm.cloud.sunhongs.com/?");
// 签名时要求对参数进行字典排序，此处用TreeMap保证顺序
for (String k : params.keySet()) {
s2s.append(k).append("=").append(params.get(k).toString()).append("&");
}
return s2s.toString().substring(0, s2s.length() - 1);
}

public static String getUrl(TreeMap<String, Object> params) throws UnsupportedEncodingException {
StringBuilder url = new StringBuilder("https://cvm.cloud.sunhongs.com/?");
// 实际请求的url中对参数顺序没有要求
for (String k : params.keySet()) {
// 需要对请求串进行urlencode，由于key都是英文字母，故此处仅对其value进行urlencode
url.append(k).append("=").append(URLEncoder.encode(params.get(k).toString(), CHARSET)).append("&");
}
return url.toString().substring(0, url.length() - 1);
}

public static void main(String[] args) throws Exception {
TreeMap<String, Object> params = new TreeMap<String, Object>(); // TreeMap可以自动排序
// 实际调用时应当使用随机数，例如：params.put("Nonce", new Random().nextInt(java.lang.Integer.MAX_VALUE));
params.put("Nonce", 11886); // 公共参数
// 实际调用时应当使用系统当前时间，例如： params.put("Timestamp", System.currentTimeMillis() / 1000);
params.put("Timestamp", 1465185768); // 公共参数
params.put("SecretId", "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"); // 公共参数
params.put("Action", "DescribeInstances"); // 公共参数
params.put("Version", "2017-03-12"); // 公共参数
params.put("Region", "ap-guangzhou"); // 公共参数
```

```
params.put("Limit", 20); // 业务参数
params.put("Offset", 0); // 业务参数
params.put("InstanceIds.0", "ins-09dx96dg"); // 业务参数
params.put("Signature", sign(getStringToSign(params), "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE", "HmacSHA1")); // 公共参数
System.out.println(getUrl(params));
}
}
```

Python

注意：如果是在 Python 2 环境中运行，需要先安装 requests 依赖包： `pip install requests` 。

```
# -*- coding: utf8 -*-
import base64
import hashlib
import hmac
import time

import requests

secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

def get_string_to_sign(method, endpoint, params):
s = method + endpoint + "/?"
query_str = "&".join("%s=%s" % (k, params[k]) for k in sorted(params))
return s + query_str

def sign_str(key, s, method):
hmac_str = hmac.new(key.encode("utf8"), s.encode("utf8"), method).digest()
return base64.b64encode(hmac_str)

if __name__ == '__main__':
endpoint = "cvm.cloud.sunhongs.com"
data = {
'Action' : 'DescribeInstances',
'InstanceIds.0' : 'ins-09dx96dg',
'Limit' : 20,
'Nonce' : 11886,
'Offset' : 0,
'Region' : 'ap-guangzhou',
'SecretId' : secret_id,
'Timestamp' : 1465185768, # int(time.time())
'Version': '2017-03-12'
}
s = get_string_to_sign("GET", endpoint, data)
data["Signature"] = sign_str(secret_key, s, hashlib.sha1)
print(data["Signature"])
# 此处会实际调用，成功后可能产生计费
# resp = requests.get("https://" + endpoint, params=data)
# print(resp.url)
```

接口签名v3

最近更新时间: 2024-09-03 18:49:46

tcecloud API 会对每个访问请求进行身份验证，即每个请求都需要在公共请求参数中包含签名信息（Signature）以验证请求者身份。 签名信息由安全凭证生成，安全凭证包括 SecretId 和 SecretKey；若用户还没有安全凭证，请前往云API密钥页面申请，否则无法调用云API接口。

1. 申请安全凭证

在第一次使用云API之前，请前往云API密钥页面申请安全凭证。 安全凭证包括 SecretId 和 SecretKey：

- SecretId 用于标识 API 调用者身份
- SecretKey 用于加密签名字符串和服务器端验证签名字符串的密钥。
- 用户必须严格保管安全凭证，避免泄露。

申请安全凭证的具体步骤如下：

1. 登录tcecloud管理中心控制台。
2. 前往云API密钥的控制台页面
3. 在云API密钥页面，点击【新建】即可以创建一对SecretId/SecretKey

注意：开发商帐号最多可以拥有两对 SecretId / SecretKey。

2. TC3-HMAC-SHA256 签名方法

注意：对于GET方法，只支持 Content-Type: application/x-www-form-urlencoded 协议格式。对于POST方法，目前支持 Content-Type: application/json 以及 Content-Type: multipart/form-data 两种协议格式，json 格式默认所有业务接口均支持，multipart 格式只有特定业务接口支持，此时该接口不能使用 json 格式调用，参考具体业务接口文档说明。

下面以云服务器查询广州区实例列表作为例子，分步骤介绍签名的计算过程。我们仅用到了查询实例列表的两个参数：Limit 和 Offset，使用 GET 方法调用。

假设用户的 SecretId 和 SecretKey 分别是：AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE 和 Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

2.1. 拼接规范请求串

按如下格式拼接规范请求串（CanonicalRequest）：

```
CanonicalRequest =
HTTPRequestMethod + '\n' +
CanonicalURI + '\n' +
CanonicalQueryString + '\n' +
CanonicalHeaders + '\n' +
SignedHeaders + '\n' +
HashedRequestPayload
```

- HTTPRequestMethod：HTTP 请求方法（GET、POST ），本示例中为 GET；
- CanonicalURI：URI 参数，API 3.0 固定为正斜杠（/）；
- CanonicalQueryString：发起 HTTP 请求 URL 中的查询字符串，对于 POST 请求，固定为空字符串，对于 GET 请求，则为 URL 中问号（?）后面的字符串内容，本示例取值为：Limit=10&Offset=0。注意：CanonicalQueryString 需要经过 URL 编码。
- CanonicalHeaders：参与签名的头部信息，至少包含 host 和 content-type 两个头部，也可加入自定义的头部参与签名以提高自身请求的唯一性和安全性。拼接规则：1）头部 key 和 value 统一转成小写，并去掉首尾空格，按照 key:value\n 格式拼接；2）多个头部，按照头部 key（小写）的字典排序进行拼接。此例中为： `content-type:application/x-www-form-urlencoded\nhost:cvm.cloud.sunhongs.com\n`

- SignedHeaders：参与签名的头部信息，说明此次请求有哪些头部参与了签名，和 CanonicalHeaders 包含的头部内容是一一对应的。content-type 和 host 为必选头部。拼接规则：1）头部 key 统一转成小写；2）多个头部 key（小写）按照字典排序进行拼接，并且以分号（;）分隔。此例中为： `content-type;host`
- HashedRequestPayload：请求正文的哈希值，计算方法为 Lowercase(HexEncode(Hash.SHA256(RequestPayload)))，对 HTTP 请求整个正文 payload 做 SHA256 哈希，然后十六进制编码，最后编码串转换成小写字母。注意：对于 GET 请求，RequestPayload 固定为空字符串，对于 POST 请求，RequestPayload 即为 HTTP 请求正文 payload。

根据以上规则，示例中得到的规范请求串如下（为了展示清晰，\n 换行符通过另起打印新的一行替代）：

```
GET
/
Limit=10&Offset=0
content-type:application/x-www-form-urlencoded
host:cvm.cloud.sunhongs.com

content-type;host
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

2.2. 拼接待签名字符串

按如下格式拼接待签名字符串：

```
StringToSign =
Algorithm + \n +
RequestTimestamp + \n +
CredentialScope + \n +
HashedCanonicalRequest
```

- Algorithm：签名算法，目前固定为 TC3-HMAC-SHA256；
- RequestTimestamp：请求时间戳，即请求头部的 X-TC-Timestamp 取值，如上示例请求为 1539084154；
- CredentialScope：凭证范围，格式为 Date/service/tc3_request，包含日期、所请求的服务和终止字符串（tc3_request）。**Date 为 UTC 标准时间的日期，取值需要和公共参数 X-TC-Timestamp 换算的 UTC 标准时间日期一致**；service 为产品名，必须与调用的产品域名一致，例如 cvm。如上示例请求，取值为 2018-10-09/cvm/tc3_request；
- HashedCanonicalRequest：前述步骤拼接所得规范请求串的哈希值，计算方法为 Lowercase(HexEncode(Hash.SHA256(CanonicalRequest)))。

注意：

> 1. Date 必须从时间戳 X-TC-Timestamp 计算得到，且时区为 UTC+0。如果加入系统本地时区信息，例如东八区，将导致白天和晚上调用成功，但是凌晨时调用必定失败。假设时间戳为 1551113065，在东八区的时间是 2019-02-26 00:44:25，但是计算得到的 Date 取 UTC+0 的日期应为 2019-02-25，而不是 2019-02-26。
> 2. Timestamp 必须是当前系统时间，且需确保系统时间和标准时间是同步的，如果相差超过五分钟则必定失败。如果长时间不和标准时间同步，可能导致运行一段时间后，请求必定失败（返回签名过期错误）。

根据以上规则，示例中得到的待签名字符串如下（为了展示清晰，\n 换行符通过另起打印新的一行替代）：

```
TC3-HMAC-SHA256
1539084154
2018-10-09/cvm/tc3_request
91c9c192c14460df6c1ffc69e34e6c5e90708de2a6d282cccf957dbf1aa7f3a7
```

2.3. 计算签名

1）计算派生签名密钥，伪代码如下

```
SecretKey = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"
SecretDate = HMAC_SHA256("TC3" + SecretKey, Date)
```

```
SecretService = HMAC_SHA256(SecretDate, Service)
SecretSigning = HMAC_SHA256(SecretService, "tc3_request")
```

- SecretKey：原始的 SecretKey；
- Date：即 Credential 中的 Date 字段信息，如上示例，为2018-10-09；
- Service：即 Credential 中的 Service 字段信息，如上示例，为 cvm；

2）计算签名，伪代码如下

```
Signature = HexEncode(HMAC_SHA256(SecretSigning, StringToSign))
```

- SecretSigning：即以上计算得到的派生签名密钥；
- StringToSign：即步骤2计算得到的待签名字符串；

2.4. 拼接 Authorization

按如下格式拼接 Authorization：

```
Authorization =
Algorithm + ' ' +
'Credential=' + SecretId + '/' + CredentialScope + ', ' +
'SignedHeaders=' + SignedHeaders + ', '
'Signature=' + Signature
```

- Algorithm：签名方法，固定为 TC3-HMAC-SHA256；
- SecretId：密钥对中的 SecretId；
- CredentialScope：见上文，凭证范围；
- SignedHeaders：见上文，参与签名的头部信息；
- Signature：签名值

根据以上规则，示例中得到的值为：

```
TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f
0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
```

最终完整的调用信息如下：

```
https://cvm.cloud.sunhongs.com/?Limit=10&Offset=0

Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2018-10-09/cvm/tc3_request, SignedHea
ders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
Content-Type: application/x-www-form-urlencoded
Host: cvm.cloud.sunhongs.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: ap-guangzhou
```

3. 签名失败

根据实际情况，存在以下签名失败的错误码，请根据实际情况处理

错误代码	错误描述
AuthFailure.SignatureExpire	签名过期

错误代码	错误描述
AuthFailure.SecretIdNotFound	密钥不存在
AuthFailure.SignatureFailure	签名错误
AuthFailure.TokenFailure	token 错误
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）

4. 签名演示

Java

```
import java.io.BufferedReader;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.net.URL;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.Map;
import java.util.TimeZone;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.net.ssl.HttpsURLConnection;
import javax.xml.bind.DatatypeConverter;

import org.apache.commons.codec.digest.DigestUtils;

public class TceCloudAPITC3Demo {
private final static String CHARSET = "UTF-8";
private final static String ENDPOINT = "cvm.cloud.sunhongs.com";
private final static String PATH = "/";
private final static String SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE";
private final static String SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE";
private final static String CT_X_WWW_FORM_URLENCODED = "application/x-www-form-urlencoded";
private final static String CT_JSON = "application/json";
private final static String CT_FORM_DATA = "multipart/form-data";

public static byte[] sign256(byte[] key, String msg) throws Exception {
Mac mac = Mac.getInstance("HmacSHA256");
SecretKeySpec secretKeySpec = new SecretKeySpec(key, mac.getAlgorithm());
mac.init(secretKeySpec);
return mac.doFinal(msg.getBytes(CHARSET));
}

public static void main(String[] args) throws Exception {
String service = "cvm";
String host = "cvm.cloud.sunhongs.com";
String region = "ap-guangzhou";
String action = "DescribeInstances";
String version = "2017-03-12";
String algorithm = "TC3-HMAC-SHA256";
String timestamp = "1539084154";
//String timestamp = String.valueOf(System.currentTimeMillis() / 1000);
SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd");
// 注意时区，否则容易出错
sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
String date = sdf.format(new Date(Long.valueOf(timestamp + "000")));
```

```
// ************* 步骤 1：拼接规范请求串 *************
String httpRequestMethod = "GET";
String canonicalUri = "/";
String canonicalQueryString = "Limit=10&Offset=0";
String canonicalHeaders = "content-type:application/x-www-form-urlencoded\n" + "host:" + host + "\n";
String signedHeaders = "content-type;host";
String hashedRequestPayload = DigestUtils.sha256Hex("");
String canonicalRequest = httpRequestMethod + "\n" + canonicalUri + "\n" + canonicalQueryString + "\n"
+ canonicalHeaders + "\n" + signedHeaders + "\n" + hashedRequestPayload;
System.out.println(canonicalRequest);

// ************* 步骤 2：拼接待签名字符串 *************
String credentialScope = date + "/" + service + "/" + "tc3_request";
String hashedCanonicalRequest = DigestUtils.sha256Hex(canonicalRequest.getBytes(CHARSET));
String stringToSign = algorithm + "\n" + timestamp + "\n" + credentialScope + "\n" + hashedCanonicalRequest;
System.out.println(stringToSign);

// ************* 步骤 3：计算签名 *************
byte[] secretDate = sign256(("TC3" + SECRET_KEY).getBytes(CHARSET), date);
byte[] secretService = sign256(secretDate, service);
byte[] secretSigning = sign256(secretService, "tc3_request");
String signature = DatatypeConverter.printHexBinary(sign256(secretSigning, stringToSign)).toLowerCase();
System.out.println(signature);

// ************* 步骤 4：拼接 Authorization *************
String authorization = algorithm + " " + "Credential=" + SECRET_ID + "/" + credentialScope + ", "
+ "SignedHeaders=" + signedHeaders + ", " + "Signature=" + signature;
System.out.println(authorization);

TreeMap<String, String> headers = new TreeMap<String, String>();
headers.put("Authorization", authorization);
headers.put("Host", host);
headers.put("Content-Type", CT_X_WWW_FORM_URLENCODED);
headers.put("X-TC-Action", action);
headers.put("X-TC-Timestamp", timestamp);
headers.put("X-TC-Version", version);
headers.put("X-TC-Region", region);
}
}
```

Python

```
# -*- coding: utf-8 -*-
import hashlib, hmac, json, os, sys, time
from datetime import datetime

# 密钥参数
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

service = "cvm"
host = "cvm.cloud.sunhongs.com"
endpoint = "https://" + host
region = "ap-guangzhou"
action = "DescribeInstances"
version = "2017-03-12"
algorithm = "TC3-HMAC-SHA256"
timestamp = 1539084154
date = datetime.utcfromtimestamp(timestamp).strftime("%Y-%m-%d")
params = {"Limit": 10, "Offset": 0}
```

```
# ************* 步骤 1：拼接规范请求串 *************
http_request_method = "GET"
canonical_uri = "/"
canonical_querystring = "Limit=10&Offset=0"
ct = "x-www-form-urlencoded"
payload = ""
if http_request_method == "POST":
canonical_querystring = ""
ct = "json"
payload = json.dumps(params)
canonical_headers = "content-type:application/%s\nhost:%s\n" % (ct, host)
signed_headers = "content-type;host"
hashed_request_payload = hashlib.sha256(payload.encode("utf-8")).hexdigest()
canonical_request = (http_request_method + "\n" +
canonical_uri + "\n" +
canonical_querystring + "\n" +
canonical_headers + "\n" +
signed_headers + "\n" +
hashed_request_payload)
print(canonical_request)

# ************* 步骤 2：拼接待签名字符串 *************
credential_scope = date + "/" + service + "/" + "tc3_request"
hashed_canonical_request = hashlib.sha256(canonical_request.encode("utf-8")).hexdigest()
string_to_sign = (algorithm + "\n" +
str(timestamp) + "\n" +
credential_scope + "\n" +
hashed_canonical_request)
print(string_to_sign)


# ************* 步骤 3：计算签名 *************
# 计算签名摘要函数
def sign(key, msg):
return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()
secret_date = sign(("TC3" + secret_key).encode("utf-8"), date)
secret_service = sign(secret_date, service)
secret_signing = sign(secret_service, "tc3_request")
signature = hmac.new(secret_signing, string_to_sign.encode("utf-8"), hashlib.sha256).hexdigest()
print(signature)

# ************* 步骤 4：拼接 Authorization *************
authorization = (algorithm + " " +
"Credential=" + secret_id + "/" + credential_scope + ", " +
"SignedHeaders=" + signed_headers + ", " +
"Signature=" + signature)
print(authorization)

# 公共参数添加到请求头部
headers = {
"Authorization": authorization,
"Host": host,
"Content-Type": "application/%s" % ct,
"X-TC-Action": action,
"X-TC-Timestamp": str(timestamp),
"X-TC-Version": version,
"X-TC-Region": region,
}
```

请求结构

最近更新时间: 2024-09-03 18:49:46

1. 服务地址

地域（Region）是指物理的数据中心的地理区域。tcecloud交付验证不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了降低访问时延、提高下载速度，建议您选择最靠近您客户的地域。

您可以通过 API接口 **查询地域列表** 查看完成的地域列表。

2. 通信协议

tcecloud API 的所有接口均通过 HTTPS 进行通信，提供高安全性的通信通道。

3. 请求方法

支持的 HTTP 请求方法:

- POST（推荐）
- GET

POST 请求支持的 Content-Type 类型：

- application/json（推荐），必须使用 TC3-HMAC-SHA256 签名方法。
- application/x-www-form-urlencoded，必须使用 HmacSHA1 或 HmacSHA256 签名方法。
- multipart/form-data（仅部分接口支持），必须使用 TC3-HMAC-SHA256 签名方法。

GET 请求的请求包大小不得超过 32 KB。POST 请求使用签名方法为 HmacSHA1、HmacSHA256 时不得超过 1 MB。POST 请求使用签名方法为 TC3-HMAC-SHA256 时支持 10 MB。

4. 字符编码

均使用UTF-8编码。

返回结果

最近更新时间: 2024-09-03 18:49:46

正确返回结果

以云服务器的接口查看实例状态列表 (DescribeInstancesStatus) 2017-03-12 版本为例，若调用成功，其可能的返回如下为：

```
{
"Response": {
"TotalCount": 0,
"InstanceStatusSet": [],
"RequestId": "b5b41468-520d-4192-b42f-595cc34b6c1c"
}
}
```

- Response 及其内部的 RequestId 是固定的字段，无论请求成功与否，只要 API 处理了，则必定会返回。
- RequestId 用于一个 API 请求的唯一标识，如果 API 出现异常，可以联系我们，并提供该 ID 来解决问题。
- 除了固定的字段外，其余均为具体接口定义的字段，不同的接口所返回的字段参见接口文档中的定义。此例中的 TotalCount 和 InstanceStatusSet 均为 DescribeInstancesStatus 接口定义的字段，由于调用请求的用户暂时还没有云服务器实例，因此 TotalCount 在此情况下的返回值为 0，InstanceStatusSet 列表为空。

错误返回结果

若调用失败，其返回值示例如下为：

```
{
"Response": {
"Error": {
"Code": "AuthFailure.SignatureFailure",
"Message": "The provided credentials could not be validated. Please check your signature is correct."
},
"RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
}
}
```

- Error 的出现代表着该请求调用失败。Error 字段连同其内部的 Code 和 Message 字段在调用失败时是必定返回的。
- Code 表示具体出错的错误码，当请求出错时可以先根据该错误码在公共错误码和当前接口对应的错误码列表里面查找对应原因和解决方案。
- Message 显示出了这个错误发生的具体原因，随着业务发展或体验优化，此文本可能会经常保持变更或更新，用户不应依赖这个返回值。
- RequestId 用于一个 API 请求的唯一标识，如果 API 出现异常，可以联系我们，并提供该 ID 来解决问题。

公共错误码 (TODO: 重复信息, 是否真的需要?)

返回结果中如果存在 Error 字段，则表示调用 API 接口失败。 Error 中的 Code 字段表示错误码，所有业务都可能出现的错误码为公共错误码，下表列出了公共错误码。

错误码	错误描述
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）。
AuthFailure.MFAFailure	MFA 错误。
AuthFailure.SecretIdNotFound	密钥不存在。

错误码	错误描述
AuthFailure.SignatureExpire	签名过期。
AuthFailure.SignatureFailure	签名错误。
AuthFailure.TokenFailure	token 错误。
AuthFailure.UnauthorizedOperation	请求未 CAM 授权。
DryRunOperation	DryRun 操作，代表请求将会是成功的，只是多传了 DryRun 参数。
FailedOperation	操作失败。
InternalError	内部错误。
InvalidAction	接口不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
NoSuchVersion	接口版本不存在。
RequestLimitExceeded	请求的次数超过了频率限制。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
UnauthorizedOperation	未授权操作。
UnknownParameter	未知参数错误。
UnsupportedOperation	操作不支持。
UnsupportedProtocol	http(s)请求协议错误，只支持 GET 和 POST 请求。
UnsupportedRegion	接口不支持所传地域。

公共参数

最近更新时间: 2024-09-03 18:49:46

公共参数是用于标识用户和接口鉴权目的的参数，如非必要，在每个接口单独的接口文档中不再对这些参数进行说明，但每次请求均需要携带这些参数，才能正常发起请求。

签名方法 v3

使用 TC3-HMAC-SHA256 签名方法时，公共参数需要统一放到 HTTP Header 请求头部中，如下：

参数名称	类型	必选	描述
X-TC-Action	String	是	操作的接口名称。取值参考接口文档中输入参数公共参数 Action 的说明。例如云服务器的查询实例列表接口，取值为 DescribeInstances。
X-TC-Region	String	是	地域参数，用来标识希望操作哪个地域的数据。接口接受的地域取值参考接口文档中输入参数公共参数 Region 的说明。注意：某些接口不需要传递该参数，接口文档中会对此特别说明，此时即使传递该参数也不会生效。
X-TC-Timestamp	Integer	是	当前 UNIX 时间戳，可记录发起 API 请求的时间。例如 1529223702。注意：如果与服务器时间相差超过5分钟，会引起签名过期错误。
X-TC-Version	String	是	操作的 API 的版本。取值参考接口文档中入参公共参数 Version 的说明。例如云服务器的版本 2017-03-12。
Authorization	String	是	HTTP 标准身份认证头部字段，例如： TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=fe5f80f77d5fa3beca038a248ff027d0445342fe2855ddc963176630326f1024 其中， - TC3-HMAC-SHA256：签名方法，目前固定取该值； - Credential：签名凭证，AKIDEXAMPLE 是 SecretId；Date 是 UTC 标准时间的日期，取值需要和公共参数 X-TC-Timestamp 换算的 UTC 标准时间日期一致；service为产品名，必须与调用的产品域名一致，例如 cvm； - SignedHeaders：参与签名计算的头部信息，content-type 和 host 为必选头部； - Signature：签名摘要。
X-TC-Token	String	否	临时证书所用的 Token ，需要结合临时密钥一起使用。临时密钥和 Token 需要到访问管理服务调用接口获取。长期密钥不需要 Token。

签名方法 v1

使用 HmacSHA1 和 HmacSHA256 签名方法时，公共参数需要统一放到请求串中，如下

参数名称	类型	必选	描述
Action	String	是	操作的接口名称。取值参考接口文档中输入参数公共参数 Action 的说明。例如云服务器的查询实例列表接口，取值为 DescribeInstances。
Region	String	是	地域参数，用来标识希望操作哪个地域的数据。接口接受的地域取值参考接口文档中输入参数公共参数 Region 的说明。注意：某些接口不需要传递该参数，接口文档中会对此特别说明，此时即使传递该参数也不会生效。
Timestamp	Integer	是	当前 UNIX 时间戳，可记录发起 API 请求的时间。例如1529223702，如果与当前时间相差过大，会引起签名过期错误。
Nonce	Integer	是	随机正整数，与 Timestamp 联合起来，用于防止重放攻击。

参数名称	类型	必选	描述
SecretId	String	是	在云API密钥上申请的标识身份的 SecretId，一个 SecretId 对应唯一的 SecretKey ，而 SecretKey 会用来生成请求签名 Signature。
Signature	String	是	请求签名，用来验证此次请求的合法性，需要用户根据实际的输入参数计算得出。具体计算方法参见接口鉴权文档。
Version	String	是	操作的 API 的版本。取值参考接口文档中入参公共参数 Version 的说明。例如云服务器的版本 2017-03-12。
SignatureMethod	String	否	签名方式，目前支持 HmacSHA256 和 HmacSHA1。只有指定此参数为 HmacSHA256 时，才使用 HmacSHA256 算法验证签名，其他情况均使用 HmacSHA1 验证签名。
Token	String	否	临时证书所用的 Token ，需要结合临时密钥一起使用。临时密钥和 Token 需要到访问管理服务调用接口获取。长期密钥不需要 Token 。

地域列表

地域（Region）是指物理的数据中心的地理区域。tcecloud交付验证不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了降低访问时延、提高下载速度，建议您选择最靠近您客户的地域。

您可以通过 API接口 **查询地域列表** 查看完成的地域列表。

告警设置相关接口
添加编辑告警策略

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

添加编辑告警策略

默认接口请求频率限制：20次/秒。

接口更新时间：2023-12-28 16:04:48。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddEditWarningRules
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
WarningRules	是	否	Array of WarningRule	告警开关策略

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	

获取告警策略列表

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

获取告警策略列表

默认接口请求频率限制：20次/秒。

接口更新时间：2024-01-02 10:12:16。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeWarningRules
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
WarningRules	WarningRule	告警策略列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	

安全合规相关接口
安全合规忽略资产+检测项列表

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

新增安全合规忽略(资产+检测项列表)列表，不显示指定的检查项包含的资产内容 参考的AddCompliancePolicyItemToWhitelist，除输入字段外，其它应该是一致的，如果有不同可能是定义的不对

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddComplianceAssetPolicySetToWhitelist
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
AssetPolicySetList	是	否	Array of ComplianceAssetPolicySetItem	资产ID+检查项IDs. 列表

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	

错误码	描述
OperationDenied	
FailedOperation	
InvalidParameter.MissingParameter	

安全合规忽略检测项+资产列表

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

新增安全合规忽略(检测项+资产)列表，不显示指定的检查项包含的资产内容 参考的AddCompliancePolicyItemToWhitelist，除输入字段外，其它应该是一致的，如果有不同可能是定义的不对

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddCompliancePolicyAssetSetToWhitelist
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
CustomerPolicyItemId	是	否	Uint64	检查项ID
CustomerAssetItemIdSet	否	否	Array of Uint64	需要忽略指定检查项内的资产ID列表

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	

错误码	描述
FailedOperation	
InvalidParameter.MissingParameter	

安全合规忽略检测项列表

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

将指定的检测项添加到白名单中，不显示未通过结果。

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddCompliancePolicyItemToWhitelist
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
CustomerPolicyItemIdSet	是	否	Array of Uint64	要忽略的检测项的ID的列表

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	
InvalidParameter.MissingParameter	

安全合规创建合规检查任务

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建合规检查任务，在资产级别触发重新检测时使用。

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateComplianceTask
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
AssetTypeSet	否	否	Array of String	指定要扫描的资产类型列表。 ASSET_CONTAINER, 容器 ASSET_IMAGE, 镜像 ASSET_HOST, 主机 ASSET_K8S, K8S资产 AssetTypeSet, PolicySetId, PeriodTaskId三个参数，必须要给其中一个参数填写有效的值。
PolicySetId	否	否	Uint64	按照策略集ID指定的策略执行合规检查。
PeriodTaskId	否	否	Uint64	按照定时任务ID指定的策略执行合规检查。

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的合规检查任务的ID。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	

错误码	描述
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	
InvalidParameter.MissingParameter	

创建一个导出安全合规信息的任务

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建一个导出安全合规信息的任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateExportComplianceStatusListJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
AssetType	是	否	String	要导出信息的资产类型
ExportByAsset	是	否	Bool	按照检测项导出，还是按照资产导出。true: 按照资产导出；false: 按照检测项导出。
IdList	否	否	Array of Uint64	要导出的资产ID列表或检测项ID列表，由ExportByAsset的取值决定。
ExportAll	是	否	Bool	true, 全部导出；false, 根据IdList来导出数据。

3. 输出参数

参数名称	类型	描述
JobId	String	返回创建的导出任务的ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
RequestLimitExceeded	

错误码	描述
LimitExceeded	
OperationDenied	
InvalidParameterValue	
FailedOperation	
InvalidParameterValue.DataNotFound	

删除安全合规忽略项， 资产+检测项列表

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

移除安全合规忽略(资产+检测项)列表，不显示指定的检查项包含的资产内容 参考的AddCompliancePolicyAssetSetToWhitelist，除输入字段外，其它应该是一致的，如果有不同可能是定义的不对

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteComplianceAssetPolicySetFromWhitelist
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
AssetItemId	是	否	Uint64	资产ID
CustomerPolicyItemIdSet	否	否	Array of Uint64	需要忽略指定资产内的检查项ID列表

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	

错误码	描述
OperationDenied	
FailedOperation	
InvalidParameter.MissingParameter	

删除检测项+资产列表的白名单策略

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

新增安全合规忽略(检测项+资产)列表，不显示指定的检查项包含的资产内容

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteCompliancePolicyAssetSetFromWhitelist
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
PolicyAssetSetList	是	否	Array of CompliancePolicyAssetSetItem	（检查项ID+资产ID列表）的列表

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

错误码	描述
InvalidParameter.MissingParameter	

安全合规取消忽略检测项列表

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

从白名单中删除将指定的检测项。

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteCompliancePolicyItemFromWhitelist
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
WhitelistIdSet	是	否	Array of Uint64	指定的白名单项的ID的列表

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

安全合规查询某个资产的详情

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询某个资产的详情

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeComplianceAssetDetailInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
CustomerAssetId	是	否	Uint64	客户资产ID。

3. 输出参数

参数名称	类型	描述
AssetDetailInfo	ComplianceAssetDetailInfo	某资产的详情。
ContainerDetailInfo	ComplianceContainerDetailInfo	当资产为容器时，返回此字段。
ImageDetailInfo	ComplianceImageDetailInfo	当资产为镜像时，返回此字段。
HostDetailInfo	ComplianceHostDetailInfo	当资产为主机时，返回此字段。
K8SDetailInfo	ComplianceK8SDetailInfo	当资产为K8S时，返回此字段。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	

错误码	描述
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	
InvalidParameter.MissingParameter	

安全合规查询某类资产的列表

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询某类资产的列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeComplianceAssetList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
AssetTypeSet	否	否	Array of String	资产类型列表。
Offset	否	否	Uint64	起始偏移量，默认为0。
Limit	否	否	Uint64	返回的数据量，默认为10，最大为100。
Filters	否	否	Array of ComplianceFilters	查询过滤器

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	返回资产的总数。
AssetInfoList	ComplianceAssetInfo	返回各类资产的列表。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	

错误码	描述
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

安全合规查询某资产下的检测项列表

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询某资产下的检测项列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeComplianceAssetPolicyItemList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
CustomerAssetId	是	否	Uint64	客户资产的ID。
Offset	否	否	Uint64	起始偏移量，默认为0。
Limit	否	否	Uint64	要获取的数据量，默认为10，最大为100。
Filters	否	否	Array of ComplianceFilters	过滤器列表。Name字段支持 RiskLevel

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	返回检测项的总数。如果用户未启用基线检查，此处返回0。
AssetPolicyItemList	ComplianceAssetPolicyItem	返回某个资产下的检测项的列表。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	

错误码	描述
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	
InvalidParameter.MissingParameter	

安全合规查询定时任务列表

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询合规检测的定时任务列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeCompliancePeriodTaskList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
AssetType	否	否	String	**此参数对外不可见。** 资产的类型，取值为： ASSET_CONTAINER, 容器 ASSET_IMAGE, 镜像 ASSET_HOST, 主机 ASSET_K8S, K8S资产
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100。

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	定时任务的总量。
PeriodTaskSet	CompliancePeriodTask	定时任务信息的列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	

安全合规查询检测项影响的资产列表

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

按照 检测项 → 资产 的两级层次展开的第二层级：资产层级。

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeCompliancePolicyItemAffectedAssetList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
CustomerPolicyItemId	是	否	Uint64	DescribeComplianceTaskPolicyItemSummaryList返回的CustomerPolicyItemId，表示检测项的ID。
Offset	否	否	Uint64	起始偏移量，默认为0。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100。
Filters	否	否	Array of ComplianceFilters	过滤条件。 Name - String Name 可取值：NodeName, CheckResult

3. 输出参数

参数名称	类型	描述
AffectedAssetList	ComplianceAffectedAsset	返回各检测项所影响的资产的列表。
TotalCount	Uint64	检测项影响的资产的总数。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

安全合规查询某检测项影响的信息

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

按照 检测项 → 资产 的两级层次展开的第一层级：检测项层级。

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeCompliancePolicyItemAffectedSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
CustomerPolicyItemId	是	否	Uint64	DescribeComplianceTaskPolicyItemSummaryList返回的CustomerPolicyItemId，表示检测项的ID。

3. 输出参数

参数名称	类型	描述
PolicyItemSummary	CompliancePolicyItemSummary	返回各检测项影响的资产的汇总信息。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	

错误码	描述
FailedOperation	

安全合规查询上次检测失败的资产的列表

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

按照 资产 → 检测项 二层结构展示的信息。这里查询第一层 资产的通过率汇总信息。

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeComplianceScanFailedAssetList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
AssetTypeSet	否	否	Array of String	资产类型列表。 ASSET_CONTAINER, 容器 ASSET_IMAGE, 镜像 ASSET_HOST, 主机 ASSET_K8S, K8S资产
Offset	否	否	Uint64	起始偏移量，默认为0。
Limit	否	否	Uint64	返回的数据量，默认为10，最大为100。
Filters	否	否	Array of ComplianceFilters	查询过滤器

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	返回检测失败的资产的总数。
ScanFailedAssetList	ComplianceScanFailedAsset	返回各类检测失败的资产的汇总信息的列表。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

安全合规查询上次任务的资产通过率汇总信息

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询上次任务的资产通过率汇总信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeComplianceTaskAssetSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
AssetTypeSet	是	否	Array of String	资产类型列表。 ASSET_CONTAINER, 容器 ASSET_IMAGE, 镜像 ASSET_HOST, 主机 ASSET_K8S, K8S资产

3. 输出参数

参数名称	类型	描述
Status	String	返回用户的状态， USER_UNINIT: 用户未初始化。 USER_INITIALIZING，表示用户正在初始化环境。 USER_NORMAL: 正常状态。
AssetSummaryList	ComplianceAssetSummary	返回各类资产的汇总信息的列表。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	

错误码	描述
OperationDenied	
FailedOperation	

安全合规查询上次任务的检测项的汇总信息列表

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询最近一次任务发现的检测项的汇总信息列表，按照 检测项 → 资产 的两级层次展开。

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeComplianceTaskPolicyItemSummaryList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
AssetType	否	否	String	资产类型。仅查询与指定资产类型相关的检测项。 ASSET_CONTAINER, 容器 ASSET_IMAGE, 镜像 ASSET_HOST, 主机 ASSET_K8S, K8S资产
Offset	否	否	Uint64	起始偏移量，默认为0。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100。
Filters	否	否	Array of ComplianceFilters	过滤条件。 Name - String Name 可取值：ItemType, StandardId, RiskLevel。 当为K8S资产时，还可取ClusterName。

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回最近一次合规检查任务的ID。这个任务为本次所展示数据的来源。
TotalCount	Uint64	返回检测项的总数。
PolicyItemSummaryList	CompliancePolicyItemSummary	返回各检测项对应的汇总信息的列表。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

安全合规查询白名单列表

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询白名单列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeComplianceWhitelistItemList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Offset	否	否	Uint64	起始偏移量，默认为0。
Limit	否	否	Uint64	要获取的数量，默认为10，最大为100。
AssetTypeSet	否	否	Array of String	资产类型列表。
Filters	否	否	Array of ComplianceFilters	查询过滤器
By	否	否	String	排序字段
Order	否	否	String	排序方式 desc asc

3. 输出参数

参数名称	类型	描述
WhitelistItemSet	ComplianceWhitelistItem	白名单项的列表。
TotalCount	Uint64	白名单项的总数。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

安全合规初始化用户的合规基线检测环境

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

为客户初始化合规基线的使用环境，创建必要的数据和选项。

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：InitializeUserComplianceEnvironment
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

安全合规编辑定时任务

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改定时任务的设置，包括检测周期、开启/禁用合规基准。

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyCompliancePeriodTask
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
PeriodTaskId	是	否	Uint64	要修改的定时任务的ID，由DescribeCompliancePeriodTaskList接口返回。
PeriodRule	否	否	CompliancePeriodTaskRule	定时任务的周期规则。不填时，不修改。
StandardSettings	否	否	Array of ComplianceBenchmarkStandardEnable	设置合规标准。不填时，不修改。

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
RequestLimitExceeded	
OperationDenied	
FailedOperation	

安全合规重新检测选定的资产

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

重新检测选定的资产

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ScanComplianceAssets
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
CustomerAssetIdSet	是	否	Array of Uint64	要重新扫描的客户资产项ID的列表。

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回重新检测任务的ID。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

错误码	描述
InvalidParameter.MissingParameter	

安全合规用指定的检测项重新检测选定的资产

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

用指定的检测项重新检测选定的资产，返回创建的合规检查任务的ID。

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ScanComplianceAssetsByPolicyItem
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
CustomerPolicyItemId	是	否	Uint64	指定的检测项的ID
CustomerAssetIdSet	是	否	Array of Uint64	要重新扫描的客户资产项ID的列表。

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回重新检测任务的ID。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	

错误码	描述
FailedOperation	
InvalidParameter.MissingParameter	

安全合规重新检测选定的检测项

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

重新检测选的检测项下的所有资产，返回创建的合规检查任务的ID。

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ScanCompliancePolicyItems
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
CustomerPolicyItemIdSet	是	否	Array of Uint64	要重新扫描的客户检测项的列表。

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回重新检测任务的ID。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

错误码	描述
InvalidParameter.MissingParameter	

安全合规重新检测上次检测失败的资产

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

重新检测选定的检测失败的资产下的所有失败的检测项，返回创建的合规检查任务的ID。

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ScanComplianceScanFailedAssets
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
CustomerAssetIdSet	是	否	Array of Uint64	要重新扫描的客户资产项ID的列表。

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回重新检测任务的ID。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

错误码	描述
InvalidParameter.MissingParameter	

安全运营-日志分析 相关接口
添加检索模板

最近更新时间: 2024-09-03 18:49:46

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

添加检索模板

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateSearchTemplate
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
SearchTemplate	是	否	SearchTemplate	搜索模板

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
InternalError.MainDBFail	

删除检索模板

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

删除检索模板

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteSearchTemplate
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	Uint64	模板ID

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
InternalError.MainDBFail	

获取ES字段聚合结果

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

获取ES字段聚合结果

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeESAggregations
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Query	是	否	String	ES聚合条件JSON

3. 输出参数

参数名称	类型	描述
Data	String	ES聚合结果JSON
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
InternalError.MainDBFail	

获取ES查询文档列表

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

获取ES查询文档列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeESHits
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Query	是	否	String	ES查询条件JSON
Offset	否	否	Uint64	偏移量，默认为0。
Limit	否	否	Uint64	返回数量，最大值为100。

3. 输出参数

参数名称	类型	描述
Data	String	ES查询结果JSON
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
InternalError.MainDBFail	

获取索引列表

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

获取索引列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeIndexList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
Data	String	ES 索引信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
InternalError.MainDBFail	

获取日志检索容量使用统计

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

获取日志检索容量使用统计

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeLogStorageStatistic
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
TotalSize	Uint64	总容量（单位：B）
UsedSize	Uint64	已使用容量（单位：B）
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
InternalError.MainDBFail	

获取公钥

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

获取公钥

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribePublicKey
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
PublicKey	String	公钥
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

导出ES查询文档列表

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

导出ES查询文档列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSearchExportList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Query	是	否	String	ES查询条件JSON

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
InternalError.MainDBFail	

获取历史搜索记录

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

获取历史搜索记录

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSearchLogs
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
Data	String	历史搜索记录 保留最新的10条
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
InternalError.MainDBFail	

获取快速检索列表

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

获取快速检索列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSearchTemplates
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Offset	否	否	Uint64	偏移量，默认为0。
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	总数
List	SearchTemplate	模板列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
InternalError.MainDBFail	

查询安全日志告警信息

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询安全日志告警信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecLogAlertMsg
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Type	否	否	Array of String	告警类型 日志储量告警: log_reserve_full 日志存储时间告警: log_save_day_limit kafka实例/公网域名不可用: kafka_instance_domain_unavailable kafka 用户名密码错误: kafka_user_passwd_wrong kafka后台报错字段: kafka_field_wrong

3. 输出参数

参数名称	类型	描述
List	SecLogAlertMsgInfo	告警消息队列
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询安全日志清理设置详情

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询安全日志清理设置详情

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecLogCleanSettingInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
ReservesLimit	Uint64	触发清理的储量底线
ReservesDeadline	Uint64	清理停止时的储量截至线
DayLimit	Uint64	触发清理的存储天数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询安全日志投递cls可选项

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询安全日志投递cls可选项

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecLogDeliveryClsOptions
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClsRegion	否	否	String	地域

3. 输出参数

参数名称	类型	描述
LogSetList	ClsLogsetInfo	cls可选日志集合列表(仅当入参ClsRegion不为空时返回)
RegionList	RegionInfo	可选地域列表(仅当入参ClsRegion为空时返回)
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询安全日志投递Cls配置

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询安全日志投递Cls配置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecLogDeliveryClsSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
LogTypeList	SecLogDeliveryClsSettingInfo	日志类型列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询安全日志投递kafka可选项

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询安全日志投递kafka可选项

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecLogDeliveryKafkaOptions
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RegionID	否	否	String	地域，若为空则返回所有可选地域

3. 输出参数

参数名称	类型	描述
InstanceList	CKafkaInstanceInfo	实例列表
RegionList	RegionInfo	地域列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询安全日志投递kafka配置

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询安全日志投递kafka配置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecLogDeliveryKafkaSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
InstanceID	String	消息队列实例ID
InstanceName	String	消息队列实例名称
Domain	String	域名
LogTypeList	SecLogDeliveryKafkaSettingInfo	日志类型队列
User	String	用户名
RegionID	String	地域ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询安全日志接入对象列表

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询安全日志接入对象列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecLogJoinObjectList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
LogType	是	否	String	**此参数对外不可见。** 日志类型 bash: "container_bash", 启动: "container_launch", "k8s": "k8s_api"
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	**此参数对外不可见。** 过滤条件。 - Status- String - 是否必填：否 - 主机状态 - HostIP- String - 是否必填：否 - 主机内网IP - PublicIP- String - 是否必填：否 - 主机外网IP - HostName- String - 是否必填：否 - 主机名称
By	否	否	String	**此参数对外不可见。** 排序字段
Order	否	否	String	**此参数对外不可见。** 排序方式

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	总数
List	SecLogJoinObjectInfo	接入对象列表

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询安全日志接入列表

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询安全日志接入列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口只验签名不鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecLogJoinTypeList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
List	SecLogJoinInfo	接入日志列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询安全日志KafkaUIN

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询安全日志KafkaUIN

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecLogKafkaUIN
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
DstUIN	String	目标UIN
Status	Bool	授权状态
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

修改安全日志清理设置信息

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改安全日志清理设置信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifySecLogCleanSettingInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ReservesLimit	是	否	Uint64	触发清理的储量底线(50-99)
ReservesDeadline	是	否	Uint64	清理停止时的储量截至线(>0,小于ReservesLimit)
DayLimit	是	否	Uint64	触发清理的存储天数(>=1)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

更新安全日志-日志投递cls配置

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

更新安全日志-日志投递cls配置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifySecLogDeliveryClsSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
List	是	否	Array of SecLogDeliveryClsSettingInfo	日志信息

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

更新安全日志投递kafka设置

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

更新安全日志投递kafka设置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifySecLogDeliveryKafkaSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
InstanceID	否	否	String	实例ID
InstanceName	否	否	String	实例名称
Domain	否	否	String	域名
User	否	否	String	用户名
Password	否	否	String	密码
LogTypeList	否	否	Array of SecLogDeliveryKafkaSettingInfo	日志类型队列
AccessType	否	否	Int64	接入类型
KafkaVersion	否	否	String	kafka版本号
RegionID	否	否	String	地域ID

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

修改安全日志接入对象

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改安全日志接入对象

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifySecLogJoinObjects
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
BindList	否	否	Array of String	**此参数对外不可见。** 绑定主机quuid列表
UnBindList	否	否	Array of String	**此参数对外不可见。** 待解绑主机quuid列表
LogType	是	否	String	**此参数对外不可见。** 日志类型 bash日志: container_bash 容器启动: container_launch k8sApi: k8s_api
NodeType	否	否	String	**此参数对外不可见。** 节点类型:
NORMAL: 普通节点(默认值)				
SUPER: 超级节点				

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

修改安全日志接入状态

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改安全日志接入状态

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifySecLogJoinState
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
LogType	是	否	String	日志类型 bash日志: container_bash 容器启动: container_launch k8sApi: k8s_api
State	是	否	Bool	状态(true:开 false:关)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

修改安全日志kafkaUIN

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改安全日志kafkaUIN

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifySecLogKafkaUIN
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
DstUIN	否	否	String	目标UIN

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

重置安全日志主题设置

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

重置安全日志主题设置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ResetSecLogTopicConfig
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ConfigType	是	否	String	配置类型(ckafka/cls)
LogType	是	否	String	日志类型

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

网络安全相关接口
容器网络创建网络策略添加并发布任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络创建网络策略添加并发布任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddAndPublishNetworkFirewallPolicyDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	是	否	String	集群Id
PolicyName	是	否	String	策略名
Namespace	否	否	String	命名空间
FromPolicyRule	是	否	Int64	入站规则 全部允许：1 全部拒绝 ：2 自定义：3
ToPolicyRule	是	否	Int64	出站规则 全部允许：1 全部拒绝 ：2 自定义：3
PodSelector	是	否	String	pod选择器
Description	否	否	String	策略描述
CustomPolicy	否	否	Array of NetworkCustomPolicy	自定义规则

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的任务的ID，为0表示创建失败。
Result	String	创建任务的结果，"Succ"为成功，"Failed"为失败

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络创建Yaml网络策略并发布任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络创建Yaml网络策略并发布任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddAndPublishNetworkFirewallPolicyYamlDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	是	否	String	集群Id
PolicyName	是	否	String	策略名
Yaml	否	否	String	base64编码的networkpolicy yaml字符串
Description	否	否	String	策略描述

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的任务的ID，为0表示创建失败。
Result	String	创建任务的结果，"Succ"为成功，"Failed"为失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络创建网络策略添加任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络创建网络策略添加任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddNetworkFirewallPolicyDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	是	否	String	集群Id
PolicyName	是	否	String	策略名
Namespace	否	否	String	命名空间
FromPolicyRule	是	否	Int64	入站规则 全部允许：1 全部拒绝 ：2 自定义：3
ToPolicyRule	是	否	Int64	出站规则 全部允许：1 全部拒绝 ：2 自定义：3
PodSelector	是	否	String	pod选择器
Description	否	否	String	策略描述
CustomPolicy	否	否	Array of NetworkCustomPolicy	自定义规则

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的任务的ID，为0表示创建失败。
Result	String	创建任务的结果，"Succ"为成功，"Failed"为失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络创建Yaml网络策略添加任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络创建Yaml网络策略添加任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddNetworkFirewallPolicyYamlDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	是	否	String	集群Id
PolicyName	是	否	String	策略名
Yaml	否	否	String	base64编码的networkpolicy yaml字符串
Description	否	否	String	策略描述

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的任务的ID，为0表示创建失败。
Result	String	创建任务的结果，"Succ"为成功，"Failed"为失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络创建检查Yaml网络策略任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络创建检查Yaml网络策略任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CheckNetworkFirewallPolicyYaml
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	是	否	String	集群Id
PolicyName	是	否	String	策略名
Yaml	否	否	String	base64编码的networkpolicy yaml字符串
Description	否	否	String	策略描述

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的任务的ID，为0表示创建失败。
Result	String	创建任务的结果，"Succ"为成功，"Failed"为失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络创建网络策略确认任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络创建网络策略确认任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ConfirmNetworkFirewallPolicy
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	是	否	String	集群Id
Id	是	否	Array of Uint64	策略Id数组

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的任务的ID，为0表示创建失败。
Result	String	创建确认任务的结果，"Succ"为成功，"Failed"为失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络集群下发刷新任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络集群下发刷新任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateNetworkFirewallClusterRefresh
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的集群检查任务的ID，为0表示创建失败。
Result	String	创建检查任务的结果，"Succ"为成功，"Failed"为失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	

错误码	描述
FailedOperation	

容器网络集群网络策略创建自动发现任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络集群网络策略创建自动发现任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateNetworkFirewallPolicyDiscover
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	是	否	String	集群Id

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的集群检查任务的ID，为0表示创建失败。
Result	String	创建检查任务的结果，"Succ"为成功，"Failed"为失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	

错误码	描述
OperationDenied	
FailedOperation	

容器网络创建网络策略发布任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络创建网络策略发布任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateNetworkFirewallPublish
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	是	否	String	集群Id
Id	是	否	Array of Uint64	策略Id数组

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的任务的ID，为0表示创建失败。
Result	String	创建任务的结果，"Succ"为成功，"Failed"为失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络创建网络策略撤销任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络创建网络策略撤销任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateNetworkFirewallUndoPublish
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	是	否	String	集群Id
Id	是	否	Array of Uint64	策略Id数组

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的任务的ID，为0表示创建失败。
Result	String	创建任务的结果，"Succ"为成功，"Failed"为失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络创建网络策略删除任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络创建网络策略删除任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteNetworkFirewallPolicyDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	是	否	String	集群Id
Id	是	否	Array of Uint64	策略Id数组

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的任务的ID，为0表示创建失败。
Result	String	创建删除任务的结果，"Succ"为成功，"Failed"为失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
RequestLimitExceeded	
OperationDenied	
FailedOperation	

查询集群策略审计列表

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询集群策略审计列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeNetworkFirewallAuditRecord
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Offset	否	否	Uint64	偏移量
Limit	否	否	Uint64	每次查询的最大记录数量
Filters	否	否	Array of ComplianceFilters	Name - Action Name 可取值：publish，unpublish，confirm，add，update，delete
By	否	否	String	排序字段
Order	否	否	String	排序方式 asc,desc

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	集群审计总数
AuditList	NetworkAuditRecord	集群的审计详细信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

查询集群策略列表

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询集群策略列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeNetworkFirewallClusterList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Offset	否	否	Uint64	偏移量
Limit	否	否	Uint64	每次查询的最大记录数量
Filters	否	否	Array of ComplianceFilters	Name - String Name 可取值：ClusterName,ClusterId,ClusterType,Region,ClusterCheckMode,ClusterAutoCheck
By	否	否	String	排序字段
Order	否	否	String	排序方式 asc,desc

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	集群总数
ClusterInfoList	NetworkClusterInfoItem	集群的详细信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络查询资产任务进度

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络查询资产任务进度

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeNetworkFirewallClusterRefreshStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskId	是	否	Uint64	任务ID

3. 输出参数

参数名称	类型	描述
TaskStatus	String	任务状态，可能为：Task_Running,Task_Succ,Task_Error,Task_NoExist
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	

错误码	描述
FailedOperation	

查询集群网络空间标签列表

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询集群网络空间标签列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeNetworkFirewallNamespaceLabelList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Offset	否	否	Uint64	偏移量
Limit	否	否	Uint64	每次查询的最大记录数量
Filters	否	否	Array of ComplianceFilters	Name - String Name 可取值：ClusterName,ClusterId,ClusterType,Region,ClusterCheckMode,ClusterAutoCheck
By	否	否	String	排序字段
Order	否	否	String	排序方式 asc,desc
ClusterId	是	否	String	集群id

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	集群总数
ClusterNamespaceLabelList	NetworkClusterNamespaceLabelInfo	集群空间标签详细信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

查询集群网络空间列表

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询集群网络空间列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeNetworkFirewallNamespaceList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Offset	否	否	Uint64	偏移量
Limit	否	否	Uint64	每次查询的最大记录数量
Filters	否	否	Array of ComplianceFilters	Name - String Name 可取值：ClusterName,ClusterId,ClusterType,Region,ClusterCheckMode,ClusterAutoCheck
By	否	否	String	排序字段
Order	否	否	String	排序方式 asc,desc
ClusterId	是	否	String	集群id

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	集群总数
ClusterNamespaceList	NetworkClusterNamespaceInfo	集群的详细信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

查询集群网络pod标签

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询集群网络pod标签

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeNetworkFirewallPodLabelsList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Offset	否	否	Uint64	偏移量
Limit	否	否	Uint64	每次查询的最大记录数量
Filters	否	否	Array of ComplianceFilters	Name - String Name 可取值：ClusterName,ClusterId,ClusterType,Region,ClusterCheckMode,ClusterAutoCheck
By	否	否	String	排序字段
Order	否	否	String	排序方式 asc,desc
ClusterId	是	否	String	集群id

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	集群pod总数
PodList	NetworkClusterPodInfo	集群pod详细信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络集群查看策略详情

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络集群查看策略详情

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeNetworkFirewallPolicyDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	Uint64	策略Id

3. 输出参数

参数名称	类型	描述
ClusterId	String	集群Id
PolicyName	String	策略名
Namespace	String	命名空间
FromPolicyRule	Int64	入站类型
ToPolicyRule	Int64	出站类型
CustomPolicy	NetworkCustomPolicy	自定义规则
PodSelector	String	pod选择器
Description	String	策略描述
PolicyCreateTime	String	策略创建时间
PolicySourceType	String	策略源类型，分为System和Manual，分别代表手动和系统添加
NetworkPolicyPlugin	String	网络策略对应的网络插件
PublishStatus	String	网络策略状态

参数名称	类型	描述
PublishResult	String	网络发布结果
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络查询网络策略自动发现任务进度

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络查询网络策略自动发现任务进度

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeNetworkFirewallPolicyDiscover
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskId	是	否	Uint64	任务ID

3. 输出参数

参数名称	类型	描述
TaskStatus	String	任务状态，可能为：Task_Running,Task_Succ,Task_Error,Task_NoExist
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	

错误码	描述
FailedOperation	

查询集群网络策略列表

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询集群网络策略列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeNetworkFirewallPolicyList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Offset	否	否	Uint64	偏移量
Limit	否	否	Uint64	每次查询的最大记录数量
Filters	否	否	Array of ComplianceFilters	Name - String Name 可取值：ClusterName,ClusterId,ClusterType,Region,ClusterCheckMode,ClusterAutoCheck
By	否	否	String	排序字段
Order	否	否	String	排序方式 asc,desc
ClusterId	是	否	String	集群id

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	集群总数
NetPolicy	NetworkPolicyInfoItem	集群的详细信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络查询网络策略策略执行状态

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络查询网络策略策略执行状态

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeNetworkFirewallPolicyStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskId	是	否	Uint64	任务ID

3. 输出参数

参数名称	类型	描述
TaskStatus	String	任务状态，可能为：Task_Running,Task_Succ,Task_Error,Task_NoExist
TaskResult	String	NameRepeat,K8sRuleIngressPortError等
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	

错误码	描述
OperationDenied	
FailedOperation	

容器网络集群查看Yaml网络策略详情

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络集群查看Yaml网络策略详情

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeNetworkFirewallPolicyYamlDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	Uint64	策略Id

3. 输出参数

参数名称	类型	描述
ClusterId	String	集群Id
PolicyName	String	策略名
Yaml	String	base64编码的yaml字符串
Description	String	策略描述
PolicyCreateTime	String	策略创建时间
PolicySourceType	String	策略源类型，分为System和Manual，分别代表手动和系统添加
NetworkPolicyPlugin	String	网络策略对应的网络插件
PublishStatus	String	网络策略状态
PublishResult	String	网络发布结果
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络创建网络策略更新并发布任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络创建网络策略更新并发布任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：UpdateAndPublishNetworkFirewallPolicyDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	是	否	String	集群Id
Id	是	否	Uint64	策略Id
Namespace	否	否	String	命名空间
FromPolicyRule	是	否	Int64	入站规则 全部允许：1 全部拒绝 ：2 自定义：3
ToPolicyRule	是	否	Int64	出站规则 全部允许：1 全部拒绝 ：2 自定义：3
PodSelector	是	否	String	pod选择器
Description	否	否	String	策略描述
CustomPolicy	否	否	Array of NetworkCustomPolicy	自定义规则

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的任务的ID，为0表示创建失败。
Result	String	创建任务的结果，"Succ"为成功，"Failed"为失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络更新Yaml网络策略并发布任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络更新Yaml网络策略并发布任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：UpdateAndPublishNetworkFirewallPolicyYamlDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	是	否	String	集群Id
Id	是	否	Uint64	策略id
Yaml	否	否	String	base64编码的networkpolicy yaml字符串
Description	否	否	String	策略描述

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的任务的ID，为0表示创建失败。
Result	String	创建任务的结果，"Succ"为成功，"Failed"为失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络创建网络策略更新任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络创建网络策略更新任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：UpdateNetworkFirewallPolicyDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	是	否	String	集群Id
Id	是	否	Uint64	策略Id
Namespace	否	否	String	命名空间
FromPolicyRule	是	否	Int64	入站规则 全部允许：1 全部拒绝 ：2 自定义：3
ToPolicyRule	是	否	Int64	出站规则 全部允许：1 全部拒绝 ：2 自定义：3
PodSelector	是	否	String	pod选择器
Description	否	否	String	策略描述
CustomPolicy	否	否	Array of NetworkCustomPolicy	自定义规则

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的任务的ID，为0表示创建失败。
Result	String	创建任务的结果，"Succ"为成功，"Failed"为失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

容器网络更新Yaml网络策略任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器网络更新Yaml网络策略任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：UpdateNetworkFirewallPolicyYamlDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	是	否	String	集群Id
Id	是	否	Uint64	策略id
Yaml	否	否	String	base64编码的networkpolicy yaml字符串
Description	否	否	String	策略描述

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的任务的ID，为0表示创建失败。
Result	String	创建任务的结果，"Succ"为成功，"Failed"为失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

计费相关接口
查询镜像授权信息

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

DescribeImageAuthorizedInfo 查询镜像授权信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:23:21。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeImageAuthorizedInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
TotalAuthorizedCnt	Uint64	总共有效的镜像授权数
UsedAuthorizedCnt	Uint64	已使用镜像授权数
ScannedImageCnt	Uint64	已开启扫描镜像数
NotScannedImageCnt	Uint64	未开启扫描镜像数
NotScannedLocalImageCnt	Uint64	本地未开启扫描镜像数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InternalError.MainDBFail	

查询专业版需购买信息

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

DescribeProVersionInfo 查询专业版需购买信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeProVersionInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
StartTime	String	专业版开始时间，补充购买时才不为空
EndTime	String	专业版结束时间，补充购买时才不为空
CoresCnt	Uint64	需购买的机器核数
MaxPostPayCoresCnt	Uint64	弹性计费上限
ResourceId	String	资源ID
BuyStatus	String	购买状态 待购: Pending 已购: Normal 隔离: Isolate
IsPurchased	Bool	是否曾经购买过(false:未曾 true:曾经购买过)
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

错误码	描述
InvalidParameter.ParsingError	
InternalError.MainDBFail	
InternalError.ErrRoleNotExist	

查询容器安全服务已购买信息

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

DescribePurchaseStateInfo 查询容器安全服务已购买信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribePurchaseStateInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
State	Int64	0：可申请试用可购买；1：只可购买(含试用审核不通过和试用过期)；2：试用生效中；3：专业版生效中；4：专业版过期
CoresCnt	Uint64	总核数
AuthorizedCoresCnt	Uint64	已购买核数
ImageCnt	Uint64	镜像数
AuthorizedImageCnt	Uint64	已授权镜像数
PurchasedAuthorizedCnt	Uint64	已购买镜像授权数
ExpirationTime	String	过期时间
AutomaticRenewal	Int64	0表示默认状态(用户未设置，即初始状态)， 1表示自动续费，2表示明确不自动续费(用户设置)
GivenAuthorizedCnt	Uint64	试用期间赠送镜像授权数，可能会过期
BeginTime	String	起始时间
SubState	String	子状态(具体意义依据State字段而定) State为4时，有效值为: ISOLATE(隔离) DESTROED(已销毁)
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
InternalError.MainDBFail	
InternalError.ErrRoleNotExist	

查询安全日志商品信息

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询安全日志商品信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecLogVasInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
BuyStatus	String	购买状态 待购: Pending 已购: Normal 隔离: Isolate
LogSaveMonth	Int64	存储时长(月)
StartTime	String	起始时间
EndTime	String	截止时间
LogCapacity	Uint64	存储容量(GB)
ResourceID	String	资源ID
IsPurchased	Bool	是否曾经购买过(false:未曾 true:曾经购买过)
TrialCapacity	Uint64	试用存储容量(GB)
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
InternalError	

资产管理相关接口
添加容器安全镜像扫描设置

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

添加容器安全镜像扫描设置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-20 15:51:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateAssetImageScanSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Enable	是	否	Bool	**此参数对外不可见。** 开关
ScanTime	是	否	String	**此参数对外不可见。** 扫描开始时间
01:00 时分				
ScanPeriod	是	否	Uint64	**此参数对外不可见。** 扫描周期
ScanVirus	是	否	Bool	**此参数对外不可见。** 扫描木马
ScanRisk	是	否	Bool	**此参数对外不可见。** 扫描敏感信息
ScanVul	是	否	Bool	**此参数对外不可见。** 扫描漏洞
All	否	否	Bool	**此参数对外不可见。** 全部镜像
Images	否	否	Array of String	**此参数对外不可见。** 自定义镜像
ContainerRunning	否	否	Bool	**此参数对外不可见。** 镜像是否存在运行中的容器

参数名称	必选	允许NULL	类型	描述
ScanScope	否	否	Uint64	**此参数对外不可见。** 扫描范围 0 全部授权镜像，1自选镜像，2 推荐扫描
ScanEndTime	否	否	String	**此参数对外不可见。** 扫描结束时间
02:00 时分				

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	

创建本地镜像木马列表导出任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建本地镜像木马列表导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateAssetImageVirusExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of AssetFilters	需要返回的数量，默认为10，最大值为10000
Limit	否	否	Uint64	偏移量，默认为0。
Offset	否	否	Uint64	过滤参数,"Filters":[{"Name":"Status","Values":["2"]}]
By	否	否	String	排序字段
Order	否	否	String	升序降序,asc desc
ExportField	是	否	Array of String	导出字段
ImageID	是	否	String	镜像id

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
FailedOperation	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

创建主机列表导出任务

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建主机列表导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateHostExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of AssetFilters	过滤条件。 - Status - String - 是否必填：否 - agent状态筛选，"ALL":"全部"(或不传该字段),"UNINSTALL"："未安装","OFFLINE"："离线", "ONLINE"："防护中" - HostName - String - 是否必填：否 - 主机名筛选 - Group- String - 是否必填：否 - 主机群组搜索 - HostIP- string - 是否必填：否 - 主机ip搜索 - HostID- string - 是否必填：否 - 主机id搜索 - DockerVersion- string - 是否必填：否 - docker版本搜索 - MachineType- string - 是否必填：否 - 主机来源MachineType搜索，"ALL":"全部"(或不传该字段),主机来源：["CVM", "ECM", "LH", "BM"] 中的之一为腾讯云服务器；["Other"]之一非腾讯云服务器； - DockerStatus- string - 是否必填：否 - docker安装状态，"ALL":"全部"(或不传该字段),"INSTALL":"已安装","UNINSTALL":"未安装" - ProjectID- string - 是否必填：否 - 所属项目id搜索 - Tag:xxx(tag:key)- string- 是否必填：否 - 标签键值搜索 示例Filters": [{"Name":"tag:tke-kind","Values":["service"]}]
Limit	否	否	Uint64	偏移量，默认为0。
Offset	否	否	Uint64	需要返回的数量，默认为10，最大值为10000
By	否	否	String	排序字段
Order	否	否	String	升序降序,asc desc
ExportField	否	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
FailedOperation	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

卸载Agent客户端

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

卸载Agent客户端

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteMachine
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Uuid	是	否	String	客户端Uuid

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
FailedOperation	
InvalidParameter.ParsingError	

错误码	描述
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	
FailedOperation.AgentOffline	

获取用户当前灰度配置

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

获取用户当前灰度配置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口只验签名不鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeABTestConfig
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ProjectName	否	否	String	灰度项目名称

3. 输出参数

参数名称	类型	描述
Config	ABTestConfig	灰度项目配置
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
AuthFailure	
InternalError	

查询平行容器安装命令

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询平行容器安装命令

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAgentDaemonSetCmd
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
IsCloud	是	否	Bool	**此参数对外不可见。** 是否是腾讯云
NetType	是	否	String	**此参数对外不可见。** 网络类型：basic-基础网络，private-VPC, public-公网，direct-专线
RegionCode	否	否	String	**此参数对外不可见。** 地域标示, NetType=direct时必填
VpcId	否	否	String	**此参数对外不可见。** VpcId, NetType=direct时必填
ExpireDate	否	否	String	**此参数对外不可见。** 命令有效期，非腾讯云时必填
ClusterCustomParameters	否	否	Array of ClusterCustomParameters	**此参数对外不可见。** 集群自定义参数

3. 输出参数

参数名称	类型	描述
Command	String	安装命令
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceInsufficient	
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询agent安装命令

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询agent安装命令

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAgentInstallCommand
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
IsCloud	是	否	Bool	是否是腾讯云
NetType	是	否	String	网络类型：basic-基础网络，private-VPC, public-公网，direct-专线
RegionCode	否	否	String	地域标示, NetType=direct时必填
VpcId	否	否	String	VpcId, NetType=direct时必填
ExpireDate	否	否	String	命令有效期，非腾讯云时必填
TagIds	否	否	Array of Uint64	标签ID列表，IsCloud=false时才会生效

3. 输出参数

参数名称	类型	描述
LinuxCommand	String	linux系统安装命令
WindowsCommand	String	windows系统安装命令（windows2008及以上）
WindowsStepOne	String	windows系统安装命令第一步（windows2003）
WindowsStepTwo	String	windows系统安装命令第二步（windows2003）
WindowsDownloadUrl	String	windows版agent下载链接
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询资产同步最近时间

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询资产同步最近时间

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-28 23:39:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetSyncLastTime
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AssetSyncLastTime	String	资产最近同步时间
TaskStatus	String	任务状态
PENDING:待处理		
PROCESSING:处理中		
PROCESSED:已完成		
TaskProcess	Int64	任务进度(百分比)
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询导出任务下载URL

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询导出任务下载URL

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeExportJobDownloadURL
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
JobID	是	否	String	任务ID

3. 输出参数

参数名称	类型	描述
DownloadURL	String	下载链接
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询导出任务管理列表

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询导出任务管理列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-12-28 16:08:09。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeExportJobManageList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	**此参数对外不可见。** 过滤条件。
ExportStatus- string -是否必填: 否 - 导出状态 RUNNING:导出中 SUCCESS:导出完成 FAILURE:失败				
ExportSource- string -是否必填: 否 - 导出来源 LocalImage:本地镜像 RegistryImage: 仓库镜像				
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Order	否	否	String	**此参数对外不可见。** 排序方式
By	否	否	String	**此参数对外不可见。** 排序字段 InsertTime: 创建时间

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	总数
List	ExportJobInfo	任务列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询检查报告

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询检查报告

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeInspectionReport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
ReportName	String	报告名称
ReportUrl	String	下载链接
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询促销活动

最近更新时间: 2024-09-03 18:49:47

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询促销活动

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribePromotionActivity
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ActiveID	是	否	Uint64	活动ID

3. 输出参数

参数名称	类型	描述
List	PromotionActivityContent	促销活动内容
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询容器安全概览信息

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询容器安全概览信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeTcssSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
ImageCnt	Uint64	镜像总数
ScannedImageCnt	Uint64	已扫描镜像数
UnScannedImageCnt	Uint64	待扫描镜像个数
LocalImageCnt	Uint64	本地镜像个数
RepositoryImageCnt	Uint64	仓库镜像个数
RiskLocalImageCnt	Uint64	风险本地镜像个数
RiskRepositoryImageCnt	Uint64	风险仓库镜像个数
ContainerCnt	Uint64	容器个数
RiskContainerCnt	Uint64	风险容器个数
ClusterCnt	Uint64	集群个数
RiskClusterCnt	Uint64	风险集群个数
UnScannedVulCnt	Uint64	待扫描漏洞个数
RiskVulCnt	Uint64	风险漏洞个数

参数名称	类型	描述
UnScannedBaseLineCnt	Uint64	安全基线待扫描项个数
RiskBaseLineCnt	Uint64	安全基线风险个数
RuntimeUnhandleEventCnt	Uint64	运行时(高危)待处理事件个数
UnScannedClusterCnt	Uint64	待扫描集群个数
ScanImageStatus	Bool	是否已扫描镜像
ScanClusterStatus	Bool	是否已扫描集群
ScanBaseLineStatus	Bool	是否已扫描基线
ScanVulStatus	Bool	是否已扫描漏洞
VulRiskImageCnt	Uint64	漏洞影响镜像数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询当天未授权核数趋势

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询当天未授权核数趋势

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeUnauthorizedCoresTendency
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
List	UnauthorizedCoresTendency	未授权核数趋势
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
FailedOperation	
UnknownParameter	

错误码	描述
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

隔离容器网络状态

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

隔离容器网络状态

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyContainerNetStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ContainerID	是	否	String	容器ID
Status	是	否	String	状态(隔离容器: EVENT_ISOLATE_CONTAINER 恢复容器: EVENT_RESOTRE_CONTAINER)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

运行时安全-反弹Shell相关接口
添加编辑反弹shell白名单

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

添加编辑运行时反弹shell白名单

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddEditReverseShellWhiteList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
WhiteListInfo	是	否	ReverseShellWhiteListInfo	增加或编辑白名单信息。新增白名单时WhiteListInfo.id为空，编辑白名单WhiteListInfo.id不能为空。
EventId	否	否	String	仅在添加事件白名单时候使用

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	

错误码	描述
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
FailedOperation.NotifyPolicyChangeFailed	
FailedOperation.RuleNameRepeat	
FailedOperation.RuleInfoRepeat	
FailedOperation.RuleSelectImageOutRange	
FailedOperation.RuleConfigTooMany	
InvalidParameter.RuleInfoInValid	
InvalidParameterValue.LengthLimit	
InvalidParameter.ReverShellKeyFieldAllEmpty	
InvalidParameter.ErrIpNoValid	
InvalidParameter.PortNoValid	

删除运行时反弹shell事件

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

删除运行时反弹shell事件

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteReverseShellEvents
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventIdSet	是	否	Array of String	事件ids

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

删除运行时反弹shell白名单

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

删除运行时反弹shell白名单

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteReverseShellWhiteLists
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
WhiteListIdSet	是	否	Array of String	白名单ids

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

运行时反弹shell事件详细信息

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时反弹shell事件详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-28 23:54:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeReverseShellDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventId	是	否	String	事件唯一id

3. 输出参数

参数名称	类型	描述
EventBaseInfo	RunTimeEventBaseInfo	事件基本信息
ProcessInfo	ProcessDetailInfo	进程信息
ParentProcessInfo	ProcessDetailBaseInfo	父进程信息
EventDetail	ReverseShellEventDescription	事件描述
AncestorProcessInfo	ProcessBaseInfo	祖先进程信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	

错误码	描述
InternalError	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InvalidParameterValue.DataNotFound	
FailedOperation.DataValueNotCorrect	

运行时反弹shell列表

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时反弹shell事件列表信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeReverseShellEvents
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	**此参数对外不可见。** 过滤参数
InnerNetAlarmShow- int - 是否必填：1 - 内网告警展示 0 - 不展示				
Order	否	否	String	**此参数对外不可见。** 升序降序,asc desc
By	否	否	String	**此参数对外不可见。** 排序字段

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	事件总数量
EventSet	ReverseShellEventInfo	反弹shell数组
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	

运行时反弹shell列表导出

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时反弹shell事件列表信息导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeReverseShellEventsExport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤参数,"Filters":[{"Name":"Status","Values":["2"]}]
Order	否	否	String	升序降序,asc desc
By	否	否	String	排序字段
ExportField	否	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	execle下载地址
JobId	String	任务ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

运行时反弹shell白名单详细信息

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时反弹shell白名单详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeReverseShellWhiteListDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
WhiteListId	是	否	String	白名单id

3. 输出参数

参数名称	类型	描述
WhiteListDetailInfo	ReverseShellWhiteListInfo	事件基本信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

错误码	描述
InvalidParameterValue.DataNotFound	
FailedOperation.DataValueNotCorrect	

运行时反弹shell白名单列表

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时运行时反弹shell白名单列表信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeReverseShellWhiteLists
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤参数,"Filters":[{"Name":"Status","Values":["2"]}]
Order	否	否	String	升序降序,asc desc
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	事件总数量
WhiteListSet	ReverseShellWhiteListBaseInfo	白名单信息列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

修改反弹shell事件状态

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改反弹shell事件的状态信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyReverseShellStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventIdSet	是	否	Array of String	处理事件ids
Status	是	否	String	标记事件的状态， EVENT_DEALED:事件处理 EVENT_INGNORE"：事件忽略 EVENT_DEL:事件删除 EVENT_ADD_WHITE:事件加白
Remark	否	否	String	事件备注

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InvalidParameterValue.DataNotFound	

运行时安全-容器逃逸相关接口
新增逃逸白名单

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

新增逃逸白名单

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddEscapeWhiteList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventType	是	否	Array of String	加白名单事件类型 ESCAPE_CGROUPS：利用cgroup机制逃逸 ESCAPE_TAMPER_SENSITIVE_FILE：篡改敏感文件逃逸 ESCAPE_DOCKER_API：访问Docker API接口逃逸 ESCAPE_VUL_OCCURRED：逃逸漏洞利用 MOUNT_SENSITIVE_PTAH：敏感路径挂载 PRIVILEGE_CONTAINER_START：特权容器 PRIVILEGE：程序提权逃逸
ImageIDs	是	否	Array of String	加白名单镜像ID数组

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

创建逃逸事件导出异步任务

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建逃逸事件导出异步任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateEscapeEventsExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，最大值为10000
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤参数,Status：EVENT_UNDEAL:未处理，EVENT_DEALED:已处理，EVENT_INGNORE:忽略
Order	否	否	String	升序降序,asc desc
By	否	否	String	排序字段：latest_found_time
ExportField	否	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	

创建逃逸白名单导出任务

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建逃逸白名单导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateEscapeWhiteListExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - EventType- String - 是否必填：否 - 加白事件类型，ESCAPE_CGROUPS：利用cgroup机制逃逸，ESCAPE_TAMPER_SENSITIVE_FILE：篡改敏感文件逃逸， ESCAPE_DOCKER_API：访问Docker API接口逃逸，ESCAPE_VUL_OCCURRED：逃逸漏洞利用，MOUNT_SENSITIVE_PTAH：敏感路径挂载，PRIVILEGE_CONTAINER_START：特权容器， PRIVILEGE：程序提权逃逸 - ImageName- string - 是否必填：否 - 镜像名称。 - ImageID- string - 是否必填：否 - 镜像ID。
Limit	否	否	Uint64	需要返回的数量，默认为10000，最大值为10000
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式：asc/desc
By	否	否	String	排序字段：主机数量：HostCount，容器数量：ContainerCount，更新时间：UpdateTime

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
FailedOperation	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

删除逃逸白名单

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

删除逃逸白名单

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteEscapeWhiteList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
IDSet	是	否	Array of Int64	白名单记录ID数组

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
FailedOperation	
UnknownParameter	

错误码	描述
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询容器逃逸事件详情

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

DescribeEscapeEventDetail 查询容器逃逸事件详情

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-28 23:54:29。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeEscapeEventDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventId	是	否	String	**此参数对外不可见。** 事件唯一id
EventType	否	否	String	**此参数对外不可见。** 事件类型

3. 输出参数

参数名称	类型	描述
EventBaseInfo	RunTimeEventBaseInfo	事件基本信息
ProcessInfo	ProcessDetailInfo	进程信息
EventDetail	EscapeEventDescription	事件描述
ParentProcessInfo	ProcessBaseInfo	父进程信息
AncestorProcessInfo	ProcessBaseInfo	祖先进程信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
AuthFailure	
InternalError	
InvalidParameter.MissingParameter	
InternalError.MainDBFail	

查询容器逃逸事件列表

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

DescribeEscapeEventInfo 查询容器逃逸事件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeEscapeEventInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。**需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。**偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	**此参数对外不可见。**过滤参数,
Status：状态(EVENT_UNDEAL:未处理，EVENT_DEALED:已处理，EVENT_INGNORE:忽略)				
EventType: 事件类型(MOUNT_SENSITIVE_PTAH:敏感路径挂载 PRIVILEGE_CONTAINER_START:特权容器 PRIVILEGE:提权事件				
ESCAPE_VUL_OCCURRED:逃逸漏洞利用 ESCAPE_DOCKER_API:访问Docker API接口逃逸 ESCAPE_TAMPER_SENSITIVE_FILE:篡改敏感文件逃逸 ESCAPE_CGROUPS:利用cgroup机制逃逸)				
ContainerNetStatus: 容器隔离状态 (NORMAL:正常 ISOLATED:已隔离 ISOLATE_FAILED:隔离失败 ISOLATE_FAILED:解除隔离失败 RESTORING:解除隔离中 ISOLATING:隔离中)				
ContainerStatus: 容器状态(CREATED:已创建 RUNNING:正常运行 PAUSED:暂停运行 STOPPED:停止运行 RESTARTING:重启中 REMOVING:迁移中 DEAD:DEAD UNKNOWN：未知 DESTROYED:已销毁)				

参数名称	必选	允许NULL	类型	描述
ForeignUniqueKey:镜像ID及事件类型唯一值				
Order	否	否	String	**此参数对外不可见。** 升序降序,asc desc
By	否	否	String	**此参数对外不可见。** 排序字段

3. 输出参数

参数名称	类型	描述
EventSet	EscapeEventInfo	逃逸事件数组
TotalCount	Uint64	事件总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询待处理逃逸事件趋势

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询待处理逃逸事件趋势

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeEscapeEventTendency
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EndTime	是	否	Date	结束时间
StartTime	是	否	Date	开始时间

3. 输出参数

参数名称	类型	描述
List	EscapeEventTendencyInfo	待处理逃逸事件趋势
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	

错误码	描述
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

统计容器逃逸各事件类型和待处理事件数

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

统计容器逃逸各事件类型和待处理事件数

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeEscapeEventTypeSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
ContainerEscapeEventCount	Int64	容器逃逸事件数
ProcessPrivilegeEventCount	Int64	程序提权事件数
RiskContainerEventCount	Int64	风险容器事件数
PendingEscapeEventCount	Int64	逃逸事件待处理数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceInsufficient	

错误码	描述
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	

查询容器逃逸事件列表导出

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

DescribeEscapeEventsExport 查询容器逃逸事件列表导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeEscapeEventsExport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤参数,"Filters":[{"Name":"Status","Values":["2"]}]
Order	否	否	String	升序降序,asc desc
By	否	否	String	排序字段
ExportField	是	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	execle下载地址
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
AuthFailure	

错误码	描述
InternalError	
ResourceNotFound	

查询容器逃逸扫描规则信息

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

DescribeEscapeRuleInfo 查询容器逃逸扫描规则信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeEscapeRuleInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
RuleSet	EscapeRule	规则信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
AuthFailure	
InternalError	

查询容器逃逸安全状态

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

DescribeEscapeSafeState 查询容器逃逸安全状态

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeEscapeSafeState
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
IsSafe	String	Unsafe：存在风险，Safe：暂无风险,UnKnown:未知风险
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
AuthFailure	
InternalError	

查询逃逸白名单

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询逃逸白名单

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeEscapeWhiteList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - EventType- String - 是否必填：否 - 加白事件类型，ESCAPE_CGROUPS：利用cgroup机制逃逸，ESCAPE_TAMPER_SENSITIVE_FILE：篡改敏感文件逃逸， ESCAPE_DOCKER_API：访问Docker API接口逃逸，ESCAPE_VUL_OCCURRED：逃逸漏洞利用，MOUNT_SENSITIVE_PTAH：敏感路径挂载，PRIVILEGE_CONTAINER_START：特权容器， PRIVILEGE：程序提权逃逸 - ImageName- string - 是否必填：否 - 镜像名称。 - ImageID- string - 是否必填：否 - 镜像ID。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式：asc/desc
By	否	否	String	排序字段：主机数量：HostCount，容器数量：ContainerCount，更新时间：UpdateTime

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	总数量
List	EscapeWhiteListInfo	逃逸白名单列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

修改容器逃逸扫描事件状态

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

ModifyEscapeEventStatus 修改容器逃逸扫描事件状态

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyEscapeEventStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventIdSet	是	否	Array of String	处理事件ids
Status	是	否	String	标记事件的状态： EVENT_UNDEAL:未处理（取消忽略）， EVENT_DEALED:已处理， EVENT_IGNORE:忽略， EVENT_DELETE：已删除 EVENT_ADD_WHITE：加白
Remark	否	否	String	备注
ImageIDs	否	否	Array of String	加白镜像ID数组
EventType	否	否	Array of String	加白事件类型 ESCAPE_CGROUPS：利用cgroup机制逃逸 ESCAPE_TAMPER_SENSITIVE_FILE：篡改敏感文件逃逸 ESCAPE_DOCKER_API：访问Docker API接口逃逸 ESCAPE_VUL_OCCURRED：逃逸漏洞利用 MOUNT_SENSITIVE_PTAH：敏感路径挂载 PRIVILEGE_CONTAINER_START：特权容器 PRIVILEGE：程序提权逃逸

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.InvalidFormat	

修改容器逃逸扫描规则信息

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

ModifyEscapeRule 修改容器逃逸扫描规则信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyEscapeRule
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleSet	是	否	Array of EscapeRuleEnabled	需要修改的数组

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameter.ParsingError	
FailedOperation.NotifyPolicyChangeFailed	

修改逃逸白名单

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改逃逸白名单

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyEscapeWhiteList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventType	是	否	Array of String	加白名单事件类型 ESCAPE_CGROUPS：利用cgroup机制逃逸 ESCAPE_TAMPER_SENSITIVE_FILE：篡改敏感文件逃逸 ESCAPE_DOCKER_API：访问Docker API接口逃逸 ESCAPE_VUL_OCCURRED：逃逸漏洞利用 MOUNT_SENSITIVE_PTAH：敏感路径挂载 PRIVILEGE_CONTAINER_START：特权容器 PRIVILEGE：程序提权逃逸
IDSet	是	否	Array of Int64	白名单记录ID

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	

错误码	描述
InternalError	
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

运行时安全-木马调用相关接口
运行时文件查杀重新检测

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时文件查杀重新检测

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateVirusScanAgain
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskId	是	否	String	任务id
ContainerIds	否	否	Array of String	需要扫描的容器id集合
TimeoutAll	否	否	Bool	是否是扫描全部超时的
Timeout	否	否	Uint64	重新设置的超时时长

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	

错误码	描述
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	
InvalidParameter.MissingParameter	

运行时文件查杀一键扫描

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时文件查杀一键扫描

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateVirusScanTask
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ScanPathAll	是	否	Bool	**此参数对外不可见。** 是否扫描所有路径
ScanPathType	否	否	Uint64	**此参数对外不可见。** 当ScanPathAll为false生效 0扫描以下路径 1、扫描除以下路径
ScanIds	否	否	Array of String	**此参数对外不可见。** 自选扫描范围的容器id或者主机id 根据ScanRangeType决定
ScanRangeType	是	否	Uint64	**此参数对外不可见。** 扫描范围0容器1主机节点
ScanRangeAll	是	否	Bool	**此参数对外不可见。** true 全选，false 自选
Timeout	是	否	Uint64	**此参数对外不可见。** 超时时长，单位小时
ScanPath	否	否	Array of String	**此参数对外不可见。** 自选排除或扫描的地址
ScanPathMode	否	否	String	**此参数对外不可见。** 扫描路径模式：
SCAN_PATH_ALL：全部路径				
SCAN_PATH_DEFAULT：默认路径				
SCAN_PATH_USER_DEFINE：用户自定义路径				

参数名称	必选	允许NULL	类型	描述

3. 输出参数

参数名称	类型	描述
TaskID	String	任务id
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InternalError.MainDBFail	

查询导出任务的结果

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询导出任务的结果

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeExportJobResult
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
JobId	是	否	String	CreateExportComplianceStatusListJob返回的JobId字段的值

3. 输出参数

参数名称	类型	描述
ExportStatus	String	导出的状态。取值为, SUCCESS:成功、FAILURE:失败，RUNNING: 进行中。
DownloadURL	String	返回下载URL
ExportProgress	Float	当ExportStatus为RUNNING时，返回导出进度。0~100范围的浮点数。
FailureMsg	String	失败原因
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
RequestLimitExceeded	
LimitExceeded	

错误码	描述
OperationDenied	
InvalidParameterValue	
FailedOperation	
InvalidParameterValue.DataNotFound	

查询木马自动隔离样本详情

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询木马自动隔离样本详情

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVirusAutoIsolateSampleDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
MD5	是	否	String	文件MD5值

3. 输出参数

参数名称	类型	描述
MD5	String	文件Md5值
Size	Uint64	文件大小(B)
VirusName	String	病毒名
RiskLevel	String	风险等级 RISK_CRITICAL, RISK_HIGH, RISK_MEDIUM, RISK_LOW, RISK_NOTICE。
KillEngine	String	查杀引擎
Tags	String	标签
HarmDescribe	String	事件描述
SuggestScheme	String	建议方案
ReferenceLink	String	参考链接
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询木马自动隔离样本下载链接

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询木马自动隔离样本下载链接

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVirusAutoIsolateSampleDownloadURL
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
MD5	是	否	String	样本Md5值

3. 输出参数

参数名称	类型	描述
FileUrl	String	样本下载链接
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询木马自动隔离样本列表

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询木马自动隔离样本列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVirusAutoIsolateSampleList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - MD5- String - 是否必填：否 - md5 - AutoIsolateSwitch- String - 是否必填：否 - 自动隔离开关 - VirusName- String - 是否必填：否 - 病毒名
By	否	否	String	排序字段
Order	否	否	String	排序方式

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	总数
List	VirusAutoIsolateSampleInfo	木马自动隔离样本列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
InternalError	

查询木马自动隔离设置

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询木马自动隔离设置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVirusAutoIsolateSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AutoIsolateSwitch	Bool	自动隔离开关(true:开 false:关)
IsKillProgress	Bool	是否中断隔离文件关联的进程(true:是 false:否)
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

运行时查询木马文件信息

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时查询木马文件信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-28 23:56:47。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVirusDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	String	**此参数对外不可见。** 木马文件id

3. 输出参数

参数名称	类型	描述
ImageId	String	镜像ID
ImageName	String	镜像名称
CreateTime	String	创建时间
Size	Uint64	木马文件大小
FilePath	String	木马文件路径
ModifyTime	String	最近生成时间
VirusName	String	病毒名称
RiskLevel	String	风险等级 RISK_CRITICAL, RISK_HIGH, RISK_MEDIUM, RISK_LOW, RISK_NOTICE。
ContainerName	String	容器名称
ContainerId	String	容器id
HostName	String	主机名称
HostId	String	主机id

参数名称	类型	描述
ProcessName	String	进程名称
ProcessPath	String	进程路径
ProcessMd5	String	进程md5
ProcessId	Uint64	进程id
ProcessArgv	String	进程参数
ProcessChan	String	进程链
ProcessAccountGroup	String	进程组
ProcessStartAccount	String	进程启动用户
ProcessFileAuthority	String	进程文件权限
SourceType	Int64	来源：0：一键扫描， 1：定时扫描 2：实时监控
Tags	String	标签
HarmDescribe	String	事件描述
SuggestScheme	String	建议方案
Mark	String	备注
FileName	String	风险文件名称
FileMd5	String	文件MD5
EventType	String	事件类型
PodName	String	集群名称
Status	String	DEAL_NONE:文件待处理 DEAL_IGNORE:已经忽略 DEAL_ADD_WHITELIST:加白 DEAL_DEL:文件已经删除 DEAL_ISOLATE:已经隔离 DEAL_ISOLATING:隔离中 DEAL_ISOLATE_FAILED:隔离失败 DEAL_RECOVERING:恢复中 DEAL_RECOVER_FAILED: 恢复失败
SubStatus	String	失败子状态: FILE_NOT_FOUND:文件不存在 FILE_ABNORMAL:文件异常 FILE_ABNORMAL_DEAL_RECOVER:恢复文件时，文件异常 BACKUP_FILE_NOT_FOUND:备份文件不存在 CONTAINER_NOT_FOUND_DEAL_ISOLATE:隔离时，容器不存在 CONTAINER_NOT_FOUND_DEAL_RECOVER:恢复时，容器不存在
HostIP	String	内网ip
ClientIP	String	外网ip
PProcessStartUser	String	父进程启动用户
PProcessUserGroup	String	父进程用户组
PProcessPath	String	父进程路径
PProcessParam	String	父进程命令行参数
AncestorProcessStartUser	String	祖先进程启动用户
AncestorProcessUserGroup	String	祖先进程用户组

参数名称	类型	描述
AncestorProcessPath	String	祖先进程路径
AncestorProcessParam	String	祖先进程命令行参数
OperationTime	String	事件最后一次处理的时间
ContainerNetStatus	String	容器隔离状态
ContainerNetSubStatus	String	容器隔离子状态
ContainerIsolateOperationSrc	String	容器隔离操作来源
CheckPlatform	String	检测平台 1: 云查杀引擎 2: tav 3: binaryAi 4: 异常行为 5: 威胁情报
FileAccessTime	String	文件访问时间
FileModifyTime	String	文件修改时间
NodeSubNetID	String	节点子网ID
NodeSubNetName	String	节点子网名称
NodeSubNetCIDR	String	节点子网网段
ClusterID	String	集群id
PodIP	String	pod ip
PodStatus	String	pod状态
NodeUniqueID	String	节点唯一ID
NodeType	String	节点类型：NORMAL普通节点、SUPER超级节点
NodeID	String	节点ID
ClusterName	String	集群名称
Namespace	String	Namespace
WorkloadType	String	工作负载类型
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InternalError.MainDBFail	

查询木马事件趋势

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询木马事件趋势

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVirusEventTendency
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
TendencyPeriod	是	否	Uint64	趋势周期(默认为7天)

3. 输出参数

参数名称	类型	描述
List	VirusTendencyInfo	趋势列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
InternalError.MainDBFail	

查询运行时文件查杀事件列表

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时文件查杀事件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVirusList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	**此参数对外不可见。** 过滤条件。 - FileName - String - 是否必填：否 - 文件名称 - FilePath - String - 是否必填：否 - 文件路径 - VirusName - String - 是否必填：否 - 病毒名称 - ContainerName- String - 是否必填：是 - 容器名称 - ContainerId- string - 是否必填：否 - 容器id - ImageName- string - 是否必填：否 - 镜像名称 - ImageId- string - 是否必填：否 - 镜像id - IsRealTime- int - 是否必填：否 - 过滤是否实时监控数据 - TaskId- string - 是否必填：否 - 任务ID - ContainerNetStatus - String -是否必填: 否 - 容器网络状态筛选 NORMAL ISOLATED ISOLATING RESTORING RESTORE_FAILED - TimeRange - string -是否必填: 否 - 时间范围筛选 ["2022-03-31 16:55:00", "2022-03-31 17:00:00"] - ContainerStatus - string -是否必填: 否 - 容器状态 RUNNING PAUSED STOPPED CREATED DESTROYED RESTARTING REMOVING - AutoIsolateMode - string -是否必填: 否 - 隔离方式 MANUAL AUTO - MD5 - string -是否必填: 否 - md5
Order	否	否	String	**此参数对外不可见。** 排序方式
By	否	否	String	**此参数对外不可见。** 排序字段

3. 输出参数

参数名称	类型	描述
List	VirusInfo	木马列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InternalError.MainDBFail	

查询木马一键检测预估超时时间

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询木马一键检测预估超时时间

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVirusManualScanEstimateTimeout
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ScanRangeType	是	否	Uint64	扫描范围0容器1主机节点
ScanRangeAll	是	否	Bool	true 全选，false 自选
ScanIds	否	否	Array of String	自选扫描范围的容器id或者主机id 根据ScanRangeType决定

3. 输出参数

参数名称	类型	描述
Timeout	Float	预估超时时间(h)
ContainerScanConcurrencyCount	Uint64	单台主机并行扫描容器数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

运行时查询文件查杀实时监控设置

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时查询文件查杀实时监控设置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVirusMonitorSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
EnableScan	Bool	是否开启实时监控
ScanPathAll	Bool	扫描全部路径
ScanPathType	Uint64	当ScanPathAll为true 生效 0扫描以下路径 1、扫描除以下路径
ScanPath	String	自选排除或扫描的地址
ScanPathMode	String	扫描路径模式：
SCAN_PATH_ALL：全部路径		
SCAN_PATH_DEFAULT：默认路径		
SCAN_PATH_USER_DEFINE：用户自定义路径		
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	

查询木马样本下载url

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询木马样本下载url

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVirusSampleDownloadUrl
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ID	是	否	String	木马id

3. 输出参数

参数名称	类型	描述
FileUrl	String	样本下载地址
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InternalError.MainDBFail	

运行时查询文件查杀设置

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时查询文件查杀设置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVirusScanSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
EnableScan	Bool	是否开启定期扫描
Cycle	Uint64	检测周期每隔多少天
BeginScanAt	String	扫描开始时间
ScanPathAll	Bool	扫描全部路径
ScanPathType	Uint64	当ScanPathAll为true 生效 0扫描以下路径 1、扫描除以下路径
Timeout	Uint64	超时时长，单位小时
ScanRangeType	Uint64	扫描范围0容器1主机节点
ScanRangeAll	Bool	true 全选，false 自选
ScanIds	String	自选扫描范围的容器id或者主机id 根据ScanRangeType决定
ScanPath	String	自选排除或扫描的地址
ClickTimeout	Uint64	一键检测的超时设置
ScanPathMode	String	扫描路径模式：
SCAN_PATH_ALL：全部路径		

参数名称	类型	描述
SCAN_PATH_DEFAULT：默认路径		
SCAN_PATH_USER_DEFINE：用户自定义路径		
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	

运行时查询文件查杀任务状态

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时查询文件查杀任务状态

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVirusScanTaskStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskID	否	否	String	任务id

3. 输出参数

参数名称	类型	描述
ContainerTotal	Uint64	查杀容器个数
RiskContainerCnt	Uint64	风险容器个数
Status	String	扫描状态 任务状态: SCAN_NONE:无， SCAN_SCANNING:正在扫描中， SCAN_FINISH：扫描完成， SCAN_TIMEOUT：扫描超时 SCAN_CANCELING: 取消中 SCAN_CANCELED:已取消
Schedule	Uint64	扫描进度 I
ContainerScanCnt	Uint64	已经扫描了的容器个数
RiskCnt	Uint64	风险个数
LeftSeconds	Uint64	剩余扫描时间
StartTime	String	扫描开始时间
EndTime	String	扫描结束时间
ScanType	String	扫描类型，"CYCLE"：周期扫描， "MANUAL"：手动扫描
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	

运行时文件扫描超时设置查询

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时文件扫描超时设置查询

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVirusScanTimeoutSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ScanType	是	否	Uint64	设置类型0一键检测，1定时检测

3. 输出参数

参数名称	类型	描述
Timeout	Uint64	超时时长单位小时
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError.MainDBFail	

运行时查询木马概览信息

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时查询木马概览信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVirusSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
TaskId	String	最近的一次扫描任务id
RiskContainerCnt	Uint64	木马影响容器个数
RiskCnt	Uint64	待处理风险个数
VirusDataBaseModifyTime	String	病毒库更新时间
RiskContainerIncrease	Int64	木马影响容器个数较昨日增长
RiskIncrease	Int64	待处理风险个数较昨日增长
IsolateIncrease	Int64	隔离事件个数较昨日新增
IsolateCnt	Int64	隔离事件总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InternalError.MainDBFail	

运行时查询文件查杀任务列表

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时查询文件查杀任务列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVirusTaskList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	**此参数对外不可见。** 过滤条件。 - ContainerName - String - 是否必填：否 - 容器名称 - ContainerId - String - 是否必填：否 - 容器id - Hostname - String - 是否必填：否 - 主机名称 - HostIp- String - 是否必填：否 - 主机IP - ImageId- String - 是否必填：否 - 镜像ID - ImageName- String - 是否必填：否 - 镜像名称 - Status- String - 是否必填：否 - 状态
TaskId	是	否	String	**此参数对外不可见。** 任务id
By	否	否	String	**此参数对外不可见。** 排序字段
Order	否	否	String	**此参数对外不可见。** 排序方式

3. 输出参数

参数名称	类型	描述
List	VirusTaskInfo	文件查杀列表
TotalCount	Uint64	总数量(容器任务数量)

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

运行时文件查杀事件列表导出

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时文件查杀事件列表导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportVirusList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - FileName - String - 是否必填：否 - 文件名称 - FilePath - String - 是否必填：否 - 文件路径 - VirusName - String - 是否必填：否 - 病毒名称 - ContainerName- String - 是否必填：是 - 容器名称 - ContainerId- string - 是否必填：否 - 容器id - ImageName- string - 是否必填：否 - 镜像名称 - ImageId- string - 是否必填：否 - 镜像id - IsRealTime- int - 是否必填：否 - 过滤是否实时监控数据 - TaskId- string - 是否必填：否 - 任务ID - TimeRange - string -是否必填: 否 - 时间范围筛选 ["2022-03-31 16:55:00", "2022-03-31 17:00:00"] - ContainerNetStatus - String -是否必填: 否 - 容器网络状态筛选 NORMAL ISOLATED ISOLATING RESTORING RESTORE_FAILED - ContainerStatus - string -是否必填: 否 - 容器状态 RUNNING PAUSED STOPPED CREATED DESTROYED RESTARTING REMOVING - AutoIsolateMode - string -是否必填: 否 - 隔离方式 MANUAL AUTO - MD5 - string -是否必填: 否 - md5
Order	否	否	String	排序方式
By	否	否	String	排序字段
ExportField	否	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	

修改木马自动隔离样本开关

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改木马自动隔离样本开关

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyVirusAutoIsolateExampleSwitch
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
MD5	是	否	String	文件Md5值
Status	是	否	Bool	开关(开:true 关: false)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

修改木马自动隔离设置

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改木马自动隔离设置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyVirusAutoIsolateSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
AutoIsolateSwitch	是	否	Bool	自动隔离开关(true:开 false:关)
IsKillProgress	是	否	Bool	是否中断隔离文件关联的进程(true:是 false:否)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

运行时更新木马文件事件状态

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时更新木马文件事件状态

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyVirusFileStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventIdSet	是	否	Array of String	处理事件id
Status	是	否	String	标记事件的状态， EVENT_DEALED:事件处理 EVENT_INGNORE"：事件忽略 EVENT_DEL:事件删除 EVENT_ADD_WHITE:事件加白 EVENT_PENDING: 事件待处理 EVENT_ISOLATE_CONTAINER: 隔离容器 EVENT_RESOTRE_CONTAINER: 恢复容器
Remark	否	否	String	事件备注
AutoIsolate	否	否	Bool	是否后续自动隔离相同MD5文件

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InvalidParameterValue.DataNotFound	

运行时更新文件查杀实时监控设置

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时更新文件查杀实时监控设置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyVirusMonitorSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EnableScan	是	否	Bool	**此参数对外不可见。** 是否开启定期扫描
ScanPathAll	是	否	Bool	**此参数对外不可见。** 扫描全部路径
ScanPathType	是	否	Uint64	**此参数对外不可见。** 当ScanPathAll为true 生效 0扫描以下路径 1、扫描除以下路径(扫描范围只能小于等于1)
ScanPath	否	否	Array of String	**此参数对外不可见。** 自选排除或扫描的地址
ScanPathMode	否	否	String	**此参数对外不可见。** 扫描路径模式：
SCAN_PATH_ALL：全部路径				
SCAN_PATH_DEFAULT：默认路径				
SCAN_PATH_USER_DEFINE：用户自定义路径				

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	

运行时更新文件查杀设置

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时更新文件查杀设置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyVirusScanSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EnableScan	是	否	Bool	**此参数对外不可见。** 是否开启定期扫描
Cycle	是	否	Uint64	**此参数对外不可见。** 检测周期每隔多少天(1|3|7)
BeginScanAt	是	否	String	**此参数对外不可见。** 扫描开始时间
ScanPathAll	是	否	Bool	**此参数对外不可见。** 扫描全部路径(true:全选,false:自选)
ScanPathType	是	否	Uint64	**此参数对外不可见。** 当ScanPathAll为true 生效 0扫描以下路径 1、扫描除以下路径
Timeout	是	否	Uint64	**此参数对外不可见。** 超时时长(5~24h)
ScanRangeType	是	否	Uint64	**此参数对外不可见。** 扫描范围0容器1主机节点
ScanRangeAll	是	否	Bool	**此参数对外不可见。** true 全选，false 自选
ScanIds	否	否	Array of String	**此参数对外不可见。** 自选扫描范围的容器id或者主机id 根据ScanRangeType决定
ScanPath	否	否	Array of String	**此参数对外不可见。** 扫描路径

参数名称	必选	允许NULL	类型	描述
ScanPathMode	否	否	String	**此参数对外不可见。** 扫描路径模式：
SCAN_PATH_ALL：全部路径				
SCAN_PATH_DEFAULT：默认路径				
SCAN_PATH_USER_DEFINE：用户自定义路径				

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

运行时文件扫描超时设置

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时文件扫描超时设置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyVirusScanTimeoutSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Timeout	是	否	Uint64	超时时长单位小时(5~24h)
ScanType	是	否	Uint64	设置类型0一键检测，1定时检测

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	

运行时停止木马查杀任务

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时停止木马查杀任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：StopVirusScanTask
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskId	是	否	String	任务ID
ContainerIds	否	否	Array of String	需要停止的容器id 为空默认停止整个任务

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

运行时安全-高危系统调用相关接口
创建异常进程规则导出任务

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建异常进程规则导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateAbnormalProcessRulesExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - RuleType - string - 是否必填: 否 -规则类型 - Status - string - 是否必填: 否 -状态
Order	否	否	String	排序方式
By	否	否	String	排序字段
ExportField	否	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
InternalError	

删除运行时高危系统调用事件

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

删除运行时高危系统调用事件

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteRiskSyscallEvents
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventIdSet	是	否	Array of String	事件ids

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

删除运行时高危系统调用白名单

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

删除运行时高危系统调用白名单

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteRiskSyscallWhiteLists
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
WhiteListIdSet	是	否	Array of String	白名单ids

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

运行时高危系统调用列表

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时运行时高危系统调用列表信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:15:12。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRiskSyscallEvents
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	**此参数对外不可见。** 过滤参数,"Filters":[{"Name":"Status","Values":["2"]}]
Order	否	否	String	**此参数对外不可见。** 升序降序,asc desc
By	否	否	String	**此参数对外不可见。** 排序字段

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	事件总数量
EventSet	RiskSyscallEventInfo	高危系统调用数组
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	

运行时高危系统调用列表导出

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

运行时高危系统调用列表导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRiskSyscallEventsExport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤参数,"Filters":[{"Name":"Status","Values":["2"]}]
Order	否	否	String	升序降序,asc desc
By	否	否	String	排序字段
ExportField	否	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	Excel下载地址
JobId	String	任务Id
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

运行时高危系统调用系统名称列表

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时高危系统调用系统名称列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRiskSyscallNames
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	事件总数量
SyscallNames	String	系统调用名称列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	

错误码	描述
InvalidParameter.InvalidFormat	

运行时高危系统调用白名单详细信息

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时高危系统调用白名单详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRiskSyscallWhiteListDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
WhiteListId	是	否	String	白名单id

3. 输出参数

参数名称	类型	描述
WhiteListDetailInfo	RiskSyscallWhiteListInfo	白名单基本信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

错误码	描述
InvalidParameterValue.DataNotFound	
FailedOperation.DataValueNotCorrect	

运行时高危系统调用白名单列表

最近更新时间: 2024-09-03 18:49:48

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时高危系统调用白名单列表信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRiskSyscallWhiteLists
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤参数,"Filters":[{"Name":"Status","Values":["2"]}]
Order	否	否	String	升序降序,asc desc
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	事件总数量
WhiteListSet	RiskSyscallWhiteListBaseInfo	白名单信息列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

修改高危系统调用事件状态

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改高危系统调用事件的状态信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyRiskSyscallStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventIdSet	是	否	Array of String	处理事件ids
Status	是	否	String	标记事件的状态， EVENT_DEALED:事件处理 EVENT_INGNORE"：事件忽略 EVENT_DEL:事件删除 EVENT_ADD_WHITE:事件加白
Remark	否	否	String	事件备注

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InvalidParameterValue.DataNotFound	

运行时安全相关接口
添加编辑异常进程策略

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

添加编辑运行时异常进程策略

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddEditAbnormalProcessRule
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleInfo	是	否	AbnormalProcessRuleInfo	增加策略信息，策略id为空，编辑策略是id不能为空
EventId	否	否	String	仅在加白的时候带上

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	

错误码	描述
FailedOperation	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
FailedOperation.NotifyPolicyChangeFailed	
FailedOperation.RuleNameRepeat	
FailedOperation.RuleInfoRepeat	
FailedOperation.RuleSelectImageOutRange	
FailedOperation.RuleConfigTooMany	
InvalidParameter.RuleInfoInValid	

添加编辑运行访问控制策略

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

添加编辑运行时访问控制策略

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddEditAccessControlRule
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleInfo	是	否	AccessControlRuleInfo	增加策略信息，策略id为空，编辑策略是id不能为空
EventId	否	否	String	仅在白名单时候使用

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	

错误码	描述
InvalidParameter.InvalidFormat	
FailedOperation.NotifyPolicyChangeFailed	
FailedOperation.RuleNameRepeat	
FailedOperation.RuleInfoRepeat	
FailedOperation.RuleSelectImageOutRange	
FailedOperation.RuleConfigTooMany	
InvalidParameter.RuleInfoInValid	

添加编辑高危系统调用白名单

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

添加编辑运行时高危系统调用白名单

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddEditRiskSyscallWhiteList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventId	否	否	String	仅在添加事件白名单时候使用
WhiteListInfo	否	否	RiskSyscallWhiteListInfo	增加或编辑白名单信。新增白名单时WhiteListInfo.id为空，编辑白名单WhiteListInfo.id不能为空.

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
InvalidParameter.MissingParameter	

错误码	描述
InvalidParameter.InvalidFormat	
FailedOperation.NotifyPolicyChangeFailed	
FailedOperation.RuleNameRepeat	
FailedOperation.RuleInfoRepeat	
FailedOperation.RuleSelectImageOutRange	
FailedOperation.RuleConfigTooMany	
InvalidParameter.RuleInfoInValid	
InvalidParameterValue.LengthLimit	

创建支持防御的漏洞导出任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建支持防御的漏洞导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateDefenceVulExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10000，最大值为10000
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - Level- String - 是否必填：否 - 威胁等级，CRITICAL:严重 HIGH:高/MIDDLE:中/LOW:低 - CVEID- string - 是否必填：否 - CVE编号 - Name- string -是否必填: 否 - 漏洞名称
Order	否	否	String	排序方式
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

创建应急漏洞导出任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建应急漏洞导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateEmergencyVulExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为50000，最大值为50000
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - Level- String - 是否必填：否 - 威胁等级，CRITICAL:严重 HIGH:高/MIDDLE:中/LOW:低 - Tags- string - 是否必填：否 - 漏洞标签，POC，EXP。 - CanBeFixed- string - 是否必填：否 - 是否可修复true,false。 - CVEID- string - 是否必填：否 - CVE编号 - ImageID- string - 是否必填：否 - 镜像ID - ImageName- String -是否必填: 否 - 镜像名称 - ContainerID- string -是否必填: 否 - 容器ID - ContainerName- string -是否必填: 否 - 容器名称 - ComponentName- string -是否必填: 否 - 组件名称 - ComponentVersion- string -是否必填: 否 - 组件版本 - Name- string -是否必填: 否 - 漏洞名称
Order	否	否	String	排序方式
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

创建异常进程事件导出异步任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建异常进程事件导出异步任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateProcessEventsExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，最大值为10000
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤参数,Status：EVENT_UNDEAL:未处理，EVENT_DEALED:已处理，EVENT_INGNORE:忽略
Order	否	否	String	升序降序,asc desc
By	否	否	String	排序字段：latest_found_time
ExportField	否	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	

创建恶意请求事件导出任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建恶意请求事件导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateRiskDnsEventExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - EventStatus- String - 是否必填：否 - 事件状态，待处理：EVENT_UNDEAL，EVENT_DEALED：已处理，已忽略：EVENT_IGNORE，EVENT_ADD_WHITE：已加白 - ContainerStatus- String - 是否必填：否 - 容器运行状态筛选，已创建：CREATED,正常运行：RUNNING, 暂定运行：PAUSED, 停止运行： STOPPED，重启中：RESTARTING, 迁移中：REMOVING, 销毁：DESTROYED - ContainerNetStatus- String -是否必填: 否 - 容器网络状态筛选 未隔离：NORMAL，已隔离：ISOLATED，隔离失败：ISOLATE_FAILED，解除隔离失败：RESTORE_FAILED，解除隔离中：RESTORING，隔离中：ISOLATING - EventType - String -是否必填: 否 - 事件类型，恶意域名请求：DOMAIN，恶意IP请求：IP - TimeRange- String -是否必填: 否 - 时间范围，第一个值表示开始时间，第二个值表示结束时间 - RiskDns- string - 是否必填：否 - 恶意域名。 - RiskIP- string - 是否必填：否 - 恶意IP。 - ContainerName- string - 是否必填：否 - 容器名称。 - ContainerID- string - 是否必填：否 - 容器ID。 - ImageName- string - 是否必填：否 - 镜像名称。 - ImageID- string - 是否必填：否 - 镜像ID。 - HostName- string - 是否必填：否 - 主机名称。 - HostIP- string - 是否必填：否 - 内网IP。 - PublicIP- string - 是否必填：否 - 外网IP。
Limit	否	否	Uint64	需要返回的数量，最大值为100000
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式：asc/desc
By	否	否	String	排序字段：事件数量：EventCount

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

创建系统漏洞导出任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建系统漏洞导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateSystemVulExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为50000，最大值为50000
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - OnlyAffectedContainer- string - 是否必填：否 - 仅展示影响容器的漏洞true,false - OnlyAffectedNewestImage-string - 是否必填：否 - 仅展示影响最新版本镜像的漏洞true,false - Level- String - 是否必填：否 - 威胁等级，CRITICAL:严重 HIGH:高/MIDDLE:中/LOW:低 - Tags- string - 是否必填：否 - 漏洞标签，POC，EXP。 - CanBeFixed- string - 是否必填：否 - 是否可修复true,false。 - CategoryType- string - 是否必填：否 - 漏洞子类型 - CVEID- string - 是否必填：否 - CVE编号 - ImageID- string - 是否必填：否 - 镜像ID - ImageName- String -是否必填: 否 - 镜像名称 - ContainerID- string -是否必填: 否 - 容器ID - ContainerName- string -是否必填: 否 - 容器名称 - ComponentName- string -是否必填: 否 - 组件名称 - ComponentVersion- string -是否必填: 否 - 组件版本 - Name- string -是否必填: 否 - 漏洞名称 - FocusOnType - string - 是否必填：否 -关注紧急度类型 。ALL :全部，SERIOUS_LEVEL： 严重和高危 ，IS_SUGGEST： 重点关注，POC_EXP 有Poc或Exp ，NETWORK_EXP: 远程Exp
Order	否	否	String	排序方式
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

创建受漏洞影响的容器导出任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建受漏洞影响的容器导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateVulContainerExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
PocID	是	否	String	漏洞PocID
Limit	否	否	Uint64	需要返回的数量，默认为50000，最大值为50000
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - OnlyAffectedNewestImage- Bool- 是否必填：否 - 仅展示影响最新版本镜像的漏洞 - ContainerID- string - 是否必填：否 - 容器ID - ContainerName- String -是否必填: 否 - 容器名称

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	

创建导出受漏洞影响的镜像任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建受漏洞影响的镜像导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateVulImageExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
PocID	是	否	String	漏洞PocID
Limit	否	否	Uint64	需要返回的数量，默认为50000，最大值为50000
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - OnlyAffectedNewestImage- Bool- 是否必填：否 - 仅展示影响最新版本镜像的漏洞 - ImageID- string - 是否必填：否 - 镜像ID - ImageName- String -是否必填: 否 - 镜像名称 - ClientIP- string -是否必填: 否 - 内网IP - PublicIP- string -是否必填: 否 - 外网IP - ComponentName- string -是否必填: 否 - 组件名称 - ComponentVersion- string -是否必填: 否 - 组件版本 - HostName- string -是否必填: 否 - 主机名称
Order	否	否	String	排序方式
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

创建漏洞扫描任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建漏洞扫描任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateVulScanTask
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
LocalImageScanType	否	否	String	本地镜像扫描范围类型。ALL:全部本地镜像，NOT_SCAN：全部已授权未扫描本地镜像，IMAGEIDS:自选本地镜像ID
LocalImageIDs	否	否	Array of String	根据已授权的本地镜像IDs扫描，优先权高于根据满足条件的已授权的本地镜像。
RegistryImageScanType	否	否	String	仓库镜像扫描范围类型。ALL:全部仓库镜像，NOT_SCAN：全部已授权未扫描仓库镜像，IMAGEIDS:自选仓库镜像ID
RegistryImageIDs	否	否	Array of Uint64	根据已授权的仓库镜像IDs扫描，优先权高于根据满足条件的已授权的仓库镜像。
LocalTaskID	否	否	Int64	本地镜像重新漏洞扫描时的任务ID
RegistryTaskID	否	否	Int64	仓库镜像重新漏洞扫描时的任务ID

3. 输出参数

参数名称	类型	描述
LocalTaskID	Int64	本地镜像重新漏洞扫描时的任务ID
RegistryTaskID	Int64	仓库镜像重新漏洞扫描时的任务ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
ResourceInUse	
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceUnavailable	
ResourceNotFound	
FailedOperation	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

创建web漏洞导出任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建web漏洞导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateWebVulExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为50000，最大值为50000
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - OnlyAffectedContainer- string - 是否必填：否 - 仅展示影响容器的漏洞true,false - OnlyAffectedNewestImage-string - 是否必填：否 - 仅展示影响最新版本镜像的漏洞true,false - Level- String - 是否必填：否 - 威胁等级，CRITICAL:严重 HIGH:高/MIDDLE:中/LOW:低 - Tags- string - 是否必填：否 - 漏洞标签，POC，EXP。 - CanBeFixed- string - 是否必填：否 - 是否可修复true,false。 - CategoryType- string - 是否必填：否 - 漏洞子类型 - CVEID- string - 是否必填：否 - CVE编号 - ImageID- string - 是否必填：否 - 镜像ID - ImageName- String -是否必填: 否 - 镜像名称 - ContainerID- string -是否必填: 否 - 容器ID - ContainerName- string -是否必填: 否 - 容器名称 - ComponentName- string -是否必填: 否 - 组件名称 - ComponentVersion- string -是否必填: 否 - 组件版本 - Name- string -是否必填: 否 - 漏洞名称 - FocusOnType - string - 是否必填：否 -关注紧急度类型 。ALL :全部，SERIOUS_LEVEL： 严重和高危 ，IS_SUGGEST： 重点关注，POC_EXP 有Poc或Exp ，NETWORK_EXP: 远程Exp
Order	否	否	String	排序方式
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

删除运行时异常进程策略

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

删除运行异常进程策略

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteAbnormalProcessRules
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleIdSet	是	否	Array of String	策略的ids

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

删除运行时访问控制策略

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

删除运行访问控制策略

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteAccessControlRules
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleIdSet	是	否	Array of String	策略的ids

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

运行时异常进程事件详细信息

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时异常进程事件详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-28 23:54:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAbnormalProcessDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventId	是	否	String	**此参数对外不可见。** 事件唯一id

3. 输出参数

参数名称	类型	描述
EventBaseInfo	RunTimeEventBaseInfo	事件基本信息
ProcessInfo	ProcessDetailInfo	进程信息
ParentProcessInfo	ProcessDetailBaseInfo	父进程信息
EventDetail	AbnormalProcessEventDescription	事件描述
AncestorProcessInfo	ProcessBaseInfo	祖先进程信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
FailedOperation.DataValueNotCorrect	

查询待处理异常进程事件趋势

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询待处理异常进程事件趋势

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAbnormalProcessEventTendency
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
StartTime	是	否	Date	开始时间
EndTime	是	否	Date	结束时间

3. 输出参数

参数名称	类型	描述
List	AbnormalProcessEventTendencyInfo	待处理异常进程事件趋势
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	

错误码	描述
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

运行时异常进程列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时异常进程事件列表信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:14:10。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAbnormalProcessEvents
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	**此参数对外不可见。** 过滤参数,"Filters":[{"Name":"Status","Values":["2"]}]
Order	否	否	String	**此参数对外不可见。** 升序降序,asc desc
By	否	否	String	**此参数对外不可见。** 排序字段

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	事件总数量
EventSet	AbnormalProcessEventInfo	异常进程数组
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

运行时异常进程列表导出

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时异常进程事件列表信息导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAbnormalProcessEventsExport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤参数,"Filters":[{"Name":"Status","Values":["2"]}]
Order	否	否	String	升序降序,asc desc
By	否	否	String	排序字段
ExportField	是	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	execle下载地址
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

统计异常进程各威胁等级待处理事件数

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

统计异常进程各威胁等级待处理事件数

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAbnormalProcessLevelSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
HighLevelEventCount	Int64	异常进程高危待处理事件数
MediumLevelEventCount	Int64	异常进程中危待处理事件数
LowLevelEventCount	Int64	异常进程低危待处理事件数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

错误码	描述
InvalidParameter.InvalidFormat	

查询运行时异常进程策略详细信息

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时异常策略详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAbnormalProcessRuleDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleId	否	否	String	策略唯一id
ImageId	否	否	String	镜像id, 在添加白名单的时候使用
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
RuleDetail	AbnormalProcessRuleInfo	异常进程策略详细信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
FailedOperation.RuleNotFind	

运行时异常进程策略列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时异常进程策略列表信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAbnormalProcessRules
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤参数,"Filters":[{"Name":"Status","Values":["2"]}]
Order	否	否	String	升序降序,asc desc
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	事件总数量
RuleSet	RuleBaseInfo	异常进程策略信息列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

运行时异常进程策略列表导出

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时异常进程策略列表信息导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAbnormalProcessRulesExport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤参数,"Filters":[{"Name":"Status","Values":["2"]}]
Order	否	否	String	升序降序,asc desc
By	否	否	String	排序字段
ExportField	是	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	execle下载地址
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

运行时访问控制事件详细信息

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时访问控制事件的详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-28 23:54:43。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAccessControlDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventId	是	否	String	**此参数对外不可见。** 事件唯一id

3. 输出参数

参数名称	类型	描述
EventBaseInfo	RunTimeEventBaseInfo	事件基本信息
ProcessInfo	ProcessDetailInfo	进程信息
TamperedFileInfo	FileAttributeInfo	被篡改信息
EventDetail	AccessControlEventDescription	事件描述
ParentProcessInfo	ProcessBaseInfo	父进程信息
AncestorProcessInfo	ProcessBaseInfo	祖先进程信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
FailedOperation	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
FailedOperation.DataValueNotCorrect	

运行时访问控制事件列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时访问控制事件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:13:50。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAccessControlEvents
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	**此参数对外不可见。** 过滤参数,"Filters":[{"Name":"Status","Values":["2"]}]
Order	否	否	String	**此参数对外不可见。** 升序降序,asc desc
By	否	否	String	**此参数对外不可见。** 排序字段

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	事件总数量
EventSet	AccessControlEventInfo	访问控制事件数组
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

运行时访问控制事件列表导出

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时访问控制事件列表导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAccessControlEventsExport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	**此参数对外不可见。** 过滤参数,"Filters":[{"Name":"Status","Values":["2"]}]
Order	否	否	String	**此参数对外不可见。** 升序降序,asc desc
By	否	否	String	**此参数对外不可见。** 排序字段
ExportField	否	否	Array of String	**此参数对外不可见。** 导出字段

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	execle下载地址
JobId	String	任务id
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询运行时访问控制策略详细信息

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时访问控制策略详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAccessControlRuleDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleId	否	否	String	策略唯一id
ImageId	否	否	String	镜像id, 仅仅在事件加白的时候使用
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
RuleDetail	AccessControlRuleInfo	运行时策略详细信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
FailedOperation.RuleNotFind	

运行时访问控制策略列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行访问控制策略列表信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAccessControlRules
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤参数,"Filters":[{"Name":"Status","Values":["2"]}]
Order	否	否	String	升序降序,asc desc
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	事件总数量
RuleSet	RuleBaseInfo	访问控制策略信息列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

运行时访问控制策略列表导出

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询运行时访问控制策略列表导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAccessControlRulesExport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤参数,"Filters":[{"Name":"Status","Values":["2"]}]
Order	否	否	String	升序降序,asc desc
By	否	否	String	排序字段
ExportField	是	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	execle下载地址
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

镜像绑定规则列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像绑定规则列表信息，包含运行时访问控制和异常进程公用

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageBindRuleInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤参数,"Filters":[{"Name":"EventType","Values":[""]}] EventType取值： "FILE_ABNORMAL_READ" 访问控制 "MALICE_PROCESS_START" 恶意进程启动
Order	否	否	String	升序降序,asc desc
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	事件总数量
ImageBindRuleSet	ImagesBindRuleInfo	镜像绑定规则列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询应急漏洞列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询应急漏洞列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:13:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeEmergencyVulList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - Level- String - 是否必填：否 - 威胁等级，CRITICAL:严重 HIGH:高/MIDDLE:中/LOW:低 - Tags- string - 是否必填：否 - 漏洞标签，POC，EXP。 - CanBeFixed- string - 是否必填：否 - 是否可修复true,false。 - CVEID- string - 是否必填：否 - CVE编号 - ImageID- string - 是否必填：否 - 镜像ID - ImageName- String -是否必填: 否 - 镜像名称 - ContainerID- string -是否必填: 否 - 容器ID - ContainerName- string -是否必填: 否 - 容器名称 - ComponentName- string -是否必填: 否 - 组件名称 - ComponentVersion- string -是否必填: 否 - 组件版本 - Name- string -是否必填: 否 - 漏洞名称
Order	否	否	String	排序方式
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	漏洞总数
List	EmergencyVulInfo	漏洞列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	

查询恶意请求事件详情

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询恶意请求事件详情

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-28 23:56:52。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRiskDnsEventDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventID	是	否	Uint64	**此参数对外不可见。** 事件ID

3. 输出参数

参数名称	类型	描述
EventID	Uint64	事件ID
EventType	String	事件类型，恶意域名请求：DOMAIN，恶意IP请求：IP
EventCount	Uint64	恶意请求次数
FoundTime	String	首次发现时间
LatestFoundTime	String	最近生成时间
ContainerID	String	容器ID
ContainerName	String	容器名称
ContainerNetStatus	String	隔离状态 未隔离 NORMAL 已隔离 ISOLATED 隔离中 ISOLATING 隔离失败 ISOLATE_FAILED 解除隔离中 RESTORING 解除隔离失败 RESTORE_FAILED
ContainerStatus	String	容器状态 正在运行: RUNNING 暂停: PAUSED 停止: STOPPED 已经创建: CREATED 已经销毁: DESTROYED 正在重启中: RESTARTING 迁移中: REMOVING

参数名称	类型	描述
ContainerNetSubStatus	String	容器子状态 "AGENT_OFFLINE" //Agent离线 "NODE_DESTROYED" //节点已销毁 "CONTAINER_EXITED" //容器已退出 "CONTAINER_DESTROYED" //容器已销毁 "SHARED_HOST" // 容器与主机共享网络 "RESOURCE_LIMIT" //隔离操作资源超限 "UNKNOW" // 原因未知
ContainerIsolateOperationSrc	String	容器隔离操作来源
ImageID	String	镜像ID
ImageName	String	镜像名称
HostName	String	主机名称
HostIP	String	内网IP
PublicIP	String	外网IP
PodName	String	节点名称
Description	String	事件描述
Solution	String	解决方案
Reference	String	参考链接
Address	String	恶意域名或IP
City	String	恶意IP所属城市
MatchRuleType	String	命中规则类型 SYSTEM：系统规则 USER：用户自定义
FeatureLabel	String	标签特征
ProcessAuthority	String	进程权限
ProcessMd5	String	进程md5
ProcessStartUser	String	进程启动用户
ProcessUserGroup	String	进程用户组
ProcessPath	String	进程路径
ProcessTree	String	进程树
ProcessParam	String	进程命令行参数
ParentProcessStartUser	String	父进程启动用户
ParentProcessUserGroup	String	父进程用户组
ParentProcessPath	String	父进程路径
ParentProcessParam	String	父进程命令行参数
AncestorProcessStartUser	String	祖先进程启动用户
AncestorProcessUserGroup	String	祖先进程用户组
AncestorProcessPath	String	祖先进程路径
AncestorProcessParam	String	祖先进程命令行参数

参数名称	类型	描述
HostID	String	主机ID
EventStatus	String	事件状态 EVENT_UNDEAL： 待处理 EVENT_DEALED：已处理 EVENT_IGNORE：已忽略 EVENT_ADD_WHITE：已加白
OperationTime	String	操作时间
Remark	String	备注
NodeType	String	节点类型
NodeName	String	节点名称
NodeSubNetID	String	节点子网ID
NodeSubNetName	String	节点子网名称
NodeSubNetCIDR	String	节点子网网段
ClusterID	String	集群ID
PodIP	String	podip
PodStatus	String	pod状态
NodeUniqueID	String	节点唯一id
NodeID	String	节点ID名称
ClusterName	String	集群名称
Namespace	String	Namespace
WorkloadType	String	工作负载类型
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	

错误码	描述
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询恶意请求事件列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询恶意请求事件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:13:27。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRiskDnsList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	**此参数对外不可见。** 过滤条件。 - EventStatus- String - 是否必填：否 - 事件状态，待处理：EVENT_UNDEAL，EVENT_DEALED：已处理，已忽略：EVENT_IGNORE，EVENT_ADD_WHITE：已加白 - ContainerStatus- String - 是否必填：否 - 容器运行状态筛选，已创建：CREATED,正常运行：RUNNING, 暂定运行：PAUSED, 停止运行： STOPPED，重启中：RESTARTING, 迁移中：REMOVING, 销毁：DESTROYED - ContainerNetStatus- String -是否必填: 否 - 容器网络状态筛选 未隔离：NORMAL，已隔离：ISOLATED，隔离失败：ISOLATE_FAILED，解除隔离失败：RESTORE_FAILED，解除隔离中：RESTORING，隔离中：ISOLATING - EventType - String -是否必填: 否 - 事件类型，恶意域名请求：DOMAIN，恶意IP请求：IP - TimeRange- String -是否必填: 否 - 时间范围，第一个值表示开始时间，第二个值表示结束时间 - RiskDns- string - 是否必填：否 - 恶意域名。 - RiskIP- string - 是否必填：否 - 恶意IP。 - ContainerName- string - 是否必填：否 - 容器名称。 - ContainerID- string - 是否必填：否 - 容器ID。 - ImageName- string - 是否必填：否 - 镜像名称。 - ImageID- string - 是否必填：否 - 镜像ID。 - HostName- string - 是否必填：否 - 主机名称。 - HostIP- string - 是否必填：否 - 内网IP。 - PublicIP- string - 是否必填：否 - 外网IP。
Order	否	否	String	**此参数对外不可见。** 排序方式：asc/desc
By	否	否	String	**此参数对外不可见。** 排序字段：告警数量：EventCount，最近生成时间：LatestFoundTime

3. 输出参数

参数名称	类型	描述
List	RiskDnsEventInfo	恶意请求事件列表
TotalCount	Int64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

运行时高危系统调用事件详细信息

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询高危系统调用事件详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-28 23:56:56。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRiskSyscallDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventId	是	否	String	**此参数对外不可见。** 事件唯一id

3. 输出参数

参数名称	类型	描述
EventBaseInfo	RunTimeEventBaseInfo	事件基本信息
ProcessInfo	ProcessDetailInfo	进程信息
ParentProcessInfo	ProcessDetailBaseInfo	父进程信息
EventDetail	RiskSyscallEventDescription	事件描述
AncestorProcessInfo	ProcessBaseInfo	祖先进程信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InvalidParameterValue.DataNotFound	
FailedOperation.DataValueNotCorrect	

查询支持防御的漏洞列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询支持防御的漏洞列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSupportDefenceVul
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - Level- String - 是否必填：否 - 威胁等级，CRITICAL:严重 HIGH:高/MIDDLE:中/LOW:低 - CVEID- string - 是否必填：否 - CVE编号 - Name- string -是否必填: 否 - 漏洞名称
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式：asc/desc
By	否	否	String	排序字段：披露时间：SubmitTime

3. 输出参数

参数名称	类型	描述
List	SupportDefenceVul	支持防御的漏洞列表
TotalCount	Int64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询受漏洞的容器列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询受漏洞的容器列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:13:19。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulContainerList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
PocID	是	否	String	漏洞PocID
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - OnlyAffectedNewestImage- Bool- 是否必填：否 - 仅展示影响最新版本镜像的漏洞 - ContainerID- string - 是否必填：否 - 容器ID - ContainerName- String -是否必填: 否 - 容器名称

3. 输出参数

参数名称	类型	描述
List	VulAffectedContainerInfo	容器列表
TotalCount	Int64	容器总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询漏洞详情

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞详情

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
PocID	是	否	String	漏洞PocID

3. 输出参数

参数名称	类型	描述
VulInfo	VulDetailInfo	漏洞详情信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

错误码	描述
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	

查询漏洞影响的镜像列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞影响的镜像列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulImageList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
PocID	是	否	String	漏洞PocID
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - OnlyAffectedNewestImage- Bool- 是否必填：否 - 仅展示影响最新版本镜像的漏洞 - ImageID- string - 是否必填：否 - 镜像ID - ImageName- String -是否必填: 否 - 镜像名称 - HostIP- string -是否必填: 否 - 内网IP - PublicIP- string -是否必填: 否 - 外网IP - ComponentName- string -是否必填: 否 - 组件名称 - ComponentVersion- string -是否必填: 否 - 组件版本 - HostName- string -是否必填: 否 - 主机名称
Order	否	否	String	排序方式
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
List	VulAffectedImageInfo	受影响的镜像列表
TotalCount	Int64	镜像总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询漏洞扫描任务信息

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞扫描任务信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:13:11。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulScanInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
LocalTaskID	否	否	Int64	本地镜像漏洞扫描任务ID，无则返回最近一次的漏洞任务扫描
RegistryTaskID	否	否	Int64	仓库镜像漏洞扫描任务ID，无则返回最近一次的漏洞任务扫描

3. 输出参数

参数名称	类型	描述
LocalImageScanCount	Int64	本次扫描的本地镜像总数
IgnoreVulCount	Int64	忽略的漏洞数量
ScanStartTime	String	漏洞扫描的开始时间
ScanEndTime	String	漏洞扫描的结束时间
FoundRiskImageCount	Int64	发现风险镜像数量
FoundVulCount	Int64	本地发现漏洞数量
ScanProgress	Float	扫描进度
RegistryImageScanCount	Int64	本次扫描的仓库镜像总数
LocalTaskID	Int64	本地镜像最近一次的漏洞任务扫描ID
Status	String	扫描状态:NOT_SCAN:未扫描，SCANNING:扫描中,SCANNED:完成，CANCELED：扫描停止
RemainingTime	Float	剩余时间，秒

参数名称	类型	描述
RegistryTaskID	Int64	仓库镜像最近一次的漏洞任务扫描ID
RegistryFoundVulCount	Int64	仓库发现漏洞数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	

查询漏洞扫描任务的本地镜像列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞扫描任务的本地镜像列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulScanLocalImageList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskID	是	否	Int64	漏洞扫描任务ID
Filters	否	否	Array of RunTimeFilters	过滤条件。 - OnlyAffectedNewestImage- Bool- 是否必填：否 - 仅展示影响最新版本镜像的漏洞 - ImageID- string - 是否必填：否 - 镜像ID - ImageName- String -是否必填: 否 - 镜像名称 - ScanStatus- string - 是否必填: 否 - 检测状态。WAIT_SCAN：待检测，SCANNING：检查中，SCANNED：检查完成，SCAN_ERR：检查失败，CANCELED：检测停止
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	镜像总数
List	VulScanImageInfo	镜像列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	

查询web应用漏洞列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询web应用漏洞列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:13:05。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeWebVulList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - OnlyAffectedContainer- string - 是否必填：否 - 仅展示影响容器的漏洞true,false - OnlyAffectedNewestImage-string - 是否必填：否 - 仅展示影响最新版本镜像的漏洞true,false - Level- String - 是否必填：否 - 威胁等级，CRITICAL:严重 HIGH:高/MIDDLE:中/LOW:低 - Tags- string - 是否必填：否 - 漏洞标签，POC，EXP。 - CanBeFixed- string - 是否必填：否 - 是否可修复true,false。 - CVEID- string - 是否必填：否 - CVE编号 - ImageID- string - 是否必填：否 - 镜像ID - ImageName- String -是否必填: 否 - 镜像名称 - ContainerID- string -是否必填: 否 - 容器ID - ContainerName- string -是否必填: 否 - 容器名称 - ComponentName- string -是否必填: 否 - 组件名称 - ComponentVersion- string -是否必填: 否 - 组件版本 - Name- string -是否必填: 否 - 漏洞名称 - FocusOnType - string - 是否必填：否 -关注紧急度类型 。ALL :全部，SERIOUS_LEVEL： 严重和高危 ，IS_SUGGEST： 重点关注，POC_EXP 有Poc或Exp ，NETWORK_EXP: 远程Exp
Order	否	否	String	排序方式
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	漏洞总数

参数名称	类型	描述
List	VulInfo	漏洞列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	

修改运行时异常进程策略状态

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改运行时异常进程策略的开启关闭状态

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyAbnormalProcessRuleStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleIdSet	是	否	Array of String	策略的ids
IsEnable	是	否	Bool	策略开关，true开启，false关闭

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	

错误码	描述
InvalidParameter.InvalidFormat	

修改异常进程事件状态

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改异常进程事件的状态信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyAbnormalProcessStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventIdSet	是	否	Array of String	处理事件ids
Status	是	否	String	标记事件的状态， EVENT_DEALED:事件处理 EVENT_INGNORE"：事件忽略 EVENT_DEL:事件删除 EVENT_ADD_WHITE:事件加白
Remark	否	否	String	事件备注

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

修改运行时访问控制策略状态

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改运行时访问控制策略的状态，启用或者禁用

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyAccessControlRuleStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleIdSet	是	否	Array of String	策略的ids
IsEnable	是	否	Bool	策略开关，true:代表开启， false代表关闭

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	

错误码	描述
InvalidParameter.InvalidFormat	

修改运行时访问控制事件状态

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改运行时访问控制事件状态信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyAccessControlStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventIdSet	是	否	Array of String	处理事件ids
Status	是	否	String	标记事件的状态， EVENT_DEALED:事件已经处理 EVENT_INGNORE：事件忽略 EVENT_DEL:事件删除 EVENT_ADD_WHITE:事件加白
Remark	否	否	String	备注事件信息

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

开通容器安全服务试用

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

开通容器安全服务试用

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:23:21。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：OpenTcssTrial
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
EndTime	String	试用开通结束时间
StartTime	String	试用开通开始时间
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
FailedOperation	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	

停止漏洞扫描任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

停止漏洞扫描任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：StopVulScanTask
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
LocalTaskID	否	否	Int64	本地镜像漏洞扫描任务ID
LocalImageIDs	否	否	Array of String	本地镜像ID，无则全部
RegistryImageIDs	否	否	Array of Uint64	仓库镜像ID，无则全部
RegistryTaskID	否	否	Int64	仓库镜像漏洞扫描任务ID

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
FailedOperation	

镜像安全相关接口
新增单个镜像仓库详细信息

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

新增单个镜像仓库详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-20 15:12:21。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddAssetImageRegistryRegistryDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Name	是	否	String	**此参数对外不可见。** 仓库名
Username	是	否	String	**此参数对外不可见。** 用户名
Password	是	否	String	**此参数对外不可见。** 密码
Url	是	否	String	**此参数对外不可见。** 仓库url
RegistryType	是	否	String	**此参数对外不可见。** 仓库类型，列表：harbor
RegistryVersion	否	否	String	**此参数对外不可见。** 仓库版本
NetType	是	否	String	**此参数对外不可见。** 网络类型，列表：public（公网）
RegistryRegion	否	否	String	**此参数对外不可见。** 区域，列表：default（默认）
SpeedLimit	否	否	Int64	**此参数对外不可见。** 限速
Insecure	否	否	Uint64	**此参数对外不可见。** 安全模式（证书校验）：0（默认） 非安全模式（跳过证书校验）：1

参数名称	必选	允许NULL	类型	描述
ConnDetectConfig	否	否	Array of ConnDetectConfig	**此参数对外不可见。** 联通性检测的记录ID
NeedScan	否	否	Bool	**此参数对外不可见。** “授权&扫描"开关

3. 输出参数

参数名称	类型	描述
HealthCheckErr	String	连接错误信息
NameRepeatErr	String	名称错误信息
RegistryId	Int64	仓库唯一id
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
FailedOperation	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
FailedOperation.DataValueNotCorrect	

新增或编辑本地镜像自动授权规则

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

新增或编辑本地镜像自动授权规则

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-20 15:34:10。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddEditImageAutoAuthorizedRule
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RangeType	是	否	String	**此参数对外不可见。** 授权范围类别，MANUAL:自选主机节点，ALL:全部镜像
HostIdSet	否	否	Array of String	**此参数对外不可见。** 自选主机id，当授权范围为MANUAL:自选主机时且HostIdFilters为空时，必填
MaxDailyCount	是	否	Int64	**此参数对外不可见。** 每天最大的镜像授权数限制, 0表示无限制
RuleId	否	否	Int64	**此参数对外不可见。** 规则id，在编辑时，必填
HostIdFilters	否	否	Array of AssetFilters	**此参数对外不可见。** 根据条件过滤，当授权范围为MANUAL:自选主机时且HostIdSet为空时，必填
ExcludeHostIdSet	否	否	Array of String	**此参数对外不可见。** 根据条件过滤而且排除指定主机id
IsEnabled	是	否	Int64	**此参数对外不可见。** 规则是否生效，0:不生效，1:已生效
AutoScanEnabled	否	否	Int64	**此参数对外不可见。** 自动扫描开关
ScanType	否	否	Array of String	**此参数对外不可见。** 自动扫描范围

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
FailedOperation	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
FailedOperation.ErrRuleNotFind	
FailedOperation.RuleNotFind	
InternalError.MainDBFail	

新增漏洞扫描忽略漏洞

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

新增漏洞扫描忽略漏洞

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddIgnoreVul
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
List	是	否	Array of ModifyIgnoreVul	漏洞PocID信息列表

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
FailedOperation	

错误码	描述
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

检查单个镜像仓库名是否重复

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

检查单个镜像仓库名是否重复

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CheckRepeatAssetImageRegistry
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Name	是	否	String	仓库名

3. 输出参数

参数名称	类型	描述
IsRepeat	Bool	是否重复
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
FailedOperation	

错误码	描述
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
FailedOperation.DataValueNotCorrect	

镜像仓库创建镜像扫描任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库创建镜像扫描任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateAssetImageRegistryScanTask
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
All	否	否	Bool	**此参数对外不可见。** 是否扫描全部镜像
Images	否	否	Array of ImageInfo	**此参数对外不可见。** 扫描的镜像列表
ScanType	否	否	Array of String	**此参数对外不可见。** 扫描类型数组
Id	否	否	Array of Uint64	**此参数对外不可见。** 扫描的镜像列表
Filters	否	否	Array of AssetFilters	**此参数对外不可见。** 过滤条件
ExcludeImageList	否	否	Array of Uint64	**此参数对外不可见。** 不需要扫描的镜像列表, 与Filters配合使用
OnlyScanLatest	否	否	Bool	**此参数对外不可见。** 是否仅扫描各repository最新版的镜像, 与Filters配合使用

3. 输出参数

参数名称	类型	描述
TaskID	Uint64	返回的任务ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
ResourceNotFound	
FailedOperation	

镜像仓库创建镜像一键扫描任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库创建镜像一键扫描任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateAssetImageRegistryScanTaskOneKey
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
All	否	否	Bool	**此参数对外不可见。** 是否扫描全部镜像(废弃)
Images	否	否	Array of ImageInfo	**此参数对外不可见。** 扫描的镜像列表
ScanType	否	否	Array of String	**此参数对外不可见。** 扫描类型数组
Id	否	否	Array of Uint64	**此参数对外不可见。** 扫描的镜像列表Id
IsLatest	否	否	Bool	**此参数对外不可见。** 是否最新镜像
ScanScope	否	否	Uint64	**此参数对外不可见。** 扫描范围 0全部镜像，1自选镜像，2推荐扫描镜像
RegistryType	否	否	Array of String	**此参数对外不可见。** 仓库类型
Namespace	否	否	Array of String	**此参数对外不可见。** 命名空间
ContainerRunning	否	否	Bool	**此参数对外不可见。** 是否存在运行中的容器
Timeout	否	否	Uint64	**此参数对外不可见。** 任务超时时长单位s

3. 输出参数

参数名称	类型	描述
TaskID	Uint64	扫描任务id
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
ResourceNotFound	
FailedOperation	

创建镜像扫描任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全创建镜像扫描任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-20 15:12:59。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateAssetImageScanTask
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
All	否	否	Bool	**此参数对外不可见。** 是否扫描全部镜像；全部镜像，镜像列表和根据过滤条件筛选三选一。
Images	否	否	Array of String	**此参数对外不可见。** 需要扫描的镜像列表；全部镜像，镜像列表和根据过滤条件筛选三选一。
ScanVul	否	否	Bool	**此参数对外不可见。** 扫描漏洞；漏洞，木马和风险需选其一
ScanVirus	否	否	Bool	**此参数对外不可见。** 扫描木马；漏洞，木马和风险需选其一
ScanRisk	否	否	Bool	**此参数对外不可见。** 扫描风险；漏洞，木马和风险需选其一
Filters	否	否	Array of AssetFilters	**此参数对外不可见。** 根据过滤条件筛选出镜像；全部镜像，镜像列表和根据过滤条件筛选三选一。
ExcludeImageIds	否	否	Array of String	**此参数对外不可见。** 根据过滤条件筛选出镜像，再排除个别镜像
ContainerRunning	否	否	Bool	**此参数对外不可见。** 镜像是否存在运行中的容器
ScanScope	否	否	Uint64	**此参数对外不可见。** 扫描范围 0 全部授权镜像，1自选镜像，2 推荐扫描
Timeout	否	否	Uint64	**此参数对外不可见。** 任务超时时长单位秒，默认1小时

3. 输出参数

参数名称	类型	描述
TaskID	String	任务id
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	
FailedOperation.ErrAlreadyScanning	

查询本地镜像组件列表导出

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询本地镜像组件列表导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateComponentExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10000，最大值为10000
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 - ComponentName- String - 是否必填：否 - 镜像组件名称 - ComponentVersion- String - 是否必填：否 - 镜像组件版本 - ComponentType- String - 是否必填：否 - 镜像组件类型 - VulLevel- String - 是否必填：否 - 漏洞威胁等级 - HasVul- String - 是否必填：否 -是否有漏洞；true：是，false，否；不传或ALL ：全部
ImageID	是	否	String	镜像ID
By	否	否	String	排序字段
Order	否	否	String	排序方式desc ，asc
ExportField	是	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	

创建镜像导出任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建镜像导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateImageExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - ImageName- String - 是否必填：否 - 镜像名称筛选， - ScanStatus - String - 是否必填：否 - 镜像扫描状态notScan，scanning，scanned，scanErr - ImageID- String - 是否必填：否 - 镜像ID筛选， - SecurityRisk- String - 是否必填：否 - 安全风险，VulCnt 、VirusCnt、RiskCnt、IsTrustImage
Offset	否	否	Uint64	偏移量，默认为0。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
By	否	否	String	排序字段
Order	否	否	String	排序方式 asc,desc
ExportField	否	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
DownloadUrl	String	excel文件下载地址
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

创建或者编辑弹性计费上限

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

CreateOrModifyPostPayCores 创建或者编辑弹性计费上限

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateOrModifyPostPayCores
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
CoresCnt	是	否	Uint64	弹性计费上限，最小值500

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
InternalError.MainDBFail	

创建漏洞防御导出任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建漏洞防御导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateVulDefenceEventExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - Status- String - 是否必填：否 - 插件状态，待处理：EVENT_UNDEAL，EVENT_DEALED：已处理，已忽略：EVENT_IGNORE，EVENT_DEFENDED：已防御 - ContainerStatus- String - 是否必填：否 - 容器运行状态筛选，已创建：CREATED,正常运行：RUNNING, 暂定运行：PAUSED, 停止运行： STOPPED，重启中：RESTARTING, 迁移中：REMOVING, 销毁：DESTROYED - ContainerNetStatus- String -是否必填: 否 - 容器网络状态筛选 未隔离：NORMAL，已隔离：ISOLATED，隔离失败：ISOLATE_FAILED，解除隔离失败：RESTORE_FAILED，解除隔离中：RESTORING，隔离中：ISOLATING - EventType - String -是否必填: 否 - 入侵状态，防御成功：EVENT_DEFENDED，尝试攻击：EVENT_ATTACK - TimeRange- String -是否必填: 否 - 时间范围，第一个值表示开始时间，第二个值表示结束时间 - VulName- string - 是否必填：否 - 漏洞名称。 - CVEID- string - 是否必填：否 - CVE编号。 - SourceIP- string - 是否必填：否 - 攻击源IP。 - ContainerName- string - 是否必填：否 - 容器名称。 - ContainerID- string - 是否必填：否 - 容器ID。 - ImageName- string - 是否必填：否 - 镜像名称。 - ImageID- string - 是否必填：否 - 镜像ID。 - HostName- string - 是否必填：否 - 主机名称。 - HostIP- string - 是否必填：否 - 内网IP。
Limit	否	否	Uint64	需要返回的数量，最大值为100000
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式：asc/desc
By	否	否	String	排序字段：事件数量：EventCount

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

创建漏洞防御主机导出任务

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建漏洞防御主机导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateVulDefenceHostExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - Status- String - 是否必填：否 - 插件状态，正常：SUCCESS，异常：FAIL， NO_DEFENCE:未防御 - KeyWords- string - 是否必填：否 - 主机名称/IP。
Limit	否	否	Uint64	需要返回的数量，最大值为100000
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式：asc/desc
By	否	否	String	排序字段：更新时间：ModifyTime/首次开启时间：CreateTime

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceInsufficient	
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询本地镜像漏洞列表导出

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询本地镜像漏洞列表导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateVulExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10000，最大值为10000
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 - ComponentName- String - 是否必填：否 - 镜像组件名称 - ComponentVersion- String - 是否必填：否 - 镜像组件版本 - ComponentType- String - 是否必填：否 - 镜像组件类型 - VulLevel- String - 是否必填：否 - 漏洞威胁等级 - HasVul- String - 是否必填：否 -是否有漏洞；true：是，false，否；不传或ALL ：全部
ImageID	是	否	String	镜像ID
By	否	否	String	排序字段
Order	否	否	String	排序方式desc ，asc
ExportField	是	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	

取消漏洞扫描忽略漏洞

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

取消漏洞扫描忽略漏洞

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteIgnoreVul
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
List	是	否	Array of ModifyIgnoreVul	漏洞PocID 信息列表

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
FailedOperation	

错误码	描述
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询app服务列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全查询app服务列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:12:07。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetAppServiceList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of AssetFilters	**此参数对外不可见。** 过滤条件。 Keywords- String - 是否必填：否 - 模糊查询可选字段

3. 输出参数

参数名称	类型	描述
List	ServiceInfo	db服务列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询容器组件列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全搜索查询容器组件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetComponentList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件
ContainerID	是	否	String	容器id

3. 输出参数

参数名称	类型	描述
List	ComponentInfo	组件列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

错误码	描述
ResourceNotFound	
InvalidParameter.ParsingError	

查询容器信息

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询容器详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetContainerDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ContainerId	是	否	String	**此参数对外不可见。** 容器id

3. 输出参数

参数名称	类型	描述
HostID	String	主机id
HostIP	String	主机ip
ContainerName	String	容器名称
Status	String	运行状态
RunAs	String	运行账户
Cmd	String	命令行
CPUUsage	Uint64	CPU使用率 * 1000
RamUsage	Uint64	内存使用 KB
ImageName	String	镜像名
ImageID	String	镜像ID
POD	String	归属POD
K8sMaster	String	k8s 主节点

参数名称	类型	描述
ProcessCnt	Uint64	容器内进程数
PortCnt	Uint64	容器内端口数
ComponentCnt	Uint64	组件数
AppCnt	Uint64	app数
WebServiceCnt	Uint64	websvc数
Mounts	ContainerMount	挂载
Network	ContainerNetwork	容器网络信息
CreateTime	String	创建时间
ImageCreateTime	String	镜像创建时间
ImageSize	Uint64	镜像大小
HostStatus	String	主机状态 offline,online,pause
NetStatus	String	网络状态 未隔离 NORMAL 已隔离 ISOLATED 隔离中 ISOLATING 隔离失败 ISOLATE_FAILED 解除隔离中 RESTORING 解除隔离失败 RESTORE_FAILED
NetSubStatus	String	网络子状态
IsolateSource	String	隔离来源
IsolateTime	String	隔离时间
NodeID	String	节点ID
NodeName	String	节点名称
NodeSubNetID	String	节点子网ID
NodeSubNetName	String	节点子网名称
NodeSubNetCIDR	String	节点子网网段
PodName	String	pod名称
PodIP	String	pod ip
PodStatus	String	pod状态
ClusterID	String	集群ID
ClusterName	String	集群名称
NodeType	String	节点类型:NORMAL: 普通节点(默认值) SUPER: 超级节点
NodeUniqueID	String	超级节点唯一id
PublicIP	String	外网ip
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询容器列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

搜索查询容器列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetContainerList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。**需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。**偏移量，默认为0。
Filters	否	否	Array of AssetFilters	**此参数对外不可见。**过滤条件。
ContainerName - String - 是否必填：否 - 容器名称模糊搜索				
Status - String - 是否必填：否 - 容器运行状态筛选，0："created",1："running", 2："paused", 3："restarting", 4："removing", 5："exited", 6："dead"				
Runas - String - 是否必填：否 - 运行用户筛选				
ImageName- String - 是否必填：否 - 镜像名称搜索				
HostIP- string - 是否必填：否 - 主机ip搜索				
OrderBy - String 是否必填：否 -排序字段，支持：cpu_usage, mem_usage的动态排序 ["cpu_usage","+"] '+'升序、'-'降序				
NetStatus - String -是否必填: 否 - 容器网络状态筛选 normal isolated isolating isolate_failed restoring restore_failed				
PodID - String -是否必填: 否 - PodID筛选				

参数名称	必选	允许NULL	类型	描述
NodeUniqueID - String -是否必填: 否 - SuperNode筛选				
PodUid - String -是否必填: 否 - Pod筛选				
PodIP - String -是否必填: 否 - PodIP筛选				
NodeType - String -是否必填: 否 - 节点类型筛选:NORMAL:普通节点;SUPER:超级节点				
By	否	否	String	**此参数对外不可见。** 排序字段
Order	否	否	String	**此参数对外不可见。** 排序方式 asc,desc

3. 输出参数

参数名称	类型	描述
List	ContainerInfo	容器列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询db服务列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全查询db服务列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetDBServiceList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of AssetFilters	**此参数对外不可见。** 过滤条件。 Keywords- String - 是否必填：否 - 模糊查询可选字段

3. 输出参数

参数名称	类型	描述
List	ServiceInfo	db服务列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询主机信息

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询主机详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetHostDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
HostId	是	否	String	**此参数对外不可见。** 主机id

3. 输出参数

参数名称	类型	描述
UUID	String	容器安全uuid
UpdateTime	String	更新时间
HostName	String	主机名
Group	String	主机分组
HostIP	String	主机IP
OsName	String	操作系统
AgentVersion	String	agent版本
KernelVersion	String	内核版本
DockerVersion	String	docker版本
DockerAPIVersion	String	docker api版本
DockerGoVersion	String	docker go 版本
DockerFileSystemDriver	String	docker 文件系统类型

参数名称	类型	描述
DockerRootDir	String	docker root 目录
ImageCnt	Uint64	镜像数
ContainerCnt	Uint64	容器数
K8sMasterIP	String	k8s IP
K8sVersion	String	k8s version
KubeProxyVersion	String	kube proxy
Status	String	"UNINSTALL"："未安装","OFFLINE"："离线", "ONLINE"："防护中
IsContainerd	Bool	是否Containerd
MachineType	String	主机来源;"TENCENTCLOUD":"腾讯云服务器","OTHERCLOUD":"非腾讯云服务器"
PublicIp	String	外网ip
InstanceID	String	主机实例ID
RegionID	Int64	地域ID
Project	ProjectInfo	所属项目
Tags	TagInfo	标签
ClusterID	String	集群ID
ClusterName	String	集群名称
ClusterAccessedStatus	String	集群接入状态
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询主机列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全搜索查询主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-12-28 16:09:40。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetHostList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of AssetFilters	**此参数对外不可见。** 过滤条件。 - Status - String - 是否必填：否 - agent状态筛选，"ALL":"全部"(或不传该字段),"UNINSTALL"："未安装","OFFLINE"："离线", "ONLINE"："防护中" - HostName - String - 是否必填：否 - 主机名筛选 - Group- String - 是否必填：否 - 主机群组搜索 - HostIP- string - 是否必填：否 - 主机ip搜索 - HostID- string - 是否必填：否 - 主机id搜索 - DockerVersion- string - 是否必填：否 - docker版本搜索 - MachineType- string - 是否必填：否 - 主机来源MachineType搜索，"ALL":"全部"(或不传该字段),主机来源：["CVM", "ECM", "LH", "BM"]中的之一为腾讯云服务器；["Other"]之一非腾讯云服务器； - DockerStatus- string - 是否必填：否 - docker安装状态，"ALL":"全部"(或不传该字段),"INSTALL":"已安装","UNINSTALL":"未安装" - ProjectID- string - 是否必填：否 - 所属项目id搜索 - Tag:xxx(tag:key)- string- 是否必填：否 - 标签键值搜索 示例Filters": [{"Name":"tag:tke-kind","Values":["service"]}]
By	否	否	String	**此参数对外不可见。** 排序字段
Order	否	否	String	**此参数对外不可见。** 排序方式 asc,desc

3. 输出参数

参数名称	类型	描述
List	HostInfo	主机列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询镜像信息

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询镜像详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-20 19:28:07。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ImageID	是	否	String	**此参数对外不可见。** 镜像id

3. 输出参数

参数名称	类型	描述
ImageID	String	镜像ID
ImageName	String	镜像名称
ImageDigest	String	镜像摘要
CreateTime	String	创建时间
Size	Uint64	镜像大小
HostCnt	Uint64	关联主机个数
ContainerCnt	Uint64	关联容器个数
ScanTime	String	最近扫描时间
VulCnt	Uint64	漏洞个数
RiskCnt	Uint64	风险行为数
SensitiveInfoCnt	Uint64	敏感信息数
IsTrustImage	Bool	是否信任镜像

参数名称	类型	描述
OsName	String	镜像系统
AgentError	String	agent镜像扫描错误
ScanError	String	后端镜像扫描错误
Architecture	String	系统架构
Author	String	作者
BuildHistory	String	构建历史
ScanVirusProgress	Uint64	木马扫描进度
ScanVulProgress	Uint64	漏洞扫进度
ScanRiskProgress	Uint64	敏感信息扫描进度
ScanVirusError	String	木马扫描错误
ScanVulError	String	漏洞扫描错误
ScanRiskError	String	敏感信息错误
ScanStatus	String	镜像扫描状态
VirusCnt	Uint64	木马病毒数
Status	Uint64	镜像扫描状态
RemainScanTime	Uint64	剩余扫描时间
IsAuthorized	Int64	授权为：1，未授权为：0
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InternalError.MainDBFail	

查询镜像关联主机

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全查询镜像关联主机

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageHostList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of AssetFilters	过滤条件 支持ImageID,HostID

3. 输出参数

参数名称	类型	描述
List	ImageHost	镜像列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询镜像列表

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全搜索查询镜像列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-21 20:43:53。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 - ImageName- String - 是否必填：否 - 镜像名称筛选， - ScanStatus - String - 是否必填：否 - 镜像扫描状态notScan，scanning，scanned，scanErr - ImageID- String - 是否必填：否 - 镜像ID筛选， - SecurityRisk- String - 是否必填：否 - 安全风险，VulCnt 、VirusCnt、RiskCnt、IsTrustImage
By	否	否	String	排序字段
Order	否	否	String	排序方式 asc,desc

3. 输出参数

参数名称	类型	描述
List	ImagesInfo	镜像列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询镜像列表导出

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全搜索查询镜像列表导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageListExport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 - ImageName- String - 是否必填：否 - 镜像名称筛选， - ScanStatus - String - 是否必填：否 - 镜像扫描状态notScan，scanning，scanned，scanErr - ImageID- String - 是否必填：否 - 镜像ID筛选， - SecurityRisk- String - 是否必填：否 - 安全风险，VulCnt 、VirusCnt、RiskCnt、IsTrustImage
By	否	否	String	排序字段
Order	否	否	String	排序方式 asc,desc
ExportField	是	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	excel文件下载地址
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查看镜像仓库资产更新进度状态

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查看镜像仓库资产更新进度状态

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRegistryAssetStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
Status	String	更新进度状态,doing更新中，success更新成功，failed失败
Err	String	错误信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

镜像仓库查询镜像仓库详情

最近更新时间: 2024-09-03 18:49:49

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库镜像仓库列表详情

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRegistryDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	否	否	Uint64	**此参数对外不可见。** 仓库列表id
ImageId	否	否	String	**此参数对外不可见。** 镜像ID

3. 输出参数

参数名称	类型	描述
ImageDigest	String	镜像Digest
ImageRepoAddress	String	镜像地址
RegistryType	String	镜像类型
ImageName	String	仓库名称
ImageTag	String	镜像版本
ScanTime	String	扫描时间
ScanStatus	String	扫描状态
VulCnt	Uint64	安全漏洞数
VirusCnt	Uint64	木马病毒数
RiskCnt	Uint64	风险行为数

参数名称	类型	描述
SentiveInfoCnt	Uint64	敏感信息数
IsTrustImage	Bool	是否可信镜像
OsName	String	镜像系统
ScanVirusError	String	木马扫描错误
ScanVulError	String	漏洞扫描错误
LayerInfo	String	层文件信息
InstanceId	String	实例id
InstanceName	String	实例名称
Namespace	String	命名空间
ScanRiskError	String	高危扫描错误
ScanVirusProgress	Uint64	木马信息扫描进度
ScanVulProgress	Uint64	漏洞扫描进度
ScanRiskProgress	Uint64	敏感扫描进度
ScanRemainTime	Uint64	剩余扫描时间秒
CveStatus	String	cve扫描状态
RiskStatus	String	高危扫描状态
VirusStatus	String	木马扫描状态
Progress	Uint64	总进度
IsAuthorized	Uint64	授权状态
ImageSize	Uint64	镜像大小
ImageId	String	镜像Id
RegistryRegion	String	镜像区域
ImageCreateTime	Datetime_iso	镜像创建的时间
SensitiveInfoCnt	Uint64	敏感信息数
Id	Uint64	Id
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
ResourceNotFound	

镜像仓库查询镜像仓库列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库镜像仓库列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-14 02:25:08。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRegistryList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0
Filters	否	否	Array of AssetFilters	**此参数对外不可见。** 过滤字段 IsAuthorized是否授权，取值全部all，未授权0，已授权1
By	否	否	String	**此参数对外不可见。** 排序字段
Order	否	否	String	**此参数对外不可见。** 排序方式，asc，desc
OnlyShowLatest	否	否	Bool	**此参数对外不可见。** 是否仅展示各repository最新的镜像, 默认为false
IsRunning	否	否	Bool	**此参数对外不可见。** 是否仅展示运行中容器镜像

3. 输出参数

参数名称	类型	描述
List	ImageRepoInfo	镜像仓库列表
TotalCount	Uint64	总数量

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
ResourceNotFound	
FailedOperation	

镜像仓库镜像列表导出

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库镜像列表导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-12-28 16:09:52。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRegistryListExport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0
Filters	否	否	Array of AssetFilters	**此参数对外不可见。** 排序字段
By	否	否	String	**此参数对外不可见。** 排序字段
Order	否	否	String	**此参数对外不可见。** 排序方式，asc，desc
ExportField	是	否	Array of String	**此参数对外不可见。** 导出字段
OnlyShowLatest	否	否	Bool	**此参数对外不可见。** 是否仅展示repository版本最新的镜像，默认为false

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	excel文件下载地址
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
ResourceNotFound	

查看单个镜像仓库详细信息

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查看单个镜像仓库详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRegistryRegistryDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RegistryId	是	否	Int64	**此参数对外不可见。** 仓库唯一id

3. 输出参数

参数名称	类型	描述
Name	String	仓库名
Username	String	用户名
Password	String	密码
Url	String	仓库url
RegistryType	String	仓库类型，列表：harbor
RegistryVersion	String	仓库版本
NetType	String	网络类型，列表：public（公网）,private（私网）
RegistryRegion	String	区域，列表:default（默认）
SpeedLimit	Uint64	限速
Insecure	Uint64	安全模式（证书校验）：0（默认） 非安全模式（跳过证书校验）：1
ConnDetectDetail	RegistryConnDetectResult	联通性检测结果详情
InstanceID	String	tcr情况下instance_id

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
FailedOperation	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
FailedOperation.DataValueNotCorrect	

镜像仓库仓库列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库仓库列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRegistryRegistryList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0
Filters	否	否	Array of AssetFilters	**此参数对外不可见。** 过滤字段 IsAuthorized是否授权，取值全部all，未授权0，已授权1
By	否	否	String	**此参数对外不可见。** 排序字段
Order	否	否	String	**此参数对外不可见。** 排序方式，asc，desc

3. 输出参数

参数名称	类型	描述
List	ImageRepoRegistryInfo	镜像仓库列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
ResourceNotFound	

镜像仓库查询镜像高危行为列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库查询镜像高危行为列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRegistryRiskInfoList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 - Level- String - 是否必填：否 - 漏洞级别筛选， - Name - String - 是否必填：否 - 漏洞名称
ImageInfo	否	否	ImageInfo	镜像id
By	否	否	String	排序字段（Level）
Order	否	否	String	排序方式 + -
Id	否	否	Uint64	镜像标识Id

3. 输出参数

参数名称	类型	描述
List	ImageRisk	镜像漏洞列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
ResourceNotFound	
FailedOperation	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

镜像仓库敏感信息列表导出

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库敏感信息列表导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRegistryRiskListExport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 - Level- String - 是否必填：否 - 漏洞级别筛选， - Name - String - 是否必填：否 - 漏洞名称
ImageInfo	否	否	ImageInfo	镜像信息
By	否	否	String	**此参数对外不可见。** 排序字段（Level）
Order	否	否	String	**此参数对外不可见。** 排序方式 + -
ExportField	是	否	Array of String	导出字段
Id	否	否	Uint64	镜像标识Id

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	excel文件下载地址
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
ResourceNotFound	

镜像仓库查询一键镜像扫描状态

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库查询一键镜像扫描状态

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRegistryScanStatusOneKey
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Images	否	否	Array of ImageInfo	**此参数对外不可见。** 需要获取进度的镜像列表
All	否	否	Bool	**此参数对外不可见。** 是否获取全部镜像
Id	否	否	Array of Uint64	**此参数对外不可见。** 需要获取进度的镜像列表Id
TaskID	否	否	Uint64	**此参数对外不可见。** 获取进度的任务ID

3. 输出参数

参数名称	类型	描述
ImageTotal	Uint64	镜像个数
ImageScanCnt	Uint64	扫描镜像个数
ImageStatus	ImageProgress	扫描进度列表
SuccessCount	Uint64	安全个数
RiskCount	Uint64	风险个数
Schedule	Uint64	总的扫描进度
Status	String	总的扫描状态

参数名称	类型	描述
ScanRemainTime	Uint64	扫描剩余时间
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InternalError	
ResourceNotFound	

镜像仓库查询镜像统计信息

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库查询镜像统计信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-20 15:34:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRegistrySummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of AssetFilters	**此参数对外不可见。** 过滤字段

3. 输出参数

参数名称	类型	描述
ImageCnt	Uint64	镜像个数
ImageHasRiskInfoCnt	Uint64	有风险的镜像个数
ImageHasVirusCnt	Uint64	有病毒的镜像个数
ImageHasVulsCnt	Uint64	有漏洞的镜像个数
ImageUntrustCnt	Uint64	不受信任的镜像个数
LatestImageScanTime	String	最近镜像扫描时间
ImageUnsafeCnt	Uint64	风险镜像个数
RegistryTypeStat	ImageRegistryTypeCount	仓库类型数量分布
ScannedImageCnt	Uint64	已扫描镜像个数
RecommendedFixImageCnt	Uint64	推荐处置镜像个数
TodayUnsafeImageCnt	Uint64	今日新增风险镜像个数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
ResourceNotFound	

镜像仓库查询木马病毒列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库查询木马病毒列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRegistryVirusList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 - Level- String - 是否必填：否 - 漏洞级别筛选， - Name - String - 是否必填：否 - 漏洞名称
ImageInfo	否	否	ImageInfo	镜像信息
By	否	否	String	**此参数对外不可见。** 排序字段（Level）
Order	否	否	String	**此参数对外不可见。** 排序方式 + -
Id	否	否	Uint64	镜像标识Id

3. 输出参数

参数名称	类型	描述
List	ImageVirus	镜像漏洞列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
ResourceNotFound	

镜像仓库木马信息列表导出

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库木马信息列表导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRegistryVirusListExport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 - Level- String - 是否必填：否 - 漏洞级别筛选， - Name - String - 是否必填：否 - 漏洞名称
ImageInfo	否	否	ImageInfo	镜像信息
By	否	否	String	**此参数对外不可见。** 排序字段（Level）
Order	否	否	String	**此参数对外不可见。** 排序方式 + -
ExportField	是	否	Array of String	导出字段
Id	否	否	Uint64	镜像标识Id

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	excel文件下载地址
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
ResourceNotFound	

镜像仓库查询镜像漏洞列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库查询镜像漏洞列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRegistryVulList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 - Level- String - 是否必填：否 - 漏洞级别筛选， - Name - String - 是否必填：否 - 漏洞名称
ImageInfo	否	否	ImageInfo	镜像信息
By	否	否	String	**此参数对外不可见。** 排序字段（Level）
Order	否	否	String	**此参数对外不可见。** 排序方式 + -
Id	否	否	Uint64	镜像标识Id

3. 输出参数

参数名称	类型	描述
List	ImageVul	镜像漏洞列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
ResourceNotFound	
FailedOperation	

镜像仓库漏洞列表导出

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库漏洞列表导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:10:59。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRegistryVulListExport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 - Level- String - 是否必填：否 - 漏洞级别筛选， - Name - String - 是否必填：否 - 漏洞名称
ImageInfo	否	否	ImageInfo	镜像信息
By	否	否	String	**此参数对外不可见。** 排序字段（Level）
Order	否	否	String	**此参数对外不可见。** 排序方式 + -
ExportField	是	否	Array of String	导出字段
Id	否	否	Uint64	镜像标识Id

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	excel文件下载地址
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
ResourceNotFound	

查询镜像风险列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全查询镜像风险列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRiskList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 - Level- String - 是否必填：否 - 风险级别 1,2,3,4， - Behavior - String - 是否必填：否 - 风险行为 1,2,3,4 - Type - String - 是否必填：否 - 风险类型 1,2,
ImageID	是	否	String	镜像id
By	否	否	String	排序字段
Order	否	否	String	排序方式

3. 输出参数

参数名称	类型	描述
List	ImageRiskInfo	镜像病毒列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

镜像风险列表导出

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全搜索查询镜像风险列表导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageRiskListExport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of AssetFilters	过滤条件。 - Level- String - 是否必填：否 - 风险级别 1,2,3,4， - Behavior - String - 是否必填：否 - 风险行为 1,2,3,4 - Type - String - 是否必填：否 - 风险类型 1,2,
ExportField	是	否	Array of String	导出字段
ImageID	是	否	String	镜像id

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	excel文件下载地址
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

错误码	描述
ResourceNotFound	
InvalidParameter.ParsingError	

获取镜像扫描设置信息

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

获取镜像扫描设置信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-20 15:47:07。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageScanSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
Enable	Bool	开关
ScanTime	String	扫描时刻(完整时间;后端按0时区解析时分秒)
ScanPeriod	Uint64	扫描间隔
ScanVirus	Bool	扫描木马
ScanRisk	Bool	扫描敏感信息
ScanVul	Bool	扫描漏洞
All	Bool	扫描全部镜像
Images	String	自定义扫描镜像
ContainerRunning	Bool	镜像是否存在运行中的容器
ScanScope	Uint64	扫描范围 0 全部授权镜像，1自选镜像，2 推荐扫描
ScanEndTime	String	扫描结束时间 02:00 时分
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
InvalidParameter.MissingParameter	

查询镜像扫描状态

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全查询镜像扫描状态

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageScanStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskID	否	否	String	任务id

3. 输出参数

参数名称	类型	描述
ImageTotal	Uint64	镜像个数
ImageScanCnt	Uint64	扫描镜像个数
Status	String	扫描状态
Schedule	Uint64	扫描进度 ImageScanCnt/ImageTotal *100
SuccessCount	Uint64	安全个数
RiskCount	Uint64	风险个数
LeftSeconds	Uint64	剩余扫描时间
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	

查询正在一键扫描的镜像扫描taskid

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询正在一键扫描的镜像扫描taskid

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-20 15:50:53。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageScanTask
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
TaskID	String	任务id
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询镜像简略信息列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全搜索查询镜像简略信息列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageSimpleList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 Keywords- String - 是否必填：否 - 镜像名、镜像id 称筛选，
By	否	否	String	排序字段
Order	否	否	String	排序方式 asc,desc

3. 输出参数

参数名称	类型	描述
List	AssetSimpleImageInfo	镜像列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询镜像病毒列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全查询镜像病毒列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageVirusList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 - Name- String - 是否必填：否 - 镜像名称筛选， - RiskLevel - String - 是否必填：否 - 风险等级 1,2,3,4
ImageID	是	否	String	镜像id
Order	否	否	String	排序 asc desc
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
List	ImageVirusInfo	镜像病毒列表
TotalCount	Uint64	总数量
VirusScanStatus	Uint64	病毒扫描状态 0:未扫描 1:扫描中 2:扫描完成 3:扫描出错 4:扫描取消
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

镜像木马列表导出

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全搜索查询镜像木马列表导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageVirusListExport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of AssetFilters	过滤条件。 - Name- String - 是否必填：否 - 镜像名称筛选， - RiskLevel - String - 是否必填：否 - 风险等级 1,2,3,4
ExportField	是	否	Array of String	列表支持字段
ImageID	是	否	String	镜像id

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	excel文件下载地址
JobId	String	任务ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

错误码	描述
ResourceNotFound	
InvalidParameter.ParsingError	

查询镜像漏洞列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全查询镜像漏洞列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageVulList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 - Name- String - 是否必填：否 - 漏洞名称名称筛选， - Level - String - 是否必填：否 - 风险等级 1,2,3,4
ImageID	是	否	String	镜像id
By	否	否	String	排序字段（Level）
Order	否	否	String	排序方式 + -

3. 输出参数

参数名称	类型	描述
List	ImagesVul	镜像漏洞列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

镜像漏洞列表导出

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全搜索查询镜像漏洞列表导出

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetImageVulListExport
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 - Name- String - 是否必填：否 - 漏洞名称名称筛选， - Level - String - 是否必填：否 - 风险等级 1,2,3,4
ExportField	是	否	Array of String	导出字段
ImageID	是	否	String	镜像id

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	excel文件下载地址
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询端口占用列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全搜索查询端口占用列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetPortList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of AssetFilters	**此参数对外不可见。** 过滤条件。 - All - String - 是否必填：否 - 模糊查询可选字段 - RunAs - String - 是否必填：否 - 运行用户筛选， - ContainerID - String - 是否必填：否 - 容器id - HostID- String - 是否必填：是 - 主机id - HostIP- string - 是否必填：否 - 主机ip搜索 - ProcessName- string - 是否必填：否 - 进程名搜索

3. 输出参数

参数名称	类型	描述
List	PortInfo	端口列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询进程列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全搜索查询进程列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetProcessList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of AssetFilters	**此参数对外不可见。** 过滤条件。 - RunAs - String - 是否必填：否 - 运行用户筛选， - ContainerID - String - 是否必填：否 - 容器id - HostID- String - 是否必填：是 - 主机id - HostIP- string - 是否必填：否 - 主机ip搜索 - ProcessName- string - 是否必填：否 - 进程名搜索 - Pid- string - 是否必填：否 - 进程id搜索(关联进程)

3. 输出参数

参数名称	类型	描述
List	ProcessInfo	端口列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询账户容器、镜像等统计信息

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询账户容器、镜像等统计信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-20 15:33:50。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AppCnt	Uint64	应用个数
ContainerCnt	Uint64	容器个数
ContainerPause	Uint64	暂停的容器个数
ContainerRunning	Uint64	运行的容器个数
ContainerStop	Uint64	停止运行的容器个数
CreateTime	String	创建时间
DbCnt	Uint64	数据库个数
ImageCnt	Uint64	镜像个数
HostOnline	Uint64	主机在线个数
HostCnt	Uint64	主机个数
ImageHasRiskInfoCnt	Uint64	有风险的镜像个数
ImageHasVirusCnt	Uint64	有病毒的镜像个数
ImageHasVulsCnt	Uint64	有漏洞的镜像个数

参数名称	类型	描述
ImageUntrustCnt	Uint64	不受信任的镜像个数
ListenPortCnt	Uint64	监听的端口个数
ProcessCnt	Uint64	进程个数
WebServiceCnt	Uint64	web服务个数
LatestImageScanTime	String	最近镜像扫描时间
ImageUnsafeCnt	Uint64	风险镜像个数
HostUnInstallCnt	Uint64	主机未安装agent数量
SuperNodeCnt	Uint64	超级节点个数
SuperNodeRunningCnt	Uint64	超级节点运行个数
TodayNewImageCnt	Uint64	今日新增镜像个数
TodayUnsafeImageCnt	Uint64	今日新增风险镜像个数
RecommendedFixImageCnt	Uint64	推荐处置镜像个数
ScannedImageCnt	Uint64	已扫描镜像个数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询web服务列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全查询web服务列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetWebServiceList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of AssetFilters	**此参数对外不可见。** 过滤条件。 - Keywords- String - 是否必填：否 - 模糊查询可选字段 - Type- String - 是否必填：否 - 主机运行状态筛选，"Apache" "Jboss" "lighttpd" "Nginx" "Tomcat"

3. 输出参数

参数名称	类型	描述
List	ServiceInfo	主机列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

查询自动授权规则授权范围主机信息

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询自动授权规则授权范围主机信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAutoAuthorizedRuleHost
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleId	是	否	Int64	规则id
Limit	否	否	Uint64	需要返回的数量，默认为全部；
Offset	否	否	Uint64	偏移量，默认为0
Order	否	否	String	排序字段
By	否	否	String	排序方式，asc，desc

3. 输出参数

参数名称	类型	描述
List	AutoAuthorizedRuleHostInfo	镜像自动授权规则授权范围主机列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
FailedOperation.ErrRuleNotFind	
FailedOperation.RuleNotFind	
InternalError.MainDBFail	

查询容器安全资产概览

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询容器资产概览信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeContainerAssetSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
ContainerTotalCnt	Uint64	容器总数
ContainerRunningCnt	Uint64	正在运行容器数量
ContainerPauseCnt	Uint64	暂停运行容器数量
ContainerStopped	Uint64	停止运行容器数量
ImageCnt	Uint64	本地镜像数量
HostCnt	Uint64	主机节点数量
HostRunningCnt	Uint64	主机正在运行节点数量
HostOfflineCnt	Uint64	主机离线节点数量
ImageRegistryCnt	Uint64	镜像仓库数量
ImageTotalCnt	Uint64	镜像总数
HostUnInstallCnt	Uint64	主机未安装agent数量
HostSuperNodeCnt	Uint64	超级节点个数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	

查询容器安全未处理事件概览

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询容器安全未处理事件信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeContainerSecEventSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
UnhandledEscapeCnt	Uint64	未处理逃逸事件
UnhandledReverseShellCnt	Uint64	未处理反弹shell事件
UnhandledRiskSyscallCnt	Uint64	未处理高危系统调用
UnhandledAbnormalProcessCnt	Uint64	未处理异常进程
UnhandledFileCnt	Uint64	未处理文件篡改
UnhandledVirusEventCnt	Uint64	未处理木马事件
UnhandledMaliciousConnectionEventCnt	Uint64	未处理恶意外连事件
UnhandledK8sApiEventCnt	Uint64	未处理k8sApi事件
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
InternalError	

查询镜像自动授权结果列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询镜像自动授权结果列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeImageAutoAuthorizedLogList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskId	是	否	Int64	自动授权任务Id
Filters	否	否	Array of AssetFilters	Status授权结果，SUCCESS:成功，REACH_LIMIT:达到授权上限，LICENSE_INSUFFICIENT:授权数不足
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0
By	否	否	String	排序字段：AuthorizedTime
Order	否	否	String	排序方式，asc，desc

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	总数量
List	AutoAuthorizedImageInfo	自动授权结果镜像列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	

查询本地镜像自动授权规则

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询本地镜像自动授权规则

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-20 15:33:55。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeImageAutoAuthorizedRule
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
IsEnabled	Int64	规则是否生效，0:不生效，1:已生效
RangeType	String	授权范围类别，MANUAL:自选主机节点，ALL:全部镜像
HostCount	Int64	授权范围是自选主机时的主机数量
MaxDailyCount	Int64	每天最大的镜像授权数限制, 0表示无限制
RuleId	Int64	规则id，用未设置时为0
AutoScanEnabled	Int64	自动扫描开关，0：关闭，1：开启
ScanType	String	自动扫描范围
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InternalError.MainDBFail	

查询镜像自动授权任务列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询镜像自动授权任务列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeImageAutoAuthorizedTaskList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
StartTime	是	否	Date	开始时间
EndTime	是	否	Date	结束时间
Filters	否	否	Array of AssetFilters	过滤字段 Status授权结果，全部授权成功：ALLSUCCSESS，部分授权失败：PARTIALFAIL,全部授权失败：ALLFAIL Type授权方式，AUTO:自动授权，MANUAL:手动授权 Source 镜像来源，LOCAL:本地镜像，REGISTRY:仓库镜像
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0

3. 输出参数

参数名称	类型	描述
List	ImageAutoAuthorizedTask	自动授权任务列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	

查询本地镜像组件列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询本地镜像组件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeImageComponentList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 - ComponentName- String - 是否必填：否 - 镜像组件名称 - ComponentVersion- String - 是否必填：否 - 镜像组件版本 - ComponentType- String - 是否必填：否 - 镜像组件类型 - VulLevel- String - 是否必填：否 - 漏洞威胁等级 - HasVul- String - 是否必填：否 -是否有漏洞；true：是，false，否；不传或ALL ：全部
ImageID	是	否	String	镜像ID
By	否	否	String	排序字段
Order	否	否	String	排序方式desc ，asc

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	总数量
List	ImageComponent	镜像组件列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	

查询用户镜像仓库下的命令空间列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询用户镜像仓库下的命令空间列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeImageRegistryNamespaceList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Offset	否	否	Uint64	**此参数对外不可见。** 本次查询的起始偏移量，默认为0。
Limit	否	否	Uint64	**此参数对外不可见。** 本次查询的数据量，默认为10，最大值为100。
Filters	否	否	Array of AssetFilters	**此参数对外不可见。** 查询的过滤条件。Name字段可取值"Namespace"。

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	可返回的命令空间的总量。
NamespaceList	String	返回的命令空间列表
NamespaceDetail	NamespaceInfo	返回的命令空间详细信息列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

镜像仓库查看定时任务

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库查看定时任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeImageRegistryTimingScanTask
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
Enable	Bool	定时扫描开关
ScanTime	String	定时任务扫描时间
ScanPeriod	Uint64	定时扫描间隔
ScanType	String	扫描类型数组
All	Bool	扫描全部镜像
Images	ImageInfo	自定义扫描镜像
Id	Uint64	自动以扫描镜像Id
Latest	Bool	是否扫描最新版本镜像
ScanEndTime	String	扫描结束时间
RegistryType	String	仓库类型 tcr,ccr,harbor
ContainerRunning	Bool	是否存在运行中的容器
ScanScope	Uint64	扫描范围 0全部镜像，1自选镜像，2推荐扫描镜像
Namespace	String	命名空间

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
ResourceNotFound	

查询本地镜像风险概览

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询本地镜像风险概览

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeImageRiskSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
VulnerabilityCnt	RunTimeRiskInfo	安全漏洞
MalwareVirusCnt	RunTimeRiskInfo	木马病毒
RiskCnt	RunTimeRiskInfo	敏感信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询容器安全本地镜像风险趋势

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询容器安全本地镜像风险趋势

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeImageRiskTendency
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
StartTime	是	否	Date	开始时间
EndTime	是	否	Date	结束时间

3. 输出参数

参数名称	类型	描述
ImageRiskTendencySet	ImageRiskTendencyInfo	本地镜像新增风险趋势信息列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	

错误码	描述
InvalidParameter.InvalidFormat	
InvalidParameterValue.DataRange	

查询全部镜像列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

DescribeImageSimpleList 查询全部镜像列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeImageSimpleList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	IsAuthorized 是否已经授权, 0:否 1:是 无:全部
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
ImageList	ImageSimpleInfo	镜像列表
ImageCnt	Uint64	镜像数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
InternalError	
InternalError.MainDBFail	

查询最新披露漏洞列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询最新披露漏洞列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:09:44。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeNewestVul
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
PocID	String	漏洞PocID
VulName	String	漏洞名称
SubmitTime	String	披露时间
Status	String	应急漏洞风险情况：NOT_SCAN：未扫描，SCANNING：扫描中，SCANNED：已扫描
CVEID	String	漏洞CVEID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	

查询后付费详情

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

DescribePostPayDetail 查询后付费详情

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:23:21。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribePostPayDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
SoftQuotaDayDetail	SoftQuotaDayInfo	弹性计费扣费详情
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InternalError.MainDBFail	

查询扫描忽略的漏洞列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询扫描忽略的漏洞列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeScanIgnoreVulList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - CVEID- string - 是否必填：否 - CVE编号 - VulName- string - 是否必填：否 - 漏洞名称
Order	否	否	String	排序方式:DESC,ACS
By	否	否	String	排序字段 UpdateTime

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	总是
List	ScanIgnoreVul	漏洞列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	

查询容器运行时安全时间趋势

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询容器运行时安全事件趋势

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecEventsTendency
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
StartTime	是	否	Date	开始时间
EndTime	是	否	Date	结束时间

3. 输出参数

参数名称	类型	描述
EventTendencySet	SecTendencyEventInfo	运行时安全事件趋势信息列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	

错误码	描述
InvalidParameter.InvalidFormat	
InvalidParameterValue.DataRange	
InternalError.MainDBFail	

查询系统漏洞列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询系统漏洞列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:09:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSystemVulList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - OnlyAffectedContainer- string - 是否必填：否 - 仅展示影响容器的漏洞true,false - OnlyAffectedNewestImage-string - 是否必填：否 - 仅展示影响最新版本镜像的漏洞true,false - Level- String - 是否必填：否 - 威胁等级，CRITICAL:严重 HIGH:高/MIDDLE:中/LOW:低 - Tags- string - 是否必填：否 - 漏洞标签，POC，EXP。 - CanBeFixed- string - 是否必填：否 - 是否可修复true,false。 - CVEID- string - 是否必填：否 - CVE编号 - ImageID- string - 是否必填：否 - 镜像ID - ImageName- String -是否必填: 否 - 镜像名称 - ContainerID- string -是否必填: 否 - 容器ID - ContainerName- string -是否必填: 否 - 容器名称 - ComponentName- string -是否必填: 否 - 组件名称 - ComponentVersion- string -是否必填: 否 - 组件版本 - Name- string -是否必填: 否 - 漏洞名称 - FocusOnType - string - 是否必填：否 -关注紧急度类型 。ALL :全部，SERIOUS_LEVEL： 严重和高危 ，IS_SUGGEST： 重点关注，POC_EXP 有Poc或Exp ，NETWORK_EXP: 远程Exp
Order	否	否	String	排序方式
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	漏洞总数

参数名称	类型	描述
List	VulInfo	漏洞列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	

查询增值服务需购买信息

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

DescribeValueAddedSrvInfo查询增值服务需购买信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:23:21。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeValueAddedSrvInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
RegistryImageCnt	Uint64	仓库镜像未授权数量
LocalImageCnt	Uint64	本地镜像未授权数量
UnusedAuthorizedCnt	Uint64	未使用的镜像安全扫描授权数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InternalError.MainDBFail	

查询漏洞防御事件列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞防御事件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulDefenceEvent
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	**此参数对外不可见。** 过滤条件。 - Status- String - 是否必填：否 - 插件状态，待处理：EVENT_UNDEAL，EVENT_DEALED：已处理，已忽略：EVENT_IGNORE，EVENT_DEFENDED：已防御 - ContainerStatus- String - 是否必填：否 - 容器运行状态筛选，已创建：CREATED,正常运行：RUNNING, 暂定运行：PAUSED, 停止运行： STOPPED，重启中：RESTARTING, 迁移中：REMOVING, 销毁：DESTROYED - ContainerNetStatus- String -是否必填: 否 - 容器网络状态筛选 未隔离：NORMAL，已隔离：ISOLATED，隔离失败：ISOLATE_FAILED，解除隔离失败：RESTORE_FAILED，解除隔离中：RESTORING，隔离中：ISOLATING - EventType - String -是否必填: 否 - 入侵状态，防御成功：EVENT_DEFENDED，尝试攻击：EVENT_ATTACK - TimeRange- String -是否必填: 否 - 时间范围，第一个值表示开始时间，第二个值表示结束时间 - VulName- string - 是否必填：否 - 漏洞名称。 - CVEID- string - 是否必填：否 - CVE编号。 - SourceIP- string - 是否必填：否 - 攻击源IP。 - ContainerName- string - 是否必填：否 - 容器名称。 - ContainerID- string - 是否必填：否 - 容器ID。 - ImageName- string - 是否必填：否 - 镜像名称。 - ImageID- string - 是否必填：否 - 镜像ID。 - HostName- string - 是否必填：否 - 主机名称。 - HostIP- string - 是否必填：否 - 内网IP。
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Order	否	否	String	**此参数对外不可见。** 排序方式：asc/desc
By	否	否	String	**此参数对外不可见。** 排序字段：事件数量：EventCount

3. 输出参数

参数名称	类型	描述
List	VulDefenceEvent	漏洞防御事件列表
TotalCount	Int64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询漏洞防御事件详情

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞防御事件详情

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-28 23:58:05。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulDefenceEventDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventID	是	否	Int64	**此参数对外不可见。** 事件ID

3. 输出参数

参数名称	类型	描述
EventDetail	VulDefenceEventDetail	漏洞防御事件详细
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	

错误码	描述
InvalidParameterValue	
FailedOperation	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询漏洞防御攻击事件趋势

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞防御攻击事件趋势

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulDefenceEventTendency
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
StartTime	是	否	Date	开始时间
EndTime	是	否	Date	结束时间

3. 输出参数

参数名称	类型	描述
DefendedList	VulDefenceEventTendency	漏洞防御事件趋势
AttackList	VulDefenceEventTendency	漏洞攻击事件趋势
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询漏洞防御的主机列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞防御的主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:10:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulDefenceHost
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	**此参数对外不可见。** 过滤条件。
Status- String - 是否必填：否 - 插件状态，正常：SUCCESS，异常：FAIL， NO_DEFENCE:未防御				
HostName- String - 是否必填：否 - 主机名称/超级节点名称				
HostIP- String - 是否必填：否 - 主机IP				
NodeType- String - 是否必填：否 - 节点类型				
HostName- String - 是否必填：否 - 超级节点名称				
NodeSubNetCIDR- String - 是否必填：否 - 超级节点CIDR				
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Order	否	否	String	**此参数对外不可见。** 排序方式：asc/desc

参数名称	必选	允许NULL	类型	描述
By	否	否	String	**此参数对外不可见。** 排序字段：更新时间：ModifyTime/首次开启时间：CreateTime

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	总数量
List	VulDefenceHost	漏洞防御的主机列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询漏洞防御插件列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞防御插件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulDefencePlugin
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
HostID	否	否	String	**此参数对外不可见。** 主机HostID或超级节点UniqueId
Limit	否	否	Uint64	**此参数对外不可见。** 需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量，默认为0。
Filters	否	否	Array of RunTimeFilters	**此参数对外不可见。** 过滤条件。
Status- String - 是否必填：否 -插件运行状态：注入中:INJECTING，注入成功：SUCCESS，注入失败：FAIL，插件超时：TIMEOUT，插件退出：QUIT				

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
TotalCount	Int64	总数量
List	VulDefencePlugin	漏洞防御插件列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询漏洞防御设置信息

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞防御设置信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulDefenceSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
IsEnabled	Int64	是否开启:0: 关闭 1:开启
Scope	Int64	漏洞防御主机范围: 0:自选主机节点，1:全部
HostCount	Int64	漏洞防御主机数量
ExceptionHostCount	Int64	开启漏洞防御异常主机数量
HostIDs	String	自选漏洞防御主机
HostTotalCount	Int64	开通容器安全的主机总数
SupportDefenseVulCount	Int64	支持防御的漏洞数
HostNodeCount	Int64	普通节点个数
SuperScope	Int64	超级节点范围
SuperNodeCount	Int64	超级节点个数
SuperNodeIds	String	超级节点Id列表
NodeTotalCount	Int64	开通容器安全的超级结点总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询漏洞扫描忽略的本地镜像列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞扫描忽略的本地镜像列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulIgnoreLocalImageList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
PocID	是	否	String	漏洞PocID
Order	否	否	String	排序方式:DESC,ACS
By	否	否	String	排序字段 ImageSize

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	总数量
List	VulIgnoreLocalImage	镜像列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询漏洞扫描忽略的仓库镜像列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞扫描忽略的仓库镜像列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulIgnoreRegistryImageList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
PocID	是	否	String	漏洞PocID

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	总数量
List	VulIgnoreRegistryImage	镜像列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

查询漏洞镜像统计

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞镜像统计

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:09:05。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulImageSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
SeriousVulImageCount	Int64	受严重或高危漏洞影响的镜像数
ScannedImageCount	Int64	已扫描的镜像数
VulTotalCount	Int64	漏洞总数量
SysTemVulCount	Int64	系统漏洞数
WebVulCount	Int64	web应用漏洞数
AllAuthorizedImageCount	Int64	已授权镜像数
EmergencyVulCount	Int64	应急漏洞数
SupportVulTotalCount	Int64	支持扫描的漏洞总数量
VulLibraryUpdateTime	String	漏洞库更新时间
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	

查询应急漏洞各威胁等级统计镜像数

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询应急漏洞各威胁等级统计镜像数

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:09:03。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulLevelImageSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
HighLevelVulLocalImagePercent	Float	高危漏洞最新本地镜像占比
MediumLevelVulLocalImagePercent	Float	中危漏洞最新本地镜像占比
LowLevelVulLocalImagePercent	Float	低危漏洞最新本地镜像占比
CriticalLevelVulLocalImagePercent	Float	严重漏洞最新本地镜像占比
LocalNewestImageCount	Int64	影响的最新版本本地镜像数
RegistryNewestImageCount	Int64	影响的最新版本仓库镜像数
HighLevelVulRegistryImagePercent	Float	高危漏洞最新仓库镜像占比
MediumLevelVulRegistryImagePercent	Float	中危漏洞最新仓库镜像占比
LowLevelVulRegistryImagePercent	Float	低危漏洞最新仓库镜像占比
CriticalLevelVulRegistryImagePercent	Float	严重漏洞最新仓库镜像占比
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	

查询漏洞各威胁等级统计数

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞各威胁等级统计数

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:09:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulLevelSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
CategoryType	是	否	String	漏洞分类: SYSTEM:系统漏洞 WEB:web应用漏洞 EMERGENCY:应急漏洞

3. 输出参数

参数名称	类型	描述
HighLevelVulCount	Int64	高危漏洞数
MediumLevelVulCount	Int64	中危漏洞数
LowLevelVulCount	Int64	低危漏洞数
CriticalLevelVulCount	Int64	严重漏洞数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	

查询漏洞影响的仓库镜像列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞影响的仓库镜像列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulRegistryImageList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
PocID	是	否	String	漏洞ID
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Filters	否	否	Array of AssetFilters	过滤条件。 OnlyAffectedNewestImage bool 是否影响最新镜像 ImageDigest 镜像Digest，支持模糊查询 ImageId 镜像ID，支持模糊查询 Namespace 命名空间，支持模糊查询 ImageTag 镜像版本，支持模糊查询 InstanceName 实例名称，支持模糊查询 ImageName 镜像名，支持模糊查询 ImageRepoAddress 镜像地址，支持模糊查询
Order	否	否	String	排序方式
By	否	否	String	排序字段

3. 输出参数

参数名称	类型	描述
TotalCount	Int64	镜像总数
List	VulAffectedRegistryImageInfo	仓库镜像列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

统计漏洞扫描页已授权和未扫描镜像数

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

统计漏洞扫描页已授权和未扫描镜像数

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulScanAuthorizedImageSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AllAuthorizedImageCount	Int64	全部已授权的本地镜像数
UnScanAuthorizedImageCount	Int64	已授权未扫描的本地镜像数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	

错误码	描述
InvalidParameter.InvalidFormat	

查询漏洞风险统计概览

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞风险统计概览

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:08:51。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	**此参数对外不可见。** 过滤条件。 - OnlyAffectedNewestImage- string- 是否必填：否 - 仅展示影响最新版本镜像的漏洞true,false - OnlyAffectedContainer-string- 是否必填：否 - 仅展示影响容器的漏洞,true,false - CategoryType- string - 是否必填：否 - 漏洞分类: SYSTEM:系统漏洞 WEB:web应用漏洞 ALL:全部漏洞

3. 输出参数

参数名称	类型	描述
VulTotalCount	Int64	漏洞总数量
SeriousVulCount	Int64	严重及高危漏洞数量
SuggestVulCount	Int64	重点关注漏洞数量
PocExpLevelVulCount	Int64	有Poc或者Exp的漏洞数量
RemoteExpLevelVulCount	Int64	有远程Exp的漏洞数量
SeriousVulNewestImageCount	Int64	受严重或高危漏洞影响的最新版本镜像数
SystemVulnerabilityFocusCount	Int64	系统漏洞重点关注数
WebVulnerabilityFocusCount	Int64	web漏洞重点关注数
SeriousVulnerabilityLocalImageCount	Int64	受影响本地镜像数
SeriousVulnerabilityRegistryImageCount	Int64	受影响仓库镜像数

参数名称	类型	描述
EmergencyVulnerabilityCount	Int64	应急漏洞数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	
InternalError.MainDBFail	

查询漏洞风险趋势

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询本地镜像、仓库镜像中严重&高危的漏洞趋势

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulTendency
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
StartTime	是	否	Date	开始时间
EndTime	是	否	Date	结束时间
SphereOfInfluence	是	否	String	枚举类型： LATEST：最新版本 CONTAINER: 运行容器

3. 输出参数

参数名称	类型	描述
VulTendencySet	VulTendencyInfo	漏洞趋势列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

查询漏洞Top排名列表

最近更新时间: 2024-09-03 18:49:50

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询漏洞Top排名列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulTopRanking
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
CategoryType	是	否	String	漏洞分类: SYSTEM:系统漏洞 WEB:web应用漏洞 EMERGENCY:应急漏洞

3. 输出参数

参数名称	类型	描述
List	VulTopRankingInfo	漏洞Top排名信息列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InternalError.MainDBFail	

主机资产刷新

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全主机资产刷新

默认接口请求频率限制：20次/秒。

接口更新时间：2023-12-05 20:25:27。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyAsset
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
All	否	否	Bool	全部同步，俩参数必选一个 All优先
Hosts	否	否	Array of String	要同步的主机列表uuid ，俩参数必选一个 All优先

3. 输出参数

参数名称	类型	描述
Status	String	同步任务发送结果
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	

镜像仓库停止镜像扫描任务

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库停止镜像扫描任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyAssetImageRegistryScanStop
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
All	否	否	Bool	**此参数对外不可见。** 是否扫描全部镜像
Images	否	否	Array of ImageInfo	**此参数对外不可见。** 扫描的镜像列表
Id	否	否	Array of Uint64	**此参数对外不可见。** 扫描的镜像列表
Filters	否	否	Array of AssetFilters	**此参数对外不可见。** 过滤条件
ExcludeImageList	否	否	Array of Uint64	**此参数对外不可见。** 不要扫描的镜像列表，与Filters配合使用
OnlyScanLatest	否	否	Bool	**此参数对外不可见。** 是否仅扫描各repository最新版本的镜像
TaskID	否	否	Uint64	**此参数对外不可见。** 停止的任务ID

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
ResourceNotFound	

镜像仓库停止镜像一键扫描任务

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库停止镜像一键扫描任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyAssetImageRegistryScanStopOneKey
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
All	否	否	Bool	**此参数对外不可见。** 是否扫描全部镜像
Images	否	否	Array of ImageInfo	**此参数对外不可见。** 扫描的镜像列表
Id	否	否	Array of Uint64	**此参数对外不可见。** 扫描的镜像列表Id
TaskID	否	否	Uint64	**此参数对外不可见。** 停止的任务ID

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
ResourceNotFound	

错误码	描述
FailedOperation	

停止镜像扫描

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

容器安全停止镜像扫描

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyAssetImageScanStop
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskID	否	否	String	任务id；任务id，镜像id和根据过滤条件筛选三选一。
Images	否	否	Array of String	镜像id；任务id，镜像id和根据过滤条件筛选三选一。
Filters	否	否	Array of AssetFilters	根据过滤条件筛选出镜像；任务id，镜像id和根据过滤条件筛选三选一。
ExcludeImageIds	否	否	String	根据过滤条件筛选出镜像，再排除个别镜像

3. 输出参数

参数名称	类型	描述
Status	String	停止状态
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
ResourceNotFound	
FailedOperation	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	

批量授权镜像扫描V2.0

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

批量授权镜像扫描V2.0

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:16:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyImageAuthorized
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
LocalImageFilter	否	否	Array of AssetFilters	根据满足条件的本地镜像授权，AllLocalImages为false且LocalImageIds为空和UpdatedLocalImageCnt大于0时，需要。
RegistryImageFilter	否	否	Array of AssetFilters	根据满足条件的仓库镜像授权，AllRegistryImages为false且RegistryImageIds为空和UpdatedRegistryImageCnt大于0时，需要。
ExcludeLocalImageIds	否	否	Array of String	根据满足条件的镜像授权,同时排除的本地镜像。
ExcludeRegistryImageIds	否	否	Array of String	根据满足条件的镜像授权,同时排除的仓库镜像。
LocalImageIds	否	否	Array of String	根据本地镜像ids授权，优先权高于根据满足条件的镜像授权。AllLocalImages为false且LocalImageFilter为空和UpdatedLocalImageCnt大于0时，需要。
RegistryImageIds	否	否	Array of String	根据仓库镜像Ids授权，优先权高于根据满足条件的镜像授。AllRegistryImages为false且RegistryImageFilter为空和UpdatedRegistryImageCnt大于0时，需要。
AllLocalImages	是	否	Bool	本地镜像是否全部授权的标识，优先权高于根据本地镜像ids授权。等于true时需UpdatedLocalImageCnt大于0。
AllRegistryImages	是	否	Bool	仓库镜像是否全部授权的标识，优先权高于根据镜像ids授权。等于true时需UpdatedRegistryImageCnt大于0。
UpdatedLocalImageCnt	是	否	Uint64	指定操作授权的本地镜像数量，判断优先权最高，实际多出的镜像随机忽略，实际不足的部分也忽略。
UpdatedRegistryImageCnt	是	否	Uint64	指定操作授权的仓库镜像数量，判断优先权最高，实际多出的镜像随机忽略，实际不足的部分也忽略；

参数名称	必选	允许NULL	类型	描述
OnlyShowLatest	否	否	Bool	是否仅最新的镜像；RegistryImageFilter不为空且UpdatedRegistryImageCnt大于0时仓库镜像需要。
ImageSourceType	是	否	String	根据满足条件的本地镜像授权,本地镜像来源；ASSETIMAGE:本地镜像列表；IMAGEALL:同步本地镜像；AllLocalImages为false且LocalImageIds为空和UpdatedLocalImageCnt大于0时，需要

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
FailedOperation	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
FailedOperation.AuthorizedNotEnough	
InternalError.MainDBFail	

修改漏洞防御事件状态

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改漏洞防御事件状态

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyVulDefenceEventStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventIDs	是	否	Array of Int64	事件IDs数组
Status	是	否	String	操作状态： EVENT_DEALED：已处理，EVENT_IGNORE：忽略，EVENT_ISOLATE_CONTAINER：隔离容器，EVENT_DEL：删除
Remark	否	否	String	备注

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
ResourceNotFound	
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

编辑漏洞防御设置

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

编辑漏洞防御设置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyVulDefenceSetting
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
IsEnabled	是	否	Int64	**此参数对外不可见。** 是否开启:0: 关闭 1:开启
Scope	否	否	Int64	**此参数对外不可见。** 漏洞防御主机范围:0：自选 1: 全部主机
HostIDs	否	否	Array of String	**此参数对外不可见。** 自选漏洞防御主机
SuperScope	否	否	Int64	**此参数对外不可见。** 漏洞防御超级节点范围:0：自选 1: 全部
NodeIds	否	否	Array of String	**此参数对外不可见。** 超级节点Id列表

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
MissingParameter	
InvalidParameter	
AuthFailure	
InternalError	
InvalidParameterValue	
FailedOperation	
UnknownParameter	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

删除单个镜像仓库详细信息

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

删除单个镜像仓库详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：RemoveAssetImageRegistryRegistryDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RegistryId	是	否	Int64	仓库唯一id

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
FailedOperation	
InvalidParameter.MissingParameter	

错误码	描述
InvalidParameter.InvalidFormat	
FailedOperation.DataValueNotCorrect	

授权镜像扫描

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

RenewImageAuthorizeState 授权镜像扫描

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-20 15:11:59。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：RenewImageAuthorizeState
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ImageIds	否	否	Array of String	**此参数对外不可见。** 镜像ids
AllImages	是	否	Bool	**此参数对外不可见。** 是否全部未授权镜像
NeedScan	否	否	Bool	**此参数对外不可见。** 是否授权后自动扫描
ScanType	否	否	Array of String	**此参数对外不可见。** 扫描类型

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

错误码	描述
FailedOperation.AuthorizedNotEnough	
InternalError.MainDBFail	

编辑本地镜像自动授权开关

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

编辑本地镜像自动授权开关

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：SwitchImageAutoAuthorizedRule
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
IsEnabled	是	否	Int64	规则是否生效，0:不生效，1:已生效
RuleId	是	否	Int64	规则id

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
FailedOperation	
InvalidParameter.ParsingError	

错误码	描述
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
FailedOperation.ErrRuleNotFind	
FailedOperation.RuleNotFind	
InternalError.MainDBFail	

镜像仓库资产刷新

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库资产刷新

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-20 15:34:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：SyncAssetImageRegistryAsset
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
All	否	否	Bool	**此参数对外不可见。** 是否同步所有镜像仓库
RegistryIds	否	否	Array of Uint64	**此参数对外不可见。** 需要同步的部分镜像仓库

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	
InvalidParameter.ParsingError	

更新单个镜像仓库详细信息

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

更新单个镜像仓库详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-09-05 07:08:12。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：UpdateAssetImageRegistryRegistryDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Name	是	否	String	**此参数对外不可见。** 仓库名
Username	是	否	String	**此参数对外不可见。** 用户名
Password	是	否	String	**此参数对外不可见。** 密码
Url	是	否	String	**此参数对外不可见。** 仓库url
RegistryType	是	否	String	**此参数对外不可见。** 仓库类型，列表：harbor
RegistryVersion	否	否	String	**此参数对外不可见。** 仓库版本
NetType	是	否	String	**此参数对外不可见。** 网络类型，列表：public（公网）
RegistryRegion	否	否	String	**此参数对外不可见。** 区域，列表：default（默认）
SpeedLimit	否	否	Int64	**此参数对外不可见。** 限速
Insecure	否	否	Uint64	**此参数对外不可见。** 安全模式（证书校验）：0（默认） 非安全模式（跳过证书校验）：1

参数名称	必选	允许NULL	类型	描述
ConnDetectConfig	否	否	Array of ConnDetectConfig	**此参数对外不可见。** 联通性检测的配置

3. 输出参数

参数名称	类型	描述
HealthCheckErr	String	连接错误信息
NameRepeatErr	String	名称错误信息
RegistryId	Int64	仓库唯一id
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
AuthFailure	
InternalError	
ResourceNotFound	
InvalidParameterValue	
FailedOperation	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
FailedOperation.DataValueNotCorrect	

镜像仓库更新定时任务

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

镜像仓库更新定时任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:21:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：UpdateImageRegistryTimingScanTask
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ScanPeriod	是	否	Uint64	**此参数对外不可见。** 定时扫描周期
ScanType	否	否	Array of String	**此参数对外不可见。** 扫描木马类型数组
Images	否	否	Array of ImageInfo	**此参数对外不可见。** 扫描镜像
All	否	否	Bool	**此参数对外不可见。** 是否扫描所有
Enable	是	否	Bool	**此参数对外不可见。** 定时扫描开关
ScanTime	是	否	String	**此参数对外不可见。** 定时扫描的时间
Id	否	否	Array of Uint64	**此参数对外不可见。** 扫描镜像Id
Latest	否	否	Bool	**此参数对外不可见。** 是否扫描最新版本
ContainerRunning	否	否	Bool	**此参数对外不可见。** 是否存在运行中的容器
ScanEndTime	否	否	String	**此参数对外不可见。** 扫描结束时间
ScanScope	否	否	Uint64	**此参数对外不可见。** 扫描范围 0全部镜像，1自选镜像，2推荐扫描镜像

参数名称	必选	允许NULL	类型	描述
RegistryType	否	否	Array of String	**此参数对外不可见。** 仓库类型 tcr,ccr,harbor
Namespace	否	否	Array of String	**此参数对外不可见。** 命名空间

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
ResourceNotFound	

集群安全相关接口
安装检查组件

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

安装检查组件，创建防护容器

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateCheckComponent
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterInfoList	是	否	Array of ClusterCreateComponentItem	要安装的集群列表信息

3. 输出参数

参数名称	类型	描述
InstallResult	String	"InstallSucc"表示安装成功，"InstallFailed"表示安装失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	

错误码	描述
OperationDenied	
FailedOperation	

创建集群检查任务

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建集群检查任务，用户检查用户的集群相关风险项

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:22:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateClusterCheckTask
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterCheckTaskList	是	否	Array of ClusterCheckTaskItem	**此参数对外不可见。** 指定要扫描的集群信息

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的集群检查任务的ID，为0表示创建失败。
CreateResult	String	创建检查任务的结果，"Succ"为成功，其他的为失败原因
NewTaskID	String	返回创建的集群新任务ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	

错误码	描述
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

下发刷新任务

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

下发刷新任务，会刷新资产信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:22:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateRefreshTask
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterIDs	否	否	Array of String	**此参数对外不可见。** 指定集群列表,若为空则标识同步所有集群
IsSyncListOnly	否	否	Bool	**此参数对外不可见。** 是否只同步列表

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回创建的集群检查任务的ID，为0表示创建失败。
CreateResult	String	创建检查任务的结果，"Succ"为成功，"Failed"为失败
NewTaskID	String	返回创建的新集群检查任务ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	

错误码	描述
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

获取受影响的集群数量

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

获取受影响的集群数量，返回数量

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:22:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAffectedClusterCount
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
SeriousRiskClusterCount	Uint64	严重风险的集群数量
HighRiskClusterCount	Uint64	高危风险的集群数量
MiddleRiskClusterCount	Uint64	中危风险的集群数量
HintRiskClusterCount	Uint64	低危风险的集群数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
RequestLimitExceeded	
OperationDenied	
FailedOperation	

查询节点类型的影响范围

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询节点类型的影响范围，返回节点列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:22:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAffectedNodeList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
CheckItemId	是	否	Int64	唯一的检测项的ID
Offset	否	否	Uint64	偏移量
Limit	否	否	Uint64	每次查询的最大记录数量
Filters	否	否	Array of ComplianceFilters	Name - String Name 可取值：ClusterName, ClusterId,InstanceId,PrivateIpAddresses
By	否	否	String	排序字段
Order	否	否	String	排序方式 asc,desc

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	受影响的节点总数
AffectedNodeList	AffectedNodeItem	受影响的节点列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

查询workload类型的影响范围

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询workload类型的影响范围，返回workload列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:22:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAffectedWorkloadList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
CheckItemId	是	否	Int64	唯一的检测项的ID
Offset	否	否	Uint64	偏移量
Limit	否	否	Uint64	每次查询的最大记录数量
Filters	否	否	Array of ComplianceFilters	Name - String Name 可取值：WorkloadType,ClusterId
By	否	否	String	排序字段
Order	否	否	String	排序方式 asc,desc

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	受影响的workload列表数量
AffectedWorkloadList	AffectedWorkloadItem	受影响的workload列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

查询所有检查项接口

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询所有检查项接口，返回总数和检查项列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:22:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeCheckItemList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量
Limit	否	否	Uint64	**此参数对外不可见。** 每次查询的最大记录数量
Filters	否	否	Array of ComplianceFilters	**此参数对外不可见。** Name 可取值：
Name: 检查项名称				
RiskType: 风险类别				
RiskLevel: 风险等级				
RiskTarget: 检查对象				
RiskAttribute: 检测项所属分型线类型				
Enable: 检查项是否开启(0:关闭 1:开启)				

3. 输出参数

参数名称	类型	描述
ClusterCheckItems	ClusterCheckItem	检查项详情数组
TotalCount	Uint64	检查项总数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

查询单个集群的详细信息

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询单个集群的详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:22:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeClusterDetail
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	是	否	String	**此参数对外不可见。** 集群id

3. 输出参数

参数名称	类型	描述
ClusterId	String	集群id
ClusterName	String	集群名字
ScanTaskProgress	Int64	当前集群扫描任务的进度，100表示扫描完成.
ClusterVersion	String	集群版本
ContainerRuntime	String	运行时组件
ClusterNodeNum	Uint64	集群节点数
ClusterStatus	String	集群状态 (Running 运行中 Creating 创建中 Abnormal 异常)
ClusterType	String	集群类型：为托管集群MANAGED_CLUSTER、独立集群INDEPENDENT_CLUSTER
Region	String	集群区域
SeriousRiskCount	Uint64	严重风险检查项的数量
HighRiskCount	Uint64	高风险检查项的数量
MiddleRiskCount	Uint64	中风险检查项的数量

参数名称	类型	描述
HintRiskCount	Uint64	提示风险检查项的数量
CheckStatus	String	检查任务的状态
DefenderStatus	String	防御容器状态
TaskCreateTime	String	扫描任务创建时间
NetworkType	String	网络类型.PublicNetwork为公网类型,VPCNetwork为VPC网络
ApiServerAddress	String	API Server地址
NodeCount	Uint64	节点数
NamespaceCount	Uint64	命名空间数
WorkloadCount	Uint64	工作负载数
PodCount	Uint64	Pod数量
ServiceCount	Uint64	Service数量
IngressCount	Uint64	Ingress数量
MasterIps	String	主节点的ip列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

查询用户集群资产总览

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询用户集群资产总览

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:22:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeClusterSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	集群总数
RiskClusterCount	Uint64	有风险的集群数量
UncheckClusterCount	Uint64	未检查的集群数量
ManagedClusterCount	Uint64	托管集群数量
IndependentClusterCount	Uint64	独立集群数量
NoRiskClusterCount	Uint64	无风险的集群数量
CheckedClusterCount	Uint64	已经检查集群数
AutoCheckClusterCount	Uint64	自动检查集群数
ManualCheckClusterCount	Uint64	手动检查集群数
FailedClusterCount	Uint64	检查失败集群数
NotImportedClusterCount	Uint64	未导入的集群数量
ServerlessClusterCount	Uint64	eks集群数量
TkeClusterCount	Uint64	TKE集群数量

参数名称	类型	描述
UserCreateTencentClusterCount	Uint64	用户自建腾讯云集群数量
UserCreateHybridClusterCount	Uint64	用户自建集群混合云数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

查询刷新任务

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询刷新任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:22:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRefreshTask
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskId	是	否	Uint64	**此参数对外不可见。** 任务ID
NewTaskID	否	否	String	**此参数对外不可见。** 新任务ID

3. 输出参数

参数名称	类型	描述
TaskStatus	String	刷新任务状态，可能为：Task_New,Task_Running,Task_Finish,Task_Error,Task_NoExist
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
RequestLimitExceeded	
OperationDenied	
FailedOperation	

查询集群风险项列表

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询最近一次任务发现的风险项的信息列表，支持根据特殊字段进行过滤

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:22:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRiskList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterId	否	否	String	要查询的集群ID，如果不指定，则查询用户所有的风险项
Offset	否	否	Uint64	偏移量
Limit	否	否	Uint64	每次查询的最大记录数量
Filters	否	否	Array of ComplianceFilters	Name - String Name 可取值：RiskLevel风险等级, RiskTarget检查对象，风险对象,RiskType风险类别,RiskAttribute检测项所属的风险类型,Name
By	否	否	String	排序字段
Order	否	否	String	排序方式 asc,desc

3. 输出参数

参数名称	类型	描述
ClusterRiskItems	ClusterRiskItem	风险详情数组
TotalCount	Uint64	风险项的总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

查询检查结果总览

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询检查结果总览，返回受影响的节点数量，返回7天的数据，总共7个

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:18:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeTaskResultSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
SeriousRiskNodeCount	Uint64	严重风险影响的节点数量,返回7天数据
HighRiskNodeCount	Uint64	高风险影响的节点的数量,返回7天数据
MiddleRiskNodeCount	Uint64	中风险检查项的节点数量,返回7天数据
HintRiskNodeCount	Uint64	提示风险检查项的节点数量,返回7天数据
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	

错误码	描述
RequestLimitExceeded	
OperationDenied	
FailedOperation	

查询未完成的刷新资产任务信息

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询未完成的刷新资产任务信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:22:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeUnfinishRefreshTask
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	返回最近的一次任务ID
TaskStatus	String	任务状态，为Task_New,Task_Running,Task_Finish,Task_Error,Task_NoExist.Task_New,Task_Running表示有任务存在，不允许新下发
NewTaskID	String	新任务ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

用户集群资产查询

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

安全概览和集群安全页进入调用该接口，查询用户集群相关信息。

默认接口请求频率限制：20次/秒。

接口更新时间：2023-12-28 16:07:34。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeUserCluster
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Offset	否	否	Uint64	**此参数对外不可见。** 偏移量
Limit	否	否	Uint64	**此参数对外不可见。** 每次查询的最大记录数量
Filters	否	否	Array of ComplianceFilters	**此参数对外不可见。** Name - String Name 可取值：ClusterName,ClusterId,ClusterType,Region,ClusterCheckMode,ClusterAutoCheck
By	否	否	String	**此参数对外不可见。** 排序字段
Order	否	否	String	**此参数对外不可见。** 排序方式 asc,desc

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	集群总数
ClusterInfoList	ClusterInfoItem	集群的详细信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

设置检测模式和自动检查

最近更新时间: 2024-09-03 18:49:51

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

设置检测模式和自动检查

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:22:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：SetCheckMode
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ClusterIds	是	否	Array of String	要设置的集群ID列表
ClusterCheckMode	否	否	String	集群检查模式(正常模式"Cluster_Normal"、主动模式"Cluster_Actived"、不设置"Cluster_Unset")
ClusterAutoCheck	否	否	Uint64	0不设置 1打开 2关闭

3. 输出参数

参数名称	类型	描述
SetCheckResult	String	"Succ"表示设置成功，"Failed"表示设置失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	
InvalidParameter	
AuthFailure	

错误码	描述
InternalError	
RequestLimitExceeded	
OperationDenied	
FailedOperation	

高级防御-k8sApi异常请求相关接口
创建文件篡改规则导出任务

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建文件篡改规则导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateAccessControlsRuleExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - RuleType - string - 是否必填: 否 -规则类型 - Status - string - 是否必填: 否 -状态
Order	否	否	String	排序方式
By	否	否	Array of String	排序字段
ExportField	否	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
InternalError	

创建k8s api异常事件导出任务

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建k8s api异常事件导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateK8sApiAbnormalEventExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - TimeRange - string -是否必填: 否 - 时间范围筛选 ["2022-03-31 16:55:00", "2022-03-31 17:00:00"] - MatchRules - string - 是否必填: 否 -命中规则筛选 - RiskLevel - string - 是否必填: 否 -威胁等级筛选 - Status - string - 是否必填: 否 -事件状态筛选 - MatchRuleType - string - 是否必填: 否 -命中规则类型筛选 - ClusterRunningStatus - string - 是否必填: 否 -集群运行状态 - ClusterName - string - 是否必填: 否 -集群名称 - ClusterID - string - 是否必填: 否 -集群ID
Order	否	否	String	排序方式
By	否	否	String	排序字段
ExportField	否	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

创建k8sApi异常规则导出任务

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建k8sApi异常规则导出任务

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateK8sApiAbnormalRuleExportJob
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - RuleType - string - 是否必填: 否 -规则类型 - Status - string - 是否必填: 否 -状态
Order	否	否	String	排序方式
By	否	否	Array of String	排序字段
ExportField	否	否	Array of String	导出字段

3. 输出参数

参数名称	类型	描述
JobId	String	导出任务ID，前端拿着任务ID查询任务进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

创建k8sapi异常事件规则

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

创建k8sapi异常事件规则

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateK8sApiAbnormalRuleInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleInfo	是	否	K8sApiAbnormalRuleInfo	规则详情
CopySrcRuleID	否	否	String	拷贝规则ID(适用于复制规则场景)
EventID	否	否	Uint64	事件ID(适用于事件加白场景)

3. 输出参数

参数名称	类型	描述
RuleID	String	规则ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

删除k8sapi异常事件规则

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

删除k8sapi异常事件规则

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteK8sApiAbnormalRule
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleIDSet	是	否	Array of String	规则ID集合

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询集群列表

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询集群列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetClusterList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - ClusterID - string - 是否必填: 否 -集群ID - ClusterName - string - 是否必填: 否 -集群名称 - Status - string - 是否必填: 否 -集群状态
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式
By	否	否	String	排序字段。

3. 输出参数

参数名称	类型	描述
List	AssetClusterListItem	集群列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
InternalError	

查询k8s api 异常事件详情

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询k8s api 异常事件详情

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeK8sApiAbnormalEventInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
ID	是	否	Uint64	事件ID

3. 输出参数

参数名称	类型	描述
Info	K8sApiAbnormalEventInfo	事件详情
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	

查询k8s api异常事件列表

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询k8s api异常事件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeK8sApiAbnormalEventList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - TimeRange - string -是否必填: 否 - 时间范围筛选 ["2022-03-31 16:55:00", "2022-03-31 17:00:00"] - MatchRules - string - 是否必填: 否 -命中规则筛选 - RiskLevel - string - 是否必填: 否 -威胁等级筛选 - Status - string - 是否必填: 否 -事件状态筛选 - MatchRuleType - string - 是否必填: 否 -命中规则类型筛选 - ClusterRunningStatus - string - 是否必填: 否 -集群运行状态 - ClusterName - string - 是否必填: 否 -集群名称 - ClusterID - string - 是否必填: 否 -集群ID
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式
By	否	否	String	排序字段 LatestFoundTime: 最近生成时间 AlarmCount: 告警数量

3. 输出参数

参数名称	类型	描述
List	K8sApiAbnormalEventListItem	事件列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询k8sapi异常请求规则详情

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询k8sapi异常请求规则详情

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeK8sApiAbnormalRuleInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleID	是	否	String	规则ID

3. 输出参数

参数名称	类型	描述
Info	K8sApiAbnormalRuleInfo	规则详情
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询k8sapi异常请求规则列表

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询k8sapi异常请求规则列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeK8sApiAbnormalRuleList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of RunTimeFilters	过滤条件。 - RuleType - string - 是否必填: 否 -规则类型 - Status - string - 是否必填: 否 -状态
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式
By	否	否	String	排序字段。 - UpdateTime - string - 是否必填: 否 -最后更新时间 - EffectClusterCount - string - 是否必填: 否 -影响集群数

3. 输出参数

参数名称	类型	描述
List	K8sApiAbnormalRuleListItem	规则列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InvalidParameter	
InternalError	

查询k8sapi 异常规则中范围列表

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询k8sapi 异常规则中范围列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeK8sApiAbnormalRuleScopeList
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
Offset	否	否	Uint64	偏移量
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
RuleID	是	否	String	规则ID
Filters	否	否	Array of RunTimeFilters	过滤条件。 - Action - string -是否必填: 否 - 执行动作 - RiskLevel - string - 是否必填: 否 -威胁等级筛选

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	总数
List	K8sApiAbnormalRuleScopeInfo	列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	

错误码	描述
InternalError	

查询k8sapi异常事件统计

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询k8sapi异常事件统计

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeK8sApiAbnormalSummary
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
UnhandleEventCount	Uint64	待处理事件个数
UnhandleHighLevelEventCount	Uint64	待处理高危事件个数
UnhandleMediumLevelEventCount	Uint64	待处理中危事件个数
UnhandleLowLevelEventCount	Uint64	待处理低危事件个数
UnhandleNoticeLevelEventCount	Uint64	待处理提示级别事件个数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

查询k8sapi异常事件趋势

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

查询k8sapi异常事件趋势

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeK8sApiAbnormalTendency
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
TendencyPeriod	是	否	Uint64	趋势周期(默认为7天)

3. 输出参数

参数名称	类型	描述
List	K8sApiAbnormalTendencyItem	趋势列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

修改k8sapi异常事件状态

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改k8sapi异常事件状态

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyK8sApiAbnormalEventStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventIDSet	是	否	Array of Uint64	事件ID集合
Status	是	否	String	状态
Remark	否	否	String	备注

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	
ResourceNotFound	

修改k8sapi异常规则信息

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改k8sapi异常规则信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyK8sApiAbnormalRuleInfo
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleInfo	是	否	K8sApiAbnormalRuleInfo	规则详情

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

修改k8sapi异常事件规则状态

最近更新时间: 2024-09-03 18:49:52

1. 接口描述

接口请求域名： tcss.api3.cloud.sunhongs.com。

修改k8sapi异常事件规则状态

默认接口请求频率限制：20次/秒。

接口更新时间：2023-11-10 10:13:49。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyK8sApiAbnormalRuleStatus
Version	是	否	String	公共参数，本接口取值：2020-11-01
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleID	是	否	String	规则ID
Status	是	否	Bool	状态(true:开 false:关)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter	
InternalError	

数据结构

最近更新时间: 2024-09-03 18:49:52

ComplianceAssetDetailInfo

表示一项资产的详情。

被如下接口引用：DescribeComplianceAssetDetailInfo

名称	必选	允许NULL	类型	描述
CustomerAssetId	是	否	Uint64	客户资产的ID。
AssetType	是	否	String	资产类别。
AssetName	是	否	String	资产的名称。
NodeName	是	否	String	资产所属的节点的名称。
HostName	是	否	String	资产所在的主机的名称。
HostIP	是	否	String	资产所在的主机的IP。
CheckStatus	是	否	String	检测状态CHECK_INIT, 待检测CHECK_RUNNING, 检测中CHECK_FINISHED, 检测完成CHECK_FAILED, 检测失败
PassedPolicyItemCount	是	否	Uint64	此类资产通过的检测项的数目。
FailedPolicyItemCount	是	否	Uint64	此类资产未通过的检测的数目。
LastCheckTime	是	是	Datetime	上次检测的时间。
CheckResult	是	是	String	检测结果：RESULT_FAILED: 未通过。RESULT_PASSED: 通过。
AssetStatus	是	否	String	资产的运行状态。
AssetCreateTime	是	否	Datetime	创建资产的时间。ASSET_NORMAL: 正常运行，ASSET_PAUSED: 暂停运行，ASSET_STOPPED: 停止运行，ASSET_ABNORMAL: 异常

VulAffectedImageInfo

受漏洞影响的镜像信息

被如下接口引用：DescribeVulImageList

名称	必选	允许NULL	类型	描述
ImageID	是	否	String	镜像ID
ImageName	是	否	String	镜像名称
HostCount	是	否	Int64	关联的主机数
ContainerCount	是	否	Int64	关联的容器数
ComponentList	是	否	Array of VulAffectedImageComponentInfo	组件列表

ImageDenyRule

镜像拦截规则

被如下接口引用：DescribeImageDenyRuleList

名称	必选	允许NULL	类型	描述
RuleID	是	否	String	规则RuleID
RuleName	是	否	String	规则名称
RuleType	是	否	String	规则类型 RULE_RISK：风险， RULE_PRIVILEGE：特权
EffectImageCount	是	否	Int64	生效的镜像数量
IsEffectAllImage	是	否	Int64	是否对全部扫描镜像生效。0:全选镜像，1:自选镜像
EffectTime	是	否	String	规则开始生效时间
UpdateTime	是	否	String	更新时间
OperationUin	是	否	String	操作用户
Status	是	否	Int64	启用状态
EffectStatus	是	否	String	生效状态 IN_THE_TEST ：观察中，IN_EFFECT：生效中
ID	是	否	Int64	规则ID

RiskDnsEventInfo

恶意请求事件信息

被如下接口引用：DescribeRiskDnsList

名称	必选	允许NULL	类型	描述
EventID	是	否	Uint64	事件ID
EventType	是	否	String	事件类型，恶意域名请求：DOMAIN，恶意IP请求：IP
Address	是	否	String	恶意请求域名/IP
ContainerID	是	否	String	容器ID
ContainerName	是	否	String	容器名称
ContainerNetStatus	是	否	String	隔离状态未隔离 NORMAL已隔离 ISOLATED隔离中 ISOLATING隔离失败 ISOLATE_FAILED解除隔离中 RESTORING解除隔离失败 RESTORE_FAILED
ContainerStatus	是	否	String	容器状态正在运行: RUNNING暂停: PAUSED停止: STOPPED已经创建: CREATED已经销毁: DESTROYED正在重启中: RESTARTING迁移中: REMOVING
ContainerNetSubStatus	是	否	String	容器子状态"AGENT_OFFLINE" //Agent离线"NODE_DESTROYED" //节点已销毁"CONTAINER_EXITED" //容器已退出"CONTAINER_DESTROYED" //容器已销毁"SHARED_HOST" // 容器与主机共享网络"RESOURCE_LIMIT" //隔离操作资源超限"UNKNOW" // 原因未知
ContainerIsolateOperationSrc	是	否	String	容器隔离操作来源

名称	必选	允许NULL	类型	描述
ImageID	是	否	String	镜像ID
ImageName	是	否	String	镜像名称
FoundTime	是	否	String	首次发现时间
LatestFoundTime	是	否	String	最近生成时间
EventStatus	是	否	String	事件状态EVENT_UNDEAL： 待处理EVENT_DEALED：已处理 EVENT_IGNORE： 已忽略EVENT_ADD_WHITE：已加白
EventCount	是	否	Int64	恶意请求次数
Description	是	否	String	事件描述
Solution	是	否	String	解决方案
City	是	否	String	恶意IP所属城市
HostName	是	否	String	主机名称
HostID	是	否	String	主机ID
HostIP	是	否	String	内网IP
PublicIP	是	否	String	外网IP
NodeType	否	否	String	节点类型：NORMAL普通节点、SUPER超级节点
NodeName	否	否	String	节点名称
PodIP	否	否	String	pod ip
PodName	否	否	String	pod 名称
ClusterID	否	否	String	集群ID
NodeID	否	否	String	节点id
NodeUniqueID	否	否	String	节点唯一id
ClusterName	否	否	String	集群名称

ContainerInfo

容器列表集合

被如下接口引用：DescribeAssetContainerList

名称	必选	允许NULL	类型	描述
ContainerID	否	否	String	容器id
ContainerName	否	否	String	容器名称
Status	否	否	String	容器运行状态
CreateTime	否	否	String	创建时间
RunAs	否	否	String	运行用户

名称	必选	允许NULL	类型	描述
Cmd	否	否	String	命令行
CPUUsage	否	否	Uint64	CPU使用率 *1000
RamUsage	否	否	Uint64	内存使用 kb
ImageName	否	否	String	镜像名称
ImageID	否	否	String	镜像id
POD	否	否	String	镜像id
HostID	否	否	String	主机id
HostIP	否	否	String	主机ip
UpdateTime	否	否	String	更新时间
HostName	否	否	String	主机名称
PublicIp	否	否	String	外网ip
NetStatus	否	否	String	网络状态未隔离 NORMAL已隔离 ISOLATED隔离中 ISOLATING隔离失败 ISOLATE_FAILED解除隔离中 RESTORING解除隔离失败 RESTORE_FAILED
NetSubStatus	否	否	String	网络子状态
IsolateSource	否	是	String	隔离来源
IsolateTime	否	是	String	隔离时间
NodeID	否	否	String	超级节点id
PodIP	否	否	String	podip
PodName	否	否	String	pod名称
NodeType	否	否	String	节点类型:节点类型：NORMAL普通节点、SUPER超级节点
NodeUniqueID	否	否	String	超级节点唯一id
PodCpu	否	否	Int64	所属Pod的CPU
PodMem	否	否	Int64	所属Pod的内存
ClusterName	否	否	String	集群名称
ClusterID	否	否	String	集群ID
PodUid	否	是	String	pod uid

VulTopRankingInfo

漏洞Top排名信息

被如下接口引用：DescribeVulTopRanking

名称	必选	允许NULL	类型	描述
VulName	是	否	String	漏洞名称

名称	必选	允许NULL	类型	描述
Level	是	否	String	威胁等级,CRITICAL:严重 HIGH:高/MIDDLE:中/LOW:低
AffectedImageCount	是	否	Int64	影响的镜像数
AffectedContainerCount	是	否	Int64	影响的容器数
ID	是	否	Int64	漏洞ID
PocID	是	否	String	漏洞PocID

RegexpRuleInfo

正则规则详情

被如下接口引用：AddModEscapeRegexpWhiteList、AddModReverseShellRegexpWhiteList、DescribeEscapeRegexpWhiteListInfo、DescribeReverseShellRegexpWhiteListInfo

名称	必选	允许NULL	类型	描述
RuleID	否	是	String	规则ID
RuleName	是	是	String	规则名称
Status	是	是	Bool	启用状态
ExpressionList	是	是	Array of WhiteListRegexpExpressionInfo	正则表达式列表
UpdateTime	否	是	String	最近更新时间
OperatorUIN	否	是	String	最近操作账号

AutoAuthImageInfo

用于仓库自动授权的自选项目空间、自选镜像仓库。

被如下接口引用：DescribeImageRegistryAutoAuthorizedRepoList、DescribeImageRegistryAutoAuthorizedRuleImage、ModifyImageRegistryAutoAuthorizedRule

名称	必选	允许NULL	类型	描述
RegistryType	是	否	String	仓库类型
InstanceName	是	否	String	仓库实例名称
Namespace	是	否	String	项目空间（命名空间）
ImageName	否	否	String	镜像名称
UniqueKey	否	是	String	唯一Key
RepoCount	否	否	Uint64	镜像仓数量

ClusterCreateComponentItem

CreateCheckComponent的入口参数,用于批量安装防御容器

被如下接口引用：CreateCheckComponent

名称	必选	允许NULL	类型	描述
ClusterId	是	否	String	要安装组件的集群ID。
ClusterRegion	是	否	String	该集群对应的地域

ClusterIngressInfo

集群Ingress信息

被如下接口引用：DescribeClusterIngressList

名称	必选	允许NULL	类型	描述
Name	是	否	String	Ingress名称
Type	是	否	String	预留字段，当前不生效.
Address	是	否	String	VIP地址
BackendInfo	是	否	String	Ingress对应的后端服务，多个以,隔开
ClusterName	是	否	String	集群名称
ClusterId	是	否	String	集群Id
Namespace	是	否	String	命名空间
Region	是	否	String	地域
CreationTimestamp	是	否	String	创建时间
BackendCount	是	否	Uint64	后端服务数量
ClusterStatus	是	否	String	集群状态
ClusterType	是	否	String	集群类型
Labels	是	否	String	标签

VulTendencyInfo

漏洞趋势信息

被如下接口引用：DescribeVulTendency

名称	必选	允许NULL	类型	描述
VulSet	是	否	Array of RunTimeTendencyInfo	漏洞趋势列表
ImageType	是	否	String	漏洞影响的镜像类型：LOCAL：本地镜像REGISTRY: 仓库镜像

ImageRepoInfo

容器安全镜像仓库列表

被如下接口引用：DescribeAssetImageRegistryList

名称	必选	允许NULL	类型	描述
ImageDigest	否	否	String	镜像Digest
ImageRepoAddress	否	否	String	镜像仓库地址
RegistryType	否	否	String	仓库类型
ImageName	否	否	String	镜像名称
ImageTag	否	否	String	镜像版本
ImageSize	否	否	Uint64	镜像大小
ScanTime	否	否	String	最近扫描时间
ScanStatus	否	否	String	扫描状态
VulCnt	否	否	Uint64	安全漏洞数
VirusCnt	否	否	Uint64	木马病毒数
RiskCnt	否	否	Uint64	风险行为数
SentiveInfoCnt	否	否	Uint64	敏感信息数
IsTrustImage	否	否	Bool	是否可信镜像
OsName	否	否	String	镜像系统
ScanVirusError	否	是	String	木马扫描错误
ScanVulError	否	是	String	漏洞扫描错误
InstanceId	否	否	String	实例id
InstanceName	否	否	String	实例名称
Namespace	否	否	String	命名空间
ScanRiskError	否	是	String	高危扫描错误
ScanVirusProgress	否	是	Uint64	敏感信息扫描进度
ScanVulProgress	否	是	Uint64	木马扫描进度
ScanRiskProgress	否	是	Uint64	漏洞扫描进度
ScanRemainTime	否	是	Uint64	剩余扫描时间秒
CveStatus	否	是	String	cve扫描状态
RiskStatus	否	是	String	高危扫描状态
VirusStatus	否	是	String	木马扫描状态
Progress	否	是	Uint64	总进度
IsAuthorized	否	否	Uint64	授权状态
RegistryRegion	否	否	String	仓库区域
Id	否	否	Uint64	列表id

名称	必选	允许NULL	类型	描述
ImageId	否	是	String	镜像Id
ImageCreateTime	否	是	Datetime_iso	镜像创建的时间
IsLatestImage	否	是	Bool	是否为镜像的最新版本
LowLevelVulCnt	否	否	Uint64	low级别漏洞个数
MediumLevelVulCnt	否	否	Uint64	medium级别漏洞个数
HighLevelVulCnt	否	否	Uint64	high级别漏洞个数
CriticalLevelVulCnt	否	否	Uint64	critical级别漏洞个数
ContainerCnt	否	否	Uint64	关联容器数
ComponentCnt	否	否	Uint64	组件数
IsRunning	否	否	Bool	是否运行中
HasNeedFixVul	否	否	Bool	是否存在必修漏洞
SensitiveInfoCnt	否	是	Uint64	敏感信息
RecommendedFix	否	否	Bool	是否推荐处置

VulIgnoreLocalImage

漏洞扫描忽略的本地镜像

被如下接口引用：DescribeVulIgnoreLocalImageList

名称	必选	允许NULL	类型	描述
ID	是	否	Int64	记录ID
ImageID	是	否	String	镜像ID
ImageName	是	否	String	镜像名称
ImageSize	是	否	Int64	镜像大小
PocID	是	否	String	漏洞PocID

ClusterWorkloadInfo

集群的工作负载信息

被如下接口引用：DescribeClusterWorkloads

名称	必选	允许NULL	类型	描述
WorkloadName	是	否	String	工作负载名称
WorkloadType	是	否	String	工作负载类型
WorkloadLabels	是	否	String	工作负载标签

名称	必选	允许NULL	类型	描述
PodCount	是	否	Uint64	关联的Pod数量
WorkloadSelectors	是	否	String	工作负载Selector
Namespace	是	否	String	命名空间

FileAttributeInfo

容器安全运行时，文件属性信息

被如下接口引用：DescribeAccessControlDetail

名称	必选	允许NULL	类型	描述
FileName	是	否	String	文件名
FileType	是	否	String	文件类型
FileSize	是	否	Uint64	文件大小(字节)
FilePath	是	否	String	文件路径
FileCreateTime	是	否	Datetime	文件创建时间
LatestTamperedFileMTime	是	否	Datetime	最近被篡改文件创建时间
NewFile	是	否	String	新文件内容
FileDiff	是	否	String	新旧文件的差异

CKafkaInstanceInfo

安全日志kafka可选信息

被如下接口引用：DescribeSecLogDeliveryKafkaOptions

名称	必选	允许NULL	类型	描述
InstanceID	否	是	String	实例ID
InstanceName	否	是	String	实例名称
TopicList	否	是	Array of CKafkaTopicInfo	主题列表
RouteList	否	是	Array of CkafkaRouteInfo	路由列表
KafkaVersion	否	是	String	kafka版本号

ImageHost

容器安全 主机镜像关联列表

被如下接口引用：DescribeAssetImageHostList

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
ImageID	是	否	String	镜像id
HostID	是	否	String	主机id

PodContainerInfo

Pod关联的容器信息

被如下接口引用：DescribePodContainers

名称	必选	允许NULL	类型	描述
ContainerName	是	否	String	容器名称
ContainerId	是	否	String	容器id
Status	是	否	String	运行状态
ImageName	是	否	String	镜像名
ImageID	是	否	String	镜像ID
CPU	是	否	Uint64	CPU使用率
Memory	是	否	Uint64	内存使用 KB
RestartCount	是	否	Uint64	重启次数

ClusterNamespaceInfo

集群命名空间信息

被如下接口引用：DescribeClustersNamespaces

名称	必选	允许NULL	类型	描述
Name	是	否	String	名称
Labels	是	否	String	标签
CreationTime	是	否	String	创建时间

ComplianceAffectedAsset

表示检测项所影响的资产的信息。

被如下接口引用：DescribeCompliancePolicyItemAffectedAssetList

名称	必选	允许NULL	类型	描述
CustomerAssetId	是	否	Uint64	为客户分配的唯一的资产项的ID。
AssetName	是	否	String	资产项的名称。
AssetType	是	否	String	资产项的类型

名称	必选	允许NULL	类型	描述
CheckStatus	是	否	String	检测状态CHECK_INIT, 待检测CHECK_RUNNING, 检测中CHECK_FINISHED, 检测完成CHECK_FAILED, 检测失败
NodeName	是	否	String	节点名称。
LastCheckTime	是	否	String	上次检测的时间，格式为"YYYY-MM-DD HH:m::SS"。如果没有检测过，此处为"0000-00-00 00:00:00"。
CheckResult	是	否	String	检测结果。取值为：RESULT_FAILED: 未通过RESULT_PASSED: 通过
HostIP	是	是	String	主机IP
ImageTag	是	是	String	镜像的tag
VerifyInfo	是	是	String	检查项验证信息
InstanceId	是	是	String	主机实例id

EscapeEventInfo

容器逃逸事件列表

被如下接口引用：DescribeEscapeEventInfo

名称	必选	允许NULL	类型	描述
EventType	是	否	String	事件类型 ESCAPE_CGROUPS：利用cgroup机制逃逸 ESCAPE_TAMPER_SENSITIVE_FILE：篡改敏感文件逃逸 ESCAPE_DOCKER_API：访问Docker API接口逃逸 ESCAPE_VUL_OCCURRED：逃逸漏洞利用 MOUNT_SENSITIVE_PTAH：敏感路径挂载 PRIVILEGE_CONTAINER_START：特权容器 PRIVILEGE：程序提权逃逸
ContainerName	是	否	String	容器名
ImageName	是	否	String	镜像名
Status	是	否	String	状态，EVENT_UNDEAL:未处理，EVENT_DEALED:已处理，EVENT_INGNORE:忽略
EventId	是	否	String	事件记录的唯一id
NodeName	是	否	String	节点名称
PodName	是	否	String	pod(实例)的名字
FoundTime	是	否	Datetime	生成时间
EventName	是	否	String	事件名字，宿主机文件访问逃逸、Syscall逃逸、MountNamespace逃逸、程序提权逃逸、特权容器启动逃逸、敏感路径挂载
ImageId	是	否	String	镜像id，用于跳转
ContainerId	是	否	String	容器id，用于跳转
Solution	是	否	String	事件解决方案
Description	是	否	String	事件描述
EventCount	是	否	Int64	事件数量

名称	必选	允许NULL	类型	描述
LatestFoundTime	是	否	Datetime	最近生成时间
NodeIP	是	是	String	节点IP
HostID	是	是	String	主机IP
ContainerNetStatus	是	是	String	网络状态未隔离 NORMAL已隔离 ISOLATED隔离中 ISOLATING隔离失败 ISOLATE_FAILED解除隔离中 RESTORING解除隔离失败 RESTORE_FAILED
ContainerNetSubStatus	是	是	String	容器子状态"AGENT_OFFLINE" //Agent离线"NODE_DESTROYED" //节点已销毁"CONTAINER_EXITED" //容器已退出"CONTAINER_DESTROYED" //容器已销毁"SHARED_HOST" // 容器与主机共享网络"RESOURCE_LIMIT" //隔离操作资源超限"UNKNOW" // 原因未知
ContainerIsolateOperationSrc	是	是	String	容器隔离操作来源
ContainerStatus	是	否	String	容器状态正在运行: RUNNING暂停: PAUSED停止: STOPPED已经创建: CREATED已经销毁: DESTROYED正在重启中: RESTARTING迁移中: REMOVING
ClusterID	否	否	String	节点所属集群ID
NodeType	否	否	String	节点类型：NORMAL普通节点、SUPER超级节点
PodIP	否	否	String	pod ip
NodeUniqueID	否	否	String	节点唯一id
PublicIP	否	否	String	节点公网ip
NodeID	否	否	String	节点id
HostIP	否	否	String	节点内网ip
ClusterName	否	否	String	集群名称

ImageDenyEvent

镜像拦截事件

被如下接口引用：DescribeImageDenyEventList

名称	必选	允许NULL	类型	描述
EventType	是	否	String	事件类型 EVENT_RISK:风险事件类型，EVENT_PRIVILEGE:特权
RuleName	是	否	String	规则名称
RuleID	是	否	String	规则RuleID
RuleType	是	否	String	规则类型
RuleStatus	是	否	Int64	规则启用状态 0:开启，1:关闭
RuleEffectStatus	是	否	String	规则策略状态 IN_THE_TEST ：观察中，IN_EFFECT：生效中
RuleInfo	是	是	Array of String	规则内容

名称	必选	允许NULL	类型	描述
RuleDescription	是	否	String	规则描述
ImageID	是	否	String	镜像ID
ImageName	是	否	String	镜像名称
NodeName	是	否	String	节点名称
NodeIP	是	否	String	内网IP
QUUID	是	否	String	主机Quuid
FoundTime	是	否	String	首次生成时间
LatestFoundTime	是	否	String	最近生成时间
EventCount	是	否	Int64	事件数量
DealBehavior	是	否	String	执行动作:BEHAVIOR_ALERT:告警，BEHAVIOR_HOLDUP_SUCCESSED:拦截
EventID	是	否	Int64	事件ID
PublicIP	是	否	String	外网IP
NodeID	否	否	String	节点ID
ClusterID	否	否	String	集群ID
NodeType	否	否	String	节点类型
NodeUniqueID	否	否	String	超级节点唯一id
PodIP	否	否	String	pod ip
PodName	否	否	String	pod name
ClusterName	否	否	String	集群名称

UnauthorizedCoresTendency

未授权核数趋势

被如下接口引用：DescribeUnauthorizedCoresTendency

名称	必选	允许NULL	类型	描述
DateTime	是	否	String	日期
CoresCount	是	否	Int64	未授权的核数

SecLogJoinSuperObjectInfo

安全日志接入超级对象详情

被如下接口引用：DescribeSecLogJoinSuperObjectList

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
NodeID	否	是	String	超级节点ID
NodeName	否	是	String	超级节点名称
ClusterName	否	是	String	所属集群名
ClusterID	否	是	String	所属集群ID
ClusterVersion	否	是	String	集群版本
Status	否	是	String	节点状态:Running,Ready,Notready,Initializing,Failed,Error
SubNetID	否	是	String	子网ID
SubNetName	否	是	String	子网名称
SubNetCidr	否	是	String	子网网段
RelatePodCount	否	是	Uint64	关联pod数
RelateContainerCount	否	是	Uint64	关联容器数
NodeUniqueID	否	是	String	节点唯一id
JoinState	否	是	Bool	接入状态(true:已接入 false:未接入)

RunTimeRiskInfo

运行时风险信息

被如下接口引用：DescribeImageRiskSummary

名称	必选	允许NULL	类型	描述
Cnt	是	否	Uint64	数量
Level	是	否	String	风险等级：CRITICAL: 严重HIGH: 高MEDIUM：中LOW: 低

WhiteListWorkload

查询集群安全白名单的workload信息

被如下接口引用：DescribeClusterWorkloadWhiteList

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	加入白名单的时间
WorkloadId	是	否	Uint64	白名单的workloadId
ClusterId	是	否	String	集群Id
ClusterName	是	否	String	集群名字
WorkloadName	是	否	String	工作负载名称
WorkloadType	是	否	String	工作负载类型

名称	必选	允许NULL	类型	描述
Region	是	否	String	地域

ImageRepoRegistryInfo

容器安全镜像仓库列表

被如下接口引用：DescribeAssetImageRegistryRegistryList

名称	必选	允许NULL	类型	描述
RegistryId	否	否	Uint64	仓库id
Name	否	否	String	仓库名
RegistryType	否	否	String	仓库类型，列表：harbor、tcr
Url	否	否	String	仓库url
NetType	否	否	String	网络类型，列表：public
RegistryRegion	否	否	String	区域，列表：default
RegistryVersion	否	否	String	仓库版本
ConnectStatus	否	否	String	仓库连接状态连接状态，成功：success 失败：failed，待废弃，请使用ConnDetectStatus
ConnectMsg	否	是	String	仓库连接错误信息，待废弃，请使用ConnDetectException
ConnDetectType	否	否	String	联通性检测方式
ConnDetectHostCount	否	否	Uint64	联通性检测主机数
ConnDetectDetail	否	否	Array of RegistryConnDetectResult	联通性检测详情
InstanceID	否	否	String	tcr情况下的instance_id
LatestSyncTime	否	否	String	最近同步成功时间
SyncStatus	否	否	String	同步状态
SyncFailReason	否	否	String	同步失败原因
SyncSolution	否	否	String	同步失败解决方案
SyncMessage	否	否	String	同步失败信息

ComponentInfo

容器组件信息

被如下接口引用：DescribeAssetComponentList

名称	必选	允许NULL	类型	描述
Name	是	否	String	名称

名称	必选	允许NULL	类型	描述
Version	是	否	String	版本

ImageVul

容器安全镜像漏洞信息

被如下接口引用：DescribeAssetImageRegistryVulList

名称	必选	允许NULL	类型	描述
CVEID	否	是	String	漏洞id
POCID	否	是	String	观点验证程序id
Name	否	是	String	漏洞名称
Components	否	是	Array of ComponentsInfo	涉及组件信息
Category	否	是	String	分类
CategoryType	否	是	String	分类2
Level	否	是	String	风险等级
Des	否	是	String	描述
OfficialSolution	否	是	String	解决方案
Reference	否	是	String	引用
DefenseSolution	否	是	String	防御方案
SubmitTime	否	是	String	提交时间
CvssScore	否	是	String	Cvss分数
CvssVector	否	是	String	Cvss信息
IsSuggest	否	是	String	是否建议修复
FixedVersions	否	是	String	修复版本号
Tag	否	是	Array of String	漏洞标签:"CanBeFixed","DynamicLevelPoc","DynamicLevelExp"
Component	否	是	String	组件名
Version	否	是	String	组件版本
AttackLevel	否	是	Int64	攻击热度 0-3
LayerInfos	否	是	Array of ImageVulLayerInfo	镜像层信息列表

IACItem

IAC检测结果

被如下接口引用：DescribeIACCheckResultList

名称	必选	允许NULL	类型	描述
RuleName	否	是	String	规则名
Severity	否	是	String	严重程度
RuleID	否	是	String	规则ID
ResourceName	否	是	String	资源名称
ResourceType	否	是	String	资源类型
Category	否	是	String	种类
Description	否	是	String	规则描述
ScanTime	否	是	String	扫描时间
Passed	否	是	String	是否通过;Pass:通过;NoPass:不通过

VirusInfo

运行时木马列表信息

被如下接口引用：DescribeVirusList

名称	必选	允许NULL	类型	描述
FileName	是	否	String	文件名称
FilePath	是	否	String	文件路径
VirusName	是	否	String	病毒名称
CreateTime	是	否	String	创建时间
ModifyTime	是	否	String	更新时间
ContainerName	是	否	String	容器名称
ContainerId	是	否	String	容器id
ContainerStatus	是	否	String	容器状态正在运行: RUNNING暂停: PAUSED停止: STOPPED已经创建: CREATED已经销毁: DESTROYED正在重启中: RESTARTING迁移中: REMOVING
ImageName	是	否	String	镜像名称
ImageId	是	否	String	镜像id
Status	是	否	String	DEAL_NONE:文件待处理DEAL_IGNORE:已经忽略DEAL_ADD_WHITELIST:加白DEAL_DEL:文件已经删除DEAL_ISOLATE:已经隔离DEAL_ISOLATING:隔离中DEAL_ISOLATE_FAILED:隔离失败DEAL_RECOVERING:恢复中DEAL_RECOVER_FAILED: 恢复失败
Id	是	否	String	事件id
HarmDescribe	是	否	String	事件描述
SuggestScheme	是	否	String	建议方案

名称	必选	允许NULL	类型	描述
SubStatus	是	否	String	失败子状态:FILE_NOT_FOUND:文件不存在FILE_ABNORMAL:文件异常FILE_ABNORMAL_DEAL_RECOVER:恢复文件时，文件异常BACKUP_FILE_NOT_FOUND:备份文件不存在CONTAINER_NOT_FOUND_DEAL_ISOLATE:隔离时，容器不存在CONTAINER_NOT_FOUND_DEAL_RECOVER:恢复时，容器不存在TIMEOUT: 超时TOO_MANY: 任务过多OFFLINE: 离线INTERNAL: 服务内部错误VALIDATION: 参数非法
ContainerNetStatus	是	否	String	网络状态未隔离 NORMAL已隔离 ISOLATED隔离中 ISOLATING隔离失败 ISOLATE_FAILED解除隔离中 RESTORING解除隔离失败 RESTORE_FAILED
ContainerNetSubStatus	是	否	String	容器子状态"AGENT_OFFLINE" //Agent离线 "NODE_DESTROYED" //节点已销毁 "CONTAINER_EXITED" //容器已退出 "CONTAINER_DESTROYED" //容器已销毁 "SHARED_HOST" // 容器与主机共享网络 "RESOURCE_LIMIT" //隔离操作资源超限 "UNKNOW" // 原因未知
ContainerIsolateOperationSrc	是	否	String	容器隔离操作来源
MD5	是	是	String	md5值
RiskLevel	是	是	String	风险等级 RISK_CRITICAL, RISK_HIGH, RISK_MEDIUM, RISK_LOW, RISK_NOTICE。
CheckPlatform	是	是	Array of String	检测平台1: 云查杀引擎2: tav3: binaryAi4: 异常行为5: 威胁情报
NodeID	否	否	String	节点ID
NodeName	否	否	String	节点名称
PodIP	否	否	String	pod ip
PodName	否	否	String	pod(实例)的名字
ClusterID	否	否	String	节点所属集群ID
NodeType	否	否	String	节点类型：NORMAL普通节点、SUPER超级节点
PublicIP	否	否	String	节点外网IP
InnerIP	否	否	String	节点内网IP
NodeUniqueID	否	否	String	节点唯一ID
HostID	否	否	String	普通节点ID
ClusterName	否	否	String	集群名称

CkafkaRouteInfo

ckafkal路由详情

被如下接口引用：DescribeSecLogDeliveryKafkaOptions

名称	必选	允许NULL	类型	描述
RouteID	否	是	Int64	路由ID

名称	必选	允许NULL	类型	描述
Domain	否	是	String	域名名称
DomainPort	否	是	Uint64	域名端口
Vip	否	是	String	虚拟ip
VipType	否	是	Int64	虚拟ip类型
AccessType	否	是	Int64	接入类型// 0：PLAINTEXT (明文方式，没有带用户信息老版本及社区版本都支持) // 1：SASL_PLAINTEXT（明文方式，不过在数据开始时，会通过SASL方式登录鉴权，仅社区版本支持） // 2：SSL（SSL加密通信，没有带用户信息，老版本及社区版本都支持） // 3：SASL_SSL（SSL加密通信，在数据开始时，会通过SASL方式登录鉴权，仅社区版本支持）

RiskSyscallEventDescription

运行时容器高危系统调用事件描述信息

被如下接口引用：DescribeRiskSyscallDetail

名称	必选	允许NULL	类型	描述
Description	是	否	String	描述信息
Solution	是	否	String	解决方案
Remark	是	是	String	事件备注信息
SyscallName	是	否	String	系统调用名称
OperationTime	是	是	String	事件最后一次处理的时间

SuperNodeInstallTaskDetailInfo

超级节点安装任务详情

被如下接口引用：DescribeSuperNodeInstallTaskDetail

名称	必选	允许NULL	类型	描述
NodeID	否	否	String	超级节点 ID
NodeName	否	否	String	超级节点名称
NodeStatus	否	否	String	超级节点状态 Running //运行中
Ready //准备				
Notready //未准备好				
Initializing //初始化				
Failed //失败				
Error //错误				
ClusterID	否	否	String	集群ID
ClusterName	否	否	String	集群名称

名称	必选	允许NULL	类型	描述
TaskStatus	否	否	String	任务状态 INSTALLING:安装中;
INSTALL_FAILURE:安装失败;				
INSTALL_SUCCESS:安装成功				
Message	否	否	String	安装任务信息
NodeUniqueID	否	否	String	超级节点唯一id
ContainerCount	否	否	Uint64	容器数
PodCount	否	否	Uint64	pod数

CompliancePeriodTask

表示一个合规基线检测定时任务的信息。

被如下接口引用：DescribeCompliancePeriodTaskList

名称	必选	允许NULL	类型	描述
PeriodTaskId	是	否	Uint64	周期任务的ID
AssetType	是	否	String	资产类型。ASSET_CONTAINER, 容器ASSET_IMAGE, 镜像ASSET_HOST, 主机ASSET_K8S, K8S资产
LastTriggerTime	是	是	Datetime	最近一次触发的时间
TotalPolicyItemCount	是	否	Uint64	总的检查项数目
PeriodRule	是	否	CompliancePeriodTaskRule	周期设置
BenchmarkStandardSet	是	否	Array of ComplianceBenchmarkStandard	合规标准列表

K8sApiAbnormalEventInfo

k8sApi异常事件详情

被如下接口引用：DescribeK8sApiAbnormalEventInfo

名称	必选	允许NULL	类型	描述
MatchRuleName	是	否	String	命中规则名称
MatchRuleType	是	否	String	命中规则类型
RiskLevel	是	否	String	告警等级
ClusterID	是	否	String	集群ID
ClusterName	是	否	String	集群名称
ClusterRunningStatus	是	否	String	集群运行状态
FirstCreateTime	是	否	String	初次生成时间

名称	必选	允许NULL	类型	描述
LastCreateTime	是	否	String	最近一次生成时间
AlarmCount	是	否	Uint64	告警数量
Status	是	否	String	状态"EVENT_UNDEAL":未处理"EVENT_DEALED": 已处理"EVENT_IGNORE": 忽略"EVENT_DEL": 删除"EVENT_ADD_WHITE": 加白
ClusterMasterIP	是	否	String	集群masterIP
K8sVersion	是	否	String	k8s版本
RunningComponent	是	否	Array of String	运行时组件
Desc	是	否	String	描述
Suggestion	是	否	String	建议
Info	是	否	String	请求信息
MatchRuleID	是	否	String	规则ID
HighLightFields	是	否	Array of String	高亮字段数组
MatchRule	是	否	K8sApiAbnormalRuleScopeInfo	命中规则

NetworkCustomPolicy

网络集群策略自定义规则

被如下接口引用：AddAndPublishNetworkFirewallPolicyDetail、AddNetworkFirewallPolicyDetail、DescribeNetworkFirewallPolicyDetail、UpdateAndPublishNetworkFirewallPolicyDetail、UpdateNetworkFirewallPolicyDetail

名称	必选	允许NULL	类型	描述
Direction	是	否	String	网络策略方向，分为FROM和TO
Ports	否	是	Array of NetworkPorts	网络策略策略端口
Peer	否	是	Array of NetworkPeer	网络策略策略对象开启待确认：PublishedNoConfirm开启已确认：PublishedConfirmed关闭中：unPublishing开启中：Publishing待开启：unPublishEdit

NetworkTopologyPodList

容器网络pod列表

被如下接口引用：DescribeNetworkTopologyWorkLoadDetail

名称	必选	允许NULL	类型	描述
PodName	否	是	String	pod名称
PodStatus	否	是	String	pod状态
PodLabels	否	是	String	pod标签

名称	必选	允许NULL	类型	描述
PodIp	否	是	String	pod Ip
NodeIp	否	是	String	Node ip
CreateTime	否	是	String	创建时间

NetworkClusterPodInfo

网络集群pod返回的结构体

被如下接口引用：DescribeNetworkFirewallPodLabelsList

名称	必选	允许NULL	类型	描述
PodName	是	否	String	pod名字
Namespace	是	是	String	pod空间
Labels	是	是	String	pod标签
WorkloadKind	是	是	String	pod类型

ProcessDetailInfo

运行是安全详情，进程信息

被如下接口引用：DescribeAbnormalProcessDetail、DescribeAccessControlDetail、DescribeEscapeEventDetail、DescribeReverseShellDetail、DescribeRiskSyscallDetail

名称	必选	允许NULL	类型	描述
ProcessName	是	否	String	进程名称
ProcessAuthority	是	否	String	进程权限
ProcessId	是	否	Uint64	进程pid
ProcessStartUser	是	否	String	进程启动用户
ProcessUserGroup	是	否	String	进程用户组
ProcessPath	是	否	String	进程路径
ProcessTree	是	否	String	进程树
ProcessMd5	是	否	String	进程md5
ProcessParam	是	否	String	进程命令行参数

WhiteListRegexpExpressionInfo

白名单正则表达式信息

被如下接口引用：AddModEscapeRegexpWhiteList、AddModReverseShellRegexpWhiteList、DescribeEscapeRegexpWhiteListInfo、DescribeReverseShellRegexpWhiteListInfo

名称	必选	允许NULL	类型	描述
LogicSymbol	否	是	String	逻辑符号
与 (AND)				
或 (OR)				
非 (NOT)				
MatchField	否	是	String	匹配字段
MatchContent	否	是	String	匹配内容

ComplianceAssetInfo

表示一项资产的信息。

被如下接口引用：DescribeComplianceAssetList

名称	必选	允许NULL	类型	描述
CustomerAssetId	是	否	Uint64	客户资产的ID。
AssetType	是	否	String	资产类别。
AssetName	是	否	String	资产的名称。
ImageTag	是	是	String	当资产为镜像时，这个字段为镜像Tag。
HostIP	是	否	String	资产所在的主机IP。
NodeName	是	否	String	资产所属的节点的名称
CheckStatus	是	否	String	检测状态CHECK_INIT, 待检测CHECK_RUNNING, 检测中CHECK_FINISHED, 检测完成CHECK_FAILED, 检测失败
PassedPolicyItemCount	是	是	Uint64	此类资产通过的检测项的数目。
FailedPolicyItemCount	是	是	Uint64	此类资产未通过的检测的数目。
LastCheckTime	是	是	Datetime	上次检测的时间。
CheckResult	是	是	String	检测结果：RESULT_FAILED: 未通过。RESULT_PASSED: 通过。
InstanceId	是	是	String	主机节点的实例id

AutoAuthorizedImageInfo

镜像自动授权结果信息

被如下接口引用：DescribeImageAutoAuthorizedLogList

名称	必选	允许NULL	类型	描述
ImageId	是	否	String	镜像id

名称	必选	允许NULL	类型	描述
ImageName	是	否	String	镜像名称
AuthorizedTime	是	否	String	授权时间
Status	是	否	String	授权结果，SUCCESS:成功，REACH_LIMIT:达到授权上限，LICENSE_INSUFFICIENT:授权数不足'
IsAuthorized	是	否	Uint64	是否授权，1：是，0：否

AccessControlChildRuleInfo

容器运行时安全，访问控制子策略信息

被如下接口引用：AddEditAccessControlRule、DescribeAccessControlDetail、DescribeAccessControlRuleDetail

名称	必选	允许NULL	类型	描述
RuleId	否	是	String	子策略id
RuleMode	是	否	String	策略模式, RULE_MODE_RELEASE: 放行 RULE_MODE_ALERT: 告警 RULE_MODE_HOLDUP: 拦截
ProcessPath	是	否	String	进程路径
TargetFilePath	是	否	String	被访问文件路径，仅仅在访问控制生效

ClusterServiceInfo

集群的Service信息

被如下接口引用：DescribeClusterServiceList

名称	必选	允许NULL	类型	描述
Name	否	否	String	service名称.
Type	否	否	String	service类型
Selectors	否	否	String	Selector信息
SelectorCount	否	否	Uint64	Selector数量
ExternalIp	否	否	String	负载均衡Ip
ClusterIp	否	否	String	服务Ip
Port	否	否	String	string类型,以,分隔
ClusterName	否	否	String	所属集群名字
ClusterId	否	否	String	所属集群Id
PodName	否	否	String	关联Pod名字
PodCount	否	否	Uint64	关联pod数量
CreationTime	否	否	String	创建时间

名称	必选	允许NULL	类型	描述
Namespace	否	否	String	命名空间
Region	否	否	String	地域
Labels	否	否	String	标签
ClusterStatus	否	否	String	集群状态
ClusterType	否	否	String	集群类型
ServiceUniqueID	否	是	String	service唯一标识符

ImagesInfo

容器安全镜像列表

被如下接口引用：DescribeAssetImageList

名称	必选	允许NULL	类型	描述
ImageID	否	否	String	镜像id
ImageName	否	否	String	镜像名称
CreateTime	否	否	String	创建时间
Size	否	否	Uint64	镜像大小
HostCnt	否	否	Uint64	主机个数
ContainerCnt	否	否	Uint64	容器个数
ScanTime	否	否	String	扫描时间
VulCnt	否	否	Uint64	漏洞个数
VirusCnt	否	否	Uint64	病毒个数
RiskCnt	否	否	Uint64	敏感信息个数
IsTrustImage	否	否	Bool	是否信任镜像
OsName	否	否	String	镜像系统
AgentError	否	否	String	agent镜像扫描错误
ScanError	否	否	String	后端镜像扫描错误
ScanStatus	否	否	String	扫描状态
ScanVirusError	否	否	String	木马扫描错误信息
ScanVulError	否	否	String	漏洞扫描错误信息
ScanRiskError	否	否	String	风险扫描错误信息
IsSuggest	否	否	Uint64	是否是重点关注镜像，为0不是，非0是
IsAuthorized	否	否	Uint64	是否授权，1是0否
ComponentCnt	否	否	Uint64	组件个数

名称	必选	允许NULL	类型	描述
CriticalLevelVulCnt	否	否	Uint64	严重漏洞数
HighLevelVulCnt	否	否	Uint64	高危漏洞数
MediumLevelVulCnt	否	否	Uint64	中危漏洞数
LowLevelVulCnt	否	否	Uint64	低危漏洞数
IsLatestImage	否	否	Bool	是否最新版本镜像
RecommendedFix	否	否	Bool	是否推荐处置

ImagesBindRuleSimpleInfo

查询镜像绑定的运行时规则信息

被如下接口引用：

名称	必选	允许NULL	类型	描述
ImageId	是	否	String	镜像id
ImageName	是	否	String	镜像名称
RuleId	是	否	String	绑定规则id
RuleName	是	否	String	规则名字

ClsLogsetInfo

cls日志集信息

被如下接口引用：DescribeSecLogDeliveryClsOptions

名称	必选	允许NULL	类型	描述
LogsetID	是	否	String	日志集ID
LogsetName	否	是	String	日志集名称
TopicList	否	是	Array of ClsTopicInfo	cls主题列表

VulDefenceEventDetail

漏洞防御事件详情

被如下接口引用：DescribeVulDefenceEventDetail

名称	必选	允许NULL	类型	描述
CVEID	否	否	String	漏洞CVEID
VulName	否	否	String	漏洞名称
PocID	否	否	String	漏洞PocID

名称	必选	允许NULL	类型	描述
EventType	否	否	String	入侵状态
SourceIP	否	否	String	攻击源IP
City	否	否	String	攻击源ip地址所在城市
EventCount	否	否	Int64	事件数量
ContainerID	否	否	String	容器ID
ContainerName	否	否	String	容器名称
ImageID	否	否	String	镜像ID
ImageName	否	否	String	镜像名称
Status	否	否	String	处理状态
SourcePort	否	否	Array of String	攻击源端口
EventID	否	否	Int64	事件ID
HostName	否	否	String	主机名称/超级节点名称
HostIP	否	否	String	主机内网IP
PublicIP	否	否	String	主机外网IP
PodName	否	否	String	Pod名称
Description	否	否	String	危害描述
OfficialSolution	否	否	String	修复建议
NetworkPayload	否	否	String	攻击包
PID	否	是	Int64	进程PID
MainClass	否	是	String	进程主类名
StackTrace	否	是	String	堆栈信息
ServerAccount	否	是	String	监听账号
ServerPort	否	是	String	监听端口
ServerExe	否	是	String	进程路径
ServerArg	否	是	String	进程命令行参数
QUUID	否	是	String	主机QUUID/超级节点ID
ContainerNetStatus	否	是	String	隔离状态未隔离 NORMAL已隔离 ISOLATED隔离中 ISOLATING隔离失败 ISOLATE_FAILED解除隔离中 RESTORING解除隔离失败 RESTORE_FAILED
ContainerNetSubStatus	否	是	String	容器子状态"AGENT_OFFLINE" //Agent离线 "NODE_DESTROYED" //节点已销毁 "CONTAINER_EXITED" //容器已退出 "CONTAINER_DESTROYED" //容器已销毁 "SHARED_HOST" // 容器与主机共享网络 "RESOURCE_LIMIT" //隔离操作资源超限 "UNKNOW" // 原因未知

名称	必选	允许NULL	类型	描述
ContainerIsolateOperationSrc	否	是	String	容器隔离操作来源
ContainerStatus	否	是	String	容器状态正在运行: RUNNING暂停: PAUSED停止: STOPPED已经创建: CREATED已经销毁: DESTROYED正在重启中: RESTARTING迁移中: REMOVING
JNDIUrl	否	是	String	接口Url
RaspDetail	否	是	Array of RaspInfo	rasp detail
NodeSubNetName	否	否	String	超级节点子网名称
NodeSubNetCIDR	否	否	String	超级节点子网网段
PodIP	否	否	String	pod ip
NodeType	否	否	String	节点类型[NORMAL:普通节点|SUPER:超级节点]
NodeID	否	否	String	超级节点ID
NodeUniqueID	否	否	String	超级节点唯一ID
NodeSubNetID	否	否	String	超级节点子网ID
ClusterID	否	否	String	集群ID
ClusterName	否	否	String	集群名称
Namespace	否	否	String	Namespace
WorkloadType	否	否	String	工作负载

SuperNodeListItem

超级节点信息

被如下接口引用：DescribeAssetSuperNodeList

名称	必选	允许NULL	类型	描述
NodeID	否	否	String	超级节点ID
NodeName	否	否	String	超级节点名称
ClusterName	否	否	String	所属集群名
ClusterID	否	否	String	所属集群ID
Status	否	否	String	节点状态:Running,Ready,Notready,Initializing,Failed,Error
SubNetID	否	否	String	子网ID
SubNetName	否	否	String	子网名称
SubNetCidr	否	否	String	子网网段
ZoneID	否	否	String	可用区ID
Zone	否	否	String	可用区

名称	必选	允许NULL	类型	描述
CreateTime	否	否	String	创建时间
RelatePodCount	否	否	Uint64	关联pod数
RelateContainerCount	否	否	Uint64	关联容器数
AgentStatus	否	否	String	agent安装状态UNINSTALL:未安装;INSTALLED:已安装;INSTALLING:安装中;
NodeUniqueID	否	否	String	节点唯一id
ClusterAccessedStatus	否	否	String	集群接入状态
ChargeCoresCnt	否	否	Uint64	计费核数
DefendStatus	否	否	String	防护状态:
已防护: Defended				
未防护: UnDefended				

ScanRangeInfo

扫描范围信息

被如下接口引用：CreateVirusScanNewTask、DescribeVirusEstimateScanTime、DescribeVirusScanConfig、ModifyVirusScanConfig

名称	必选	允许NULL	类型	描述
IsAll	否	否	Bool	true:选择全部；
false:部分选择				
RangeType	否	否	String	SCAN_NORMAL:普通节点；
SCAN_SUPER:超级节点				
SCAN_CONTAINER:容器				
IDs	否	否	Array of String	选择的ID

VulAffectedContainerInfo

受漏洞影响的容器信息

被如下接口引用：DescribeVulContainerList

名称	必选	允许NULL	类型	描述
HostIP	是	否	String	内网IP
ContainerID	是	否	String	容器ID
ContainerName	是	否	String	容器名称
PodName	是	否	String	Pod名称
PodIP	是	否	String	PodIP值

名称	必选	允许NULL	类型	描述
HostName	是	否	String	主机名称
HostID	是	否	String	主机ID
PublicIP	是	否	String	外网IP
ClusterID	否	否	String	集群ID
ClusterName	否	否	String	集群名称
NodeType	否	否	String	节点类型[NORMAL:普通节点|SUPER:超级节点]
NodeUniqueID	否	否	String	超级节点唯一ID
NodeID	否	否	String	超级节点ID
NodeName	否	否	String	超级节点名称

ComponentsInfo

组件信息

被如下接口引用：DescribeAssetImageRegistryImageLayerDetail、DescribeAssetImageRegistryVulList

名称	必选	允许NULL	类型	描述
Component	否	是	String	组件名称
Version	是	是	String	组件版本信息
FixedVersion	否	是	String	可修复版本
Path	否	是	String	路径
Type	否	是	String	类型
Name	否	是	String	组件名称

ServiceInfo

容器安全服务信息列表

被如下接口引用：DescribeAssetAppServiceList、DescribeAssetDBServiceList、DescribeAssetWebServiceList

名称	必选	允许NULL	类型	描述
ServiceID	是	否	String	服务id
HostID	是	否	String	主机id
HostIP	是	否	String	主机ip
ContainerName	是	否	String	容器名
Type	是	否	String	服务名 例如nginx/redis
Version	是	否	String	版本

名称	必选	允许NULL	类型	描述
RunAs	是	否	String	账号
Listen	是	否	Array of String	监听端口
Config	是	否	String	配置
ProcessCnt	是	否	Uint64	关联进程数
AccessLog	是	否	String	访问日志
ErrorLog	是	否	String	错误日志
DataPath	是	否	String	数据目录
WebRoot	是	否	String	web目录
Pids	是	否	Array of Uint64	关联的进程id
MainType	是	否	String	服务类型 app,web,db
Exe	是	否	String	执行文件
Parameter	是	否	String	服务命令行参数
ContainerId	是	否	String	容器id
HostName	是	否	String	主机名称
PublicIp	是	否	String	外网ip
NodeID	否	否	String	节点id
PodIP	否	否	String	podip
PodName	否	否	String	pod名称
NodeType	否	否	String	节点类型
NodeUniqueID	否	否	String	超级节点唯一id

AccessControlSystemChildRuleInfo

容器运行时安全，访问控制系统策略的子策略信息

被如下接口引用：AddEditAccessControlRule、DescribeAccessControlRuleDetail

名称	必选	允许NULL	类型	描述
RuleId	是	否	String	子策略Id
RuleMode	是	否	String	策略模式, RULE_MODE_RELEASE: 放行 RULE_MODE_ALERT: 告警 RULE_MODE_HOLDUP:拦截
IsEnable	是	否	Bool	子策略状态，true为开启，false为关闭
RuleType	是	否	String	子策略检测的入侵行为类型CHANGE_CRONTAB：篡改计划任务CHANGE_SYS_BIN：篡改系统程序CHANGE_USRCFG：篡改用户配置

ClusterNodeInfo

集群的节点信息

被如下接口引用：DescribeClusterNodes

名称	必选	允许NULL	类型	描述
InstanceId	否	否	String	实例id
PrivateIpAddresses	否	否	String	内网ip地址
InstanceRole	否	否	String	节点的角色，Master、Work等
InstanceState	否	否	String	实例的状态（running 运行中，initializing 初始化中，failed 异常）
NodeName	否	否	String	节点名称
AgentStatus	否	是	String	agent安装状态
PublicIP	否	是	String	公网ip
HostID	否	是	String	节点ID
MachineType	否	是	String	主机类型(普通节点情况)
NodeType	否	是	String	节点类型(
NORMAL: 普通节点				
SUPER:超级节点				
)				
UUID	否	是	String	uuid
ChargeCoresCnt	否	是	Uint64	计费核数
DefendStatus	否	是	String	防护状态:
已防护: Defended				
未防护: UnDefended				

ComplianceAssetSummary

表示一类资产的总览信息。

被如下接口引用：DescribeComplianceTaskAssetSummary

名称	必选	允许NULL	类型	描述
AssetType	是	否	String	资产类别。
IsCustomerFirstCheck	是	否	Bool	是否为客户的首次检测。与CheckStatus配合使用。
CheckStatus	是	否	String	检测状态CHECK_UNINIT, 用户未启用此功能CHECK_INIT, 待检测CHECK_RUNNING, 检测中CHECK_FINISHED, 检测完成CHECK_FAILED, 检测失败
CheckProgress	是	是	Float	此类别的检测进度，为 0~100 的数。若未在检测中，无此字段。

名称	必选	允许NULL	类型	描述
PassedPolicyItemCount	是	否	Uint64	此类资产通过的检测项的数目。
FailedPolicyItemCount	是	否	Uint64	此类资产未通过的检测的数目。
FailedCriticalPolicyItemCount	是	否	Uint64	此类资产下未通过的严重级别的检测项的数目。
FailedHighRiskPolicyItemCount	是	否	Uint64	此类资产下未通过的高危检测项的数目。
FailedMediumRiskPolicyItemCount	是	否	Uint64	此类资产下未通过的中危检测项的数目。
FailedLowRiskPolicyItemCount	是	否	Uint64	此类资产下未通过的低危检测项的数目。
NoticePolicyItemCount	是	否	Uint64	此类资产下提示级别的检测项的数目。
PassedAssetCount	是	否	Uint64	通过检测的资产的数目。
FailedAssetCount	是	否	Uint64	未通过检测的资产的数目。
AssetPassedRate	是	否	Float	此类资产的合规率，0~100的数。
ScanFailedAssetCount	是	否	Uint64	检测失败的资产的数目。
CheckCostTime	是	是	Float	上次检测的耗时，单位为秒。
LastCheckTime	是	是	Datetime	上次检测的时间。
PeriodRule	是	否	CompliancePeriodTaskRule	定时检测规则。
OpenPolicyItemCount	否	是	Uint64	已开启的检查项总数
IgnoredPolicyItemCount	否	是	Uint64	已忽略的检查项总数

NetworkPeer

网络集群策略自定义规则

被如下接口引用：AddAndPublishNetworkFirewallPolicyDetail、AddNetworkFirewallPolicyDetail、DescribeNetworkFirewallPolicyDetail、UpdateAndPublishNetworkFirewallPolicyDetail、UpdateNetworkFirewallPolicyDetail

名称	必选	允许NULL	类型	描述
PeerType	是	否	String	对象类型：命名空间：NamespaceSelector，代表NamespaceSelector有值pod类型：PodSelector，代表NamespaceSelector和PodSelector都有值ip类型：IPBlock，代表只有IPBlock有值
NamespaceSelector	否	是	String	空间选择器
PodSelector	否	是	String	pod选择器
IPBlock	否	是	String	Ip选择器

RegexpRuleListItem

正则规则列表Item

被如下接口引用：DescribeEscapeRegexpWhiteList、DescribeReverseShellRegexpWhiteList

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
RuleID	否	是	String	规则ID
RuleName	否	是	String	规则名称
EffectiveExpression	否	是	Uint64	生效表达式个数
UpdateTime	否	是	String	最新编辑时间
OperatorUin	否	是	String	最近编辑账号
Status	否	是	Bool	启用状态

AssetSimpleImageInfo

容器安全资产镜像简略信息

被如下接口引用：DescribeAssetImageSimpleList

名称	必选	允许NULL	类型	描述
ImageID	是	否	String	镜像ID
ImageName	是	否	String	镜像名称
ContainerCnt	是	否	Uint64	关联容器个数
ScanTime	是	否	String	最后扫描时间
Size	是	否	Uint64	镜像大小

ComplianceIgnoredAsset

检查项中忽略的资产信息

被如下接口引用：DescribeCompliancePolicyItemIgnoredAssetList

名称	必选	允许NULL	类型	描述
CustomerAssetId	是	是	String	资产项的ID，如容器id。
AssetName	是	否	String	资产项的名称。
AssetType	是	否	String	资产项的类型
AssetId	是	否	Uint64	为客户分配的唯一的资产项的ID。
AssetStatus	是	是	String	资产状态， CONTAINER_UNKNOWN //未知状态，处于三种状态之外 CONTAINER_EXIT //容器处于退出状态 CONTAINER_RUNNING //容器处于正常运行状态 CONTAINER_PAUSE //容器处于暂停状态 CONTAINER_ERROR //查询容器状态出错
NodeName	是	否	String	节点名称。
HostIP	是	是	String	主机IP
ImageTag	是	是	String	镜像的tag

ExportJobInfo

导出任务详情

被如下接口引用：DescribeExportJobManageList

名称	必选	允许NULL	类型	描述
JobID	是	否	String	任务ID
JobName	是	否	String	任务名称
Source	是	否	String	来源
ExportStatus	是	否	String	导出状态
ExportProgress	是	否	Int64	导出进度
FailureMsg	是	否	String	失败原因
Timeout	是	否	String	超时时间
InsertTime	是	否	String	插入时间

ImagesVul

容器安全镜像漏洞

被如下接口引用：DescribeAssetImageVulList

名称	必选	允许NULL	类型	描述
CVEID	否	否	String	漏洞id
Name	否	否	String	漏洞名称
Component	否	否	String	组件
Version	否	否	String	版本
Category	否	否	String	分类
CategoryType	否	否	String	分类2
Level	否	否	Uint64	风险等级
Des	否	否	String	描述
OfficialSolution	否	否	String	解决方案
Reference	否	否	String	引用
DefenseSolution	否	否	String	防御方案
SubmitTime	否	否	String	提交时间
CVSSV3Score	否	否	Float	CVSS V3分数
CVSSV3Desc	否	否	String	CVSS V3描述
IsSuggest	否	否	Bool	是否是重点关注：true：是，false：不是

名称	必选	允许NULL	类型	描述
FixedVersions	否	是	String	修复版本号
Tag	否	是	Array of String	漏洞标签:"CanBeFixed","DynamicLevelPoc","DynamicLevelExp"
AttackLevel	否	是	Int64	攻击热度

NetworkClusterNamespaceInfo

网络集群网络空间返回的结构体

被如下接口引用：DescribeNetworkFirewallNamespaceList

名称	必选	允许NULL	类型	描述
Labels	是	否	String	网络空间标签
Name	是	否	String	网络空间名字

FocusVulnerabilityRuleItem

重点关注漏洞规则项

被如下接口引用：DescribeVulnerabilityFocusRuleDetail

名称	必选	允许NULL	类型	描述
CvssScore	否	否	Float	CVSS V3评分
Tags	否	是	Array of VulnerabilityFocusRuleTags	漏洞标签

ReverseShellWhiteListBaseInfo

反弹shell白名单信息

被如下接口引用：DescribeReverseShellWhiteLists

名称	必选	允许NULL	类型	描述
Id	是	否	String	白名单id
ImageCount	是	否	Uint64	镜像数量
ProcessName	是	否	String	连接进程名字
DstIp	是	否	String	目标地址ip
CreateTime	是	否	Datetime	创建时间
UpdateTime	是	否	Datetime	更新时间
DstPort	是	否	String	目标端口
IsGlobal	是	否	Bool	是否是全局白名单，true全局
ImageIds	是	否	Array of String	镜像id数组，为空代表全部

K8sApiAbnormalRuleInfo

k8a api 异常请求规则详情

被如下接口引用：CreateK8sApiAbnormalRuleInfo、DescribeK8sApiAbnormalRuleInfo、ModifyK8sApiAbnormalRuleInfo

名称	必选	允许NULL	类型	描述
RuleID	否	否	String	规则ID
RuleName	是	否	String	规则名称
Status	是	否	Bool	状态
RuleInfoList	是	否	Array of K8sApiAbnormalRuleScopeInfo	规则信息列表
EffectClusterIDSet	是	否	Array of String	生效集群IDSet
RuleType	是	否	String	规则类型RT_SYSTEM 系统规则RT_USER 用户自定义
EffectAllCluster	是	否	Bool	是否所有集群生效

VulScanRegistryImageInfo

漏洞扫描的镜像信息

被如下接口引用：DescribeVulScanRegistryImageList

名称	必选	允许NULL	类型	描述
ImageID	是	否	String	镜像ID
ImageName	是	否	String	镜像名称
ScanStatus	是	否	String	扫描状态。NOT_SCAN:未扫描，SCANNING:扫描中,SCANNED:完成，CANCELED：扫描停止;SCAN_ERR：检查失败
ScanDuration	是	是	Int64	扫描时长
HighLevelVulCount	是	否	Int64	高危漏洞数
MediumLevelVulCount	是	否	Int64	中危漏洞数
LowLevelVulCount	是	否	Int64	低危漏洞数
CriticalLevelVulCount	是	否	Int64	严重漏洞数
ImageTag	是	否	String	镜像版本
ImageRepoAddress	是	否	String	镜像地址
ScanStartTime	是	否	String	漏洞扫描的开始时间
ScanEndTime	是	否	String	漏洞扫描的结束时间
Message	是	否	String	扫描任务消息"MessageRegistryDownload": "仓库镜像层下载错误","MessageRegistryNet": "仓库镜像层信息获取错误，可能原因是仓库未开启外网访问","MessageRegistryTimeout": "仓库镜像任务超时","MessageRegistryScan": "仓库镜像扫描错误","MessageRegistryInner": "仓库内部拉取错误,请检查仓库配置","MessageRegistryInnerTimeout": "仓库内部拉取超时,可能原因是仓库未开启外网访问"

名称	必选	允许NULL	类型	描述
IsLatestImage	是	否	Bool	是否是最新镜像
Id	是	否	Uint64	仓库内部镜像ID

RegistryConnDetectParam

镜像仓库联通性检测

被如下接口引用：ImageRegistryConnDetect

名称	必选	允许NULL	类型	描述
RegistryName	是	否	String	镜像仓库名称
Region	是	否	String	区域
UserName	是	否	String	检测的用户名
Password	是	否	String	检测的密码
Url	是	否	String	检测地址
Quuid	是	否	String	检测主机的quuid 或者 backend
Uuid	是	否	String	检测主机的uuid 或者 backend
RegistryType	是	否	String	仓库类型
ApiVersion	是	否	String	api版本
BusinessType	是	否	String	retry:重试
first:首次调用联通性检测				
query:查询结果				
InstanceID	否	否	String	tcr情况下instance_id

CompliancePolicyItemSummary

表示一条检测项对应的汇总信息。

被如下接口引用：DescribeCompliancePolicyItemAffectedSummary、DescribeComplianceTaskPolicyItemSummaryList

名称	必选	允许NULL	类型	描述
CustomerPolicyItemId	是	否	Uint64	为客户分配的唯一的检测项的ID。
BasePolicyItemId	是	否	Uint64	检测项的原始ID。
Name	是	否	String	检测项的名称。
Category	是	否	String	检测项所属的类型，枚举字符串。
BenchmarkStandardName	是	否	String	所属的合规标准
RiskLevel	是	否	String	威胁等级。RISK_CRITICAL, RISK_HIGH, RISK_MEDIUM, RISK_LOW, RISK_NOTICE。

名称	必选	允许NULL	类型	描述
AssetType	是	否	String	检测项所属的资产类型
LastCheckTime	是	是	Datetime	最近检测的时间
CheckStatus	是	否	String	检测状态CHECK_INIT, 待检测CHECK_RUNNING, 检测中CHECK_FINISHED, 检测完成CHECK_FAILED, 检测失败
CheckResult	是	是	String	检测结果。RESULT_PASSED: 通过RESULT_FAILED: 未通过
PassedAssetCount	是	是	Uint64	通过检测的资产的数目
FailedAssetCount	是	是	Uint64	未通过检测的资产的数目
WhitelistId	是	是	Uint64	检测项对应的白名单项的ID。如果存在且非0，表示检测项被用户忽略。
FixSuggestion	是	否	String	处理建议。
BenchmarkStandardId	是	否	Uint64	所属的合规标准的ID
ApplicableVersion	是	是	String	检测项适用的版本
Description	否	是	String	检查项描述
AuditProcedure	否	是	String	检查项审计方法

ComplianceHostDetailInfo

表示主机资产专属的详情。

被如下接口引用：DescribeComplianceAssetDetailInfo

名称	必选	允许NULL	类型	描述
DockerVersion	是	是	String	主机上的Docker版本。
K8SVersion	是	是	String	主机上的K8S的版本。
ContainerdVersion	否	是	String	主机上Containerd版本

VirusTendencyInfo

木马趋势详情

被如下接口引用：DescribeVirusEventTendency

名称	必选	允许NULL	类型	描述
Date	是	否	Date	日期
PendingEventCount	是	否	Uint64	待处理事件总数
RiskContainerCount	是	否	Uint64	风险容器总数
EventCount	是	否	Uint64	事件总数
IsolateEventCount	是	否	Uint64	隔离事件总数

EmergencyVulInfo

应急漏洞列表信息

被如下接口引用：DescribeEmergencyVulList

名称	必选	允许NULL	类型	描述
Name	是	否	String	漏洞名称
Tags	是	是	Array of String	漏洞标签
CVSSV3Score	是	是	Float	CVSS V3分数
Level	是	是	String	风险等级
CVEID	是	否	String	CVE编号
Category	是	是	String	漏洞类型
SubmitTime	是	是	String	漏洞披露时间
LatestFoundTime	是	是	String	最近发现时间
Status	是	否	String	应急漏洞风险情况：NOT_SCAN：未扫描，SCANNING：扫描中，SCANNED_NOT_RISK：已扫描，暂未风险 ，SCANNED_RISK：已扫描存在风险
ID	是	否	Int64	漏洞ID
PocID	是	否	String	漏洞PocID
DefenceStatus	是	是	String	防御状态，NO_DEFENDED:未防御，DEFENDED:已防御
DefenceScope	是	是	String	漏洞防御主机范围: MANUAL:自选主机节点，ALL:全部
DefenceHostCount	是	是	Int64	漏洞防御主机数量
DefendedCount	是	是	Int64	已防御攻击次数

VulDetailInfo

漏洞详情信息

被如下接口引用：DescribeVulDetail

名称	必选	允许NULL	类型	描述
CVEID	是	否	String	CVE编号
Name	是	否	String	漏洞名称
Tags	是	是	Array of String	漏洞标签
CategoryType	是	是	String	漏洞类型
Level	是	是	String	漏洞威胁等级
SubmitTime	是	是	String	漏洞披露时间
Description	是	否	String	漏洞描述

名称	必选	允许NULL	类型	描述
CVSSV3Desc	是	否	String	CVSS V3描述
OfficialSolution	是	否	String	漏洞修复建议
DefenseSolution	是	否	String	缓解措施
Reference	是	否	Array of String	参考链接
CVSSV3Score	是	否	Float	CVSS V3分数
ComponentList	是	否	Array of VulAffectedComponentInfo	受漏洞影响的组件列表
LocalImageCount	是	否	Int64	影响本地镜像数
ContainerCount	是	否	Int64	影响容器数
RegistryImageCount	是	否	Int64	影响仓库镜像数
Category	是	否	String	漏洞子类型
LocalNewestImageCount	是	否	Int64	影响最新本地镜像数
RegistryNewestImageCount	是	否	Int64	影响最新仓库镜像数
PocID	是	否	String	漏洞PocID
DefenceStatus	是	是	String	防御状态，NO_DEFENDED:未防御，DEFENDED:已防御
DefenceScope	是	是	String	漏洞防御主机范围: MANUAL:自选主机节点，ALL:全部
DefenceHostCount	是	是	Int64	漏洞防御主机数量
DefendedCount	是	是	Int64	已防御攻击次数
ScanStatus	是	是	String	是否已扫描，NOT_SCAN:未扫描,SCANNED:已扫描

NetworkClusterInfoItem

网络集群资产返回的结构体

被如下接口引用：DescribeNetworkFirewallClusterList

名称	必选	允许NULL	类型	描述
ClusterId	是	否	String	集群id
ClusterName	是	否	String	集群名字
ClusterVersion	是	否	String	集群版本
ClusterOs	是	否	String	集群操作系统
ClusterType	是	否	String	集群类型
Region	是	否	String	集群区域

名称	必选	允许NULL	类型	描述
NetworkPolicyPlugin	是	否	String	集群网络插件
ClusterStatus	是	否	String	集群状态
TotalRuleCount	是	否	Int64	总策略数量
EnableRuleCount	是	否	Int64	已开启策略数量
NetworkPolicyPluginStatus	是	否	String	集群网络插件状态，正常：Running 不正常：Error
NetworkPolicyPluginError	是	是	String	集群网络插件错误信息
ClusterNetworkSettings	否	是	String	容器网络插件

ClusterRiskItem

风险项是检查完之后，有问题的检测项，并且加了一些检查结果信息。

被如下接口引用：DescribeRiskList

名称	必选	允许NULL	类型	描述
CheckItem	是	否	ClusterCheckItem	检测项相关信息
VerifyInfo	是	否	String	验证信息
ErrorMessage	是	否	String	事件描述,检查的错误信息
AffectedClusterCount	是	否	Uint64	受影响的集群数量
AffectedNodeCount	是	否	Uint64	受影响的节点数量

VulDefencePlugin

漏洞防护的插件信息

被如下接口引用：DescribeVulDefencePlugin

名称	必选	允许NULL	类型	描述
PID	是	否	Int64	java进程pid
MainClass	是	否	String	进程主类名
Status	是	否	String	插件运行状态：注入中:INJECTING，注入成功：SUCCESS，注入失败：FAIL，插件超时：TIMEOUT，插件退出：QUIT
ErrorLog	是	否	String	错误日志

ClusterRiskTarget

检查对象风险分布数据

被如下接口引用：DescribeRiskTargetCount

名称	必选	允许NULL	类型	描述
RiskTarget	是	否	String	检查对象名称
SeriousRiskCount	是	否	Uint64	严重的风险数量
HighRiskCount	是	否	Uint64	高危的风险数量
MiddleRiskCount	是	否	Uint64	中危的风险数量
HintRiskCount	是	否	Uint64	提示的风险数量

ImageAutoAuthorizedTask

镜像自动授权任务信息

被如下接口引用：DescribeImageAutoAuthorizedTaskList

名称	必选	允许NULL	类型	描述
TaskId	是	否	Int64	任务id
Type	是	否	String	授权方式，AUTO:自动授权，MANUAL:手动授权
AuthorizedDate	是	否	Date	任务日期
Source	是	否	String	镜像来源，LOCAL:本地镜像，REGISTRY:仓库镜像
LastAuthorizedTime	是	否	String	最近授权时间
SuccessCount	是	否	Int64	自动授权成功数
FailCount	是	否	Int64	自动授权失败数
LatestFailCode	是	否	String	最近任务失败码，REACH_LIMIT:达到授权上限，LICENSE_INSUFFICIENT:授权数不足

ImageComponent

容器安全镜像组件信息

被如下接口引用：DescribeImageComponentList

名称	必选	允许NULL	类型	描述
Name	是	否	String	组件名称
Version	是	否	String	组件版本
Path	是	否	String	组件路径
Type	是	否	String	组件类型
VulCount	是	是	Uint64	组件漏洞数量
ImageID	是	是	String	镜像ID

SuperNodeInfo

超级节点详情

被如下接口引用：DescribeAssetSuperNodeInfo

名称	必选	允许NULL	类型	描述
SuperNodeID	是	否	String	超级节点ID
SuperNodeName	是	否	String	超级节点名称
Status	否	否	String	节点状态:Running,Ready,Notready,Initializing,Failed,Error
SubNetName	是	否	String	子网名称
SubNetID	否	否	String	子网ID
SubNetCIDR	否	否	String	子网网段
Region	否	否	String	地域
ZoneID	否	否	String	可用区ID
ZoneName	否	否	String	可用区名称
CpuOnline	否	否	Int64	核心数
MemTotal	否	否	Int64	总内存
ClusterInfo	否	否	AssetClusterListItem	集群信息
RelatePodCount	否	否	Uint64	关联pod数量
RelateContainerCount	否	否	Uint64	关联容器数量
AgentStatus	否	否	String	agent安装状态:
UNINSTALL:未安装;				
INSTALLED:已安装;				
INSTALLING:安装中;				
NodeUniqueID	否	否	String	超级节点唯一id
CreateTime	否	否	String	创建时间
KubeletVersion	否	否	String	Kubelet版本

VulInfo

漏洞列表信息

被如下接口引用：DescribeSystemVulList、DescribeWebVulList

名称	必选	允许NULL	类型	描述
Name	是	否	String	漏洞名称
Tags	是	是	Array of String	漏洞标签
CVSSV3Score	是	是	Float	CVSS V3分数
Level	是	是	String	风险等级

名称	必选	允许NULL	类型	描述
CVEID	是	否	String	CVE编号
Category	是	是	String	漏洞子类型
FoundTime	是	是	String	首次发现时间
LatestFoundTime	是	是	String	最近发现时间
ID	是	否	Int64	漏洞ID
LocalImageCount	是	否	Int64	影响本地镜像数
ContainerCount	是	是	Int64	影响容器数
RegistryImageCount	是	是	Int64	影响仓库镜像数
PocID	是	是	String	漏洞PocID
DefenceStatus	是	是	String	防御状态，NO_DEFENDED:未防御，DEFENDED:已防御
DefenceScope	是	是	String	漏洞防御主机范围: MANUAL:自选主机节点，ALL:全部
DefenceHostCount	是	是	Int64	漏洞防御主机数量
DefendedCount	是	是	Int64	已防御攻击次数

NetworkPorts

网络集群策略自定义规则端口

被如下接口引用：AddAndPublishNetworkFirewallPolicyDetail、AddNetworkFirewallPolicyDetail、DescribeNetworkFirewallPolicyDetail、UpdateAndPublishNetworkFirewallPolicyDetail、UpdateNetworkFirewallPolicyDetail

名称	必选	允许NULL	类型	描述
Protocol	否	是	String	网络策略协议
Port	否	是	String	网络策略策略端口

ContainerMount

容器挂载信息

被如下接口引用：DescribeAssetContainerDetail

名称	必选	允许NULL	类型	描述
Type	是	否	String	挂载类型 bind
Source	是	否	String	宿主机路径
Destination	是	否	String	容器内路径
Mode	是	否	String	模式
RW	是	否	Bool	读写权限
Propagation	是	否	String	传播类型

名称	必选	允许NULL	类型	描述
Name	是	否	String	名称
Driver	是	否	String	驱动

ClusterCheckItem

表示一条集群安全检测项的详细信息

被如下接口引用：DescribeCheckItemList、DescribeRiskList

名称	必选	允许NULL	类型	描述
CheckItemId	是	是	Int64	唯一的检测项的ID
Name	是	否	String	风险项的名称
ItemDetail	是	是	String	检测项详细描述。
RiskLevel	是	是	String	威胁等级。严重Serious,高危High,中危Middle,提示Hint
RiskTarget	是	是	String	检查对象、风险对象.Runc,Kubelet,Containerd,Pods
RiskType	是	是	String	风险类别,漏洞风险CVERisk,配置风险ConfigRisk
RiskAttribute	是	是	String	检测项所属的风险类型,权限提升:PrivilegePromotion,拒绝服务:RefuseService,目录穿越:DirectoryEscape,未授权访问:UnauthorizedAccess,权限许可和访问控制问题:PrivilegeAndAccessControl,敏感信息泄露:SensitiveInfoLeak
RiskProperty	是	是	String	风险特征,Tag.存在EXP:ExistEXP,存在POD:ExistPOC,无需重启:NoNeedReboot, 服务重启:ServerRestart,远程信息泄露:RemoteInfoLeak,远程拒绝服务:RemoteRefuseService,远程利用:RemoteExploit,远程执行:RemoteExecute
CVENumber	是	是	String	CVE编号
DiscoverTime	是	是	String	披露时间
Solution	是	是	String	解决方案
CVSS	是	是	String	CVSS信息,用于画图
CVSSScore	是	是	String	CVSS分数
RelateLink	是	是	String	参考连接
AffectedType	是	是	String	影响类型，为Node或者Workload
AffectedVersion	是	是	String	受影响的版本信息
IgnoredAssetNum	是	是	Int64	忽略的资产数量
IsIgnored	是	是	Bool	是否忽略该检测项
RiskAssessment	是	是	String	受影响评估

WarningRule

告警配置策略

被如下接口引用：AddEditWarningRules、DescribeWarningRules

名称	必选	允许NULL	类型	描述
Type	是	否	String	告警事件类型：镜像仓库安全-木马：IMG_REG_VIRUS镜像仓库安全-漏洞：IMG_REG_VUL镜像仓库安全-敏感信息：IMG_REG_RISK镜像安全-木马：IMG_VIRUS镜像安全-漏洞：IMG_VUL镜像安全-敏感信息：IMG_RISK镜像安全-镜像拦截：IMG_INTERCEPT运行时安全-容器逃逸：RUNTIME_ESCAPE运行时安全-异常进程：RUNTIME_FILE运行时安全-异常文件访问：RUNTIME_PROCESS运行时安全-高危系统调用：RUNTIME_SYSCALL运行时安全-反弹Shell：RUNTIME_REVERSE_SHELL运行时安全-木马：RUNTIME_VIRUS
Switch	是	否	String	开关状态：打开：ON关闭：OFF
BeginTime	是	否	String	告警开始时间，格式: HH:mm
EndTime	是	否	String	告警结束时间，格式: HH:mm
ControlBits	是	否	String	告警等级策略控制，二进制位每位代表一个含义，值以字符串类型传递控制开关分为高、中、低，则二进制位分别为：第1位:低，第2位:中，第3位:高，0表示关闭、1表示打开。如：高危和中危打开告警，低危关闭告警，则二进制值为：110告警类型不区分等级控制，则传1。

ContainerPortInfo

容器端口信息

被如下接口引用：DescribeAssetContainerPortList

名称	必选	允许NULL	类型	描述
HostIP	是	否	String	宿主机IP
HostPort	是	否	Uint64	宿主机端口
ContainerPort	是	否	Uint64	容器端口
ProtocolType	是	否	String	协议类型

ReverseShellEventInfo

容器安全运行时高危系统调用信息

被如下接口引用：DescribeReverseShellEvents

名称	必选	允许NULL	类型	描述
ProcessName	是	否	String	进程名称
ProcessPath	是	否	String	进程路径
ImageId	是	否	String	镜像id
ContainerId	是	否	String	容器id
ImageName	是	否	String	镜像名
ContainerName	是	否	String	容器名
FoundTime	是	否	String	生成时间
Solution	是	否	String	事件解决方案

名称	必选	允许NULL	类型	描述
Description	是	否	String	事件详细描述
Status	是	否	String	状态，EVENT_UNDEAL:事件未处理 EVENT_DEALED:事件已经处理 EVENT_INGNORE：事件已经忽略 EVENT_ADD_WHITE：时间已经加白
EventId	是	否	String	事件id
Remark	是	否	String	备注
PProcessName	是	否	String	父进程名
EventCount	是	否	Int64	事件数量
LatestFoundTime	是	否	String	最近生成时间
DstAddress	是	否	String	目标地址
ContainerNetStatus	是	否	String	网络状态未隔离 NORMAL已隔离 ISOLATED隔离中 ISOLATING隔离失败 ISOLATE_FAILED解除隔离中 RESTORING解除隔离失败 RESTORE_FAILED
ContainerNetSubStatus	是	否	String	容器子状态"AGENT_OFFLINE" //Agent离线 "NODE_DESTROYED" //节点已销毁 "CONTAINER_EXITED" //容器已退出 "CONTAINER_DESTROYED" //容器已销毁 "SHARED_HOST" // 容器与主机共享网络 "RESOURCE_LIMIT" //隔离操作资源超限 "UNKNOW" // 原因未知
ContainerIsolateOperationSrc	是	否	String	容器隔离操作来源
ContainerStatus	是	否	String	容器状态正在运行: RUNNING暂停: PAUSED停止: STOPPED已经创建: CREATED已经销毁: DESTROYED正在重启中: RESTARTING迁移中: REMOVING

VulAffectedComponentInfo

受漏洞影响的组件信息

被如下接口引用：DescribeVulDetail

名称	必选	允许NULL	类型	描述
Name	是	是	String	组件名称
Version	是	是	Array of String	组件版本
FixedVersion	是	是	Array of String	组件修复版本

SuperNodeInstallTaskListItem

超级节点 agent 安装任务列表item

被如下接口引用：DescribeSuperNodeInstallTaskList

名称	必选	允许NULL	类型	描述
TaskID	否	否	String	任务id
StartTime	否	否	String	安装起始时间

名称	必选	允许NULL	类型	描述
SuperNodeCount	否	否	Uint64	安装超级节点个数
Source	否	否	String	安装来源:
TCSS:容器安全服务				
EKS:容器服务				
Status	否	否	String	状态 INSTALLING:安装中;
INSTALLATIONFAILURE:安装失败;				
INSTALLATIONSUCCESS:安装成功				
PARTIALINSTALLATIONFAILURE:部分安装失败				
SuccessCount	否	否	Uint64	成功个数
FailCount	否	否	Uint64	失败个数

SupportDefenceVul

支持防御的漏洞

被如下接口引用：DescribeSupportDefenceVul

名称	必选	允许NULL	类型	描述
PocID	是	否	String	漏洞PocID
Name	是	否	String	漏洞名称
Tags	是	否	Array of String	漏洞标签
CVSSV3Score	是	否	Float	漏洞CVSS
Level	是	否	String	漏洞威胁等级
CVEID	是	否	String	漏洞CVEID
SubmitTime	是	否	String	漏洞披露时间

EscapeWhiteListInfo

逃逸白名单

被如下接口引用：DescribeEscapeWhiteList

名称	必选	允许NULL	类型	描述
ImageID	是	否	String	镜像ID
ImageName	是	否	String	镜像名称
ID	是	否	Int64	白名单记录ID
HostCount	是	否	Int64	关联主机数量

名称	必选	允许NULL	类型	描述
ContainerCount	是	否	Int64	关联容器数量
EventType	是	否	Array of String	加白事件类型
InsertTime	是	否	String	创建时间
UpdateTime	是	否	String	更新时间
ImageSize	是	否	Int64	镜像大小

RunTimeTendencyInfo

运行时趋势信息

被如下接口引用：DescribeImageRiskTendency、DescribeSecEventsTendency、DescribeVulTendency

名称	必选	允许NULL	类型	描述
CurTime	是	否	Date	当天时间
Cnt	是	否	Uint64	当前数量

NamespaceInfo

返回的命名空间列表信息

被如下接口引用：DescribeImageRegistryNamespaceList

名称	必选	允许NULL	类型	描述
Namespace	否	否	String	命名空间名称
RegistryCnt	否	否	Int64	包含仓库数
ImageCnt	否	否	Int64	包含镜像数
RiskImageCnt	否	否	Int64	包含风险镜像数

AssetFilters

容器安全 描述键值对过滤器，用于条件过滤查询。例如过滤ID、名称、状态等 若存在多个Filter时，Filter间的关系为逻辑与（AND）关系。 若同一个Filter存在多个Values，同一Filter下Values间的关系为逻辑或（OR）关系。

被如下接口引用：AddEditImageAutoAuthorizedRule、CreateAssetContainerExportJob、CreateAssetImageRegistryScanTask、CreateAssetImageRiskExportJob、CreateAssetImageScanTask、CreateAssetImageVirusExportJob、CreateComponentExportJob、CreateHostExportJob、CreateProcessEventsExportJob、CreateSuperNodeExportJob、CreateSuperNodeInstallTaskExportJob、CreateSuperNodePodExportJob、CreateVulExportJob、CreateVulRegistryImageExportJob、DescribeAssetAppServiceList、DescribeAssetComponentList、DescribeAssetContainerList、DescribeAssetDBServiceList、DescribeAssetHostList、DescribeAssetImageHostList、DescribeAssetImageList、DescribeAssetImageListExport、DescribeAssetImageRegistryImageLayerDetail、DescribeAssetImageRegistryList、DescribeAssetImageRegistryListExport、DescribeAssetImageRegistryRegistryList、DescribeAssetImageRegistryRiskInfoList、DescribeAssetImageRegistryRiskListExport、DescribeAssetImageRegistrySummary、DescribeAssetImageRegistryVirusList、DescribeAssetImageRegistryVirusListExport、DescribeAssetImageRegistryVulList、DescribeAssetImageRegistryVulListExport、DescribeAssetImageRiskList、DescribeAssetImageRiskListExport、

DescribeAssetImageSimpleList、DescribeAssetImageVirusList、DescribeAssetImageVirusListExport、DescribeAssetImageVulList、DescribeAssetImageVulListExport、DescribeAssetPortList、DescribeAssetProcessList、DescribeAssetWebServiceList、DescribeImageAutoAuthorizedLogList、DescribeImageAutoAuthorizedTaskList、DescribeImageComponentList、DescribeImageRegistryAutoAuthorizedRepoList、DescribeImageRegistryNamespaceList、DescribeUpgradeAgentList、DescribeVulRegistryImageList、DescribeVulScanRegistryImageList、ModifyAssetImageRegistryScanStop、ModifyAssetImageScanStop、ModifyImageAuthorized、ModifyImageRegistryAutoAuthorizedRule

名称	必选	允许NULL	类型	描述
Name	是	否	String	过滤键的名称
Values	是	否	Array of String	一个或者多个过滤值。
ExactMatch	否	否	Bool	是否模糊查询

AutoAuthorizedRuleHostInfo

自动授权镜像规则授权范围主机列表

被如下接口引用：DescribeAutoAuthorizedRuleHost

名称	必选	允许NULL	类型	描述
HostID	是	否	String	主机id
HostIP	是	否	String	主机ip即内网ip
HostName	是	否	String	主机名称
ImageCnt	是	否	Uint64	镜像个数
ContainerCnt	是	否	Uint64	容器个数
PublicIp	是	否	String	外网ip
InstanceID	是	否	String	主机实例ID
MachineType	是	否	String	主机来源：["CVM", "ECM", "LH", "BM"] 中的之一为腾讯云服务器；["Other"]之一非腾讯云服务器；
DockerVersion	是	否	String	docker 版本
Status	是	否	String	agent运行状态

EscapeRuleEnabled

修改容器逃逸扫描策略开关信息

被如下接口引用：ModifyEscapeRule

名称	必选	允许NULL	类型	描述
Type	是	否	String	规则类型 ESCAPE_HOST_ACESS_FILE:宿主机文件访问逃逸 ESCAPE_MOUNT_NAMESPACE:MountNamespace逃逸 ESCAPE_PRIVILEDGE:程序提权逃逸 ESCAPE_PRIVILEDGE_CONTAINER_START:特权容器启动逃逸 ESCAPE_MOUNT_SENSITIVE_PTAH:敏感路径挂载 ESCAPE_SYSCALL:Syscall逃逸
IsEnable	是	否	Bool	是否打开：false否 ，true是

ImageProgress

基本镜像信息

被如下接口引用：DescribeAssetImageRegistryScanStatusOneKey

名称	必选	允许NULL	类型	描述
ImageId	否	是	String	镜像id
RegistryType	否	是	String	仓库类型
ImageRepoAddress	否	是	String	镜像仓库地址
InstanceId	否	是	String	实例id
InstanceName	否	是	String	实例名称
Namespace	否	是	String	命名空间
ImageName	否	是	String	仓库名称
ImageTag	否	是	String	镜像tag
ScanStatus	否	是	String	镜像扫描状态
CveProgress	否	是	Uint64	镜像cve扫描进度
RiskProgress	是	是	Uint64	镜像敏感扫描进度
VirusProgress	是	是	Uint64	镜像木马扫描进度

WhiteListNodeInfo

白名单的node信息

被如下接口引用：DescribeClusterNodeWhiteList

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	加入白名单的时间
NodeId	是	否	Uint64	白名单节点Id
InstanceId	是	否	String	实例id
ClusterId	是	否	String	集群ID
ClusterName	是	否	String	集群名字
Region	是	否	String	地域
InstanceRole	是	否	String	节点的角色，Master、Work等
PrivateIpAddresses	是	否	String	内网ip地址
NodeName	否	否	String	节点名称

VulScanImageInfo

漏洞扫描的镜像信息

被如下接口引用：DescribeVulScanLocalImageList

名称	必选	允许NULL	类型	描述
ImageID	是	否	String	镜像ID
ImageName	是	否	String	镜像名称
Size	是	否	Float	镜像大小
ScanStatus	是	否	String	任务状态:SCANNING:扫描中 FAILED:失败 FINISHED:完成 CANCELED:取消
ScanDuration	是	是	Float	扫描时长
HighLevelVulCount	是	否	Int64	高危漏洞数
MediumLevelVulCount	是	否	Int64	中危漏洞数
LowLevelVulCount	是	否	Int64	低危漏洞数
CriticalLevelVulCount	是	否	Int64	严重漏洞数
TaskID	是	否	Int64	本地镜像漏洞扫描任务ID
ScanStartTime	是	否	String	漏洞扫描的开始时间
ScanEndTime	是	否	String	漏洞扫描的结束时间
ErrorStatus	是	否	String	失败原因:TIMEOUT:超时 TOO_MANY:任务过多 OFFLINE:离线

ReverseShellEventDescription

运行时容器反弹shell事件描述信息

被如下接口引用：DescribeReverseShellDetail

名称	必选	允许NULL	类型	描述
Description	是	否	String	描述信息
Solution	是	否	String	解决方案
Remark	是	是	String	事件备注信息
DstAddress	是	否	String	目标地址
OperationTime	是	是	String	事件最后一次处理的时间

SecLogJoinInfo

安全日志接入详情

被如下接口引用：DescribeSecLogJoinTypeList

名称	必选	允许NULL	类型	描述
Count	是	否	Uint64	已接入普通主机数量

名称	必选	允许NULL	类型	描述
SuperNodeCount	否	否	Uint64	已接入超级节点数量
IsJoined	是	否	Bool	是否已接入(true:已接入 false:未接入)
LogType	是	否	String	日志类型(容器bash: "container_bash"容器启动: "container_launch"k8sApi: "k8s_api")

ImagesBindRuleInfo

查询镜像绑定的运行时规则信息

被如下接口引用：DescribeAssetImageBindRuleInfo

名称	必选	允许NULL	类型	描述
ImageId	是	否	String	镜像id
ImageName	是	否	String	镜像名称
ContainerCnt	是	否	Int64	关联容器数量
RuleId	是	是	String	绑定规则id
RuleName	是	是	String	规则名字
ImageSize	是	是	Int64	镜像大小
ScanTime	是	是	String	最近扫描时间

AffectedWorkloadItem

集群安全检查受影响的工作负载Item

被如下接口引用：AddClusterWorkloadToWhiteList、DescribeAffectedWorkloadList

名称	必选	允许NULL	类型	描述
ClusterId	是	否	String	集群Id
ClusterName	是	否	String	集群名字
WorkloadName	是	否	String	工作负载名称
WorkloadType	是	否	String	工作负载类型
Region	是	否	String	区域
VerifyInfo	是	否	String	检测结果的验证信息

ProcessDetailBaseInfo

运行是安全详情，进程基础信息

被如下接口引用：DescribeAbnormalProcessDetail、DescribeReverseShellDetail、DescribeRiskSyscallDetail

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
ProcessName	是	否	String	进程名称
ProcessId	是	否	Uint64	进程pid
ProcessStartUser	是	否	String	进程启动用户
ProcessUserGroup	是	否	String	进程用户组
ProcessPath	是	否	String	进程路径
ProcessParam	是	否	String	进程命令行参数

AbnormalProcessRuleInfo

运行时安全，异常进程检测策略

被如下接口引用：AddEditAbnormalProcessRule、DescribeAbnormalProcessRuleDetail

名称	必选	允许NULL	类型	描述
RuleId	否	是	String	策略id
IsEnable	是	否	Bool	true:策略启用，false:策略禁用
ImageIds	是	否	Array of String	生效镜像id，空数组代表全部镜像
ChildRules	是	否	Array of AbnormalProcessChildRuleInfo	用户策略的子策略数组
RuleName	是	否	String	策略名字
SystemChildRules	否	否	Array of AbnormalProcessSystemChildRuleInfo	系统策略的子策略数组
IsDefault	否	否	Bool	是否是系统默认策略

CompliancePolicyAssetSetItem

检查项+资产ids 的集合单元

被如下接口引用：DeleteCompliancePolicyAssetSetFromWhitelist

名称	必选	允许NULL	类型	描述
CustomerPolicyItemId	是	否	Uint64	检查项ID
CustomerAssetItemIdSet	否	否	Array of Uint64	需要忽略指定检查项内的资产ID列表，为空表示所有

VirusTaskInfo

运行时文件查杀任务容器列表信息

被如下接口引用：DescribeVirusTaskList

名称	必选	允许NULL	类型	描述
ContainerName	是	否	String	容器名称

名称	必选	允许NULL	类型	描述
ContainerId	是	否	String	容器id
ImageName	是	否	String	镜像名称
ImageId	是	否	String	镜像Id
HostName	是	否	String	节点名
HostIp	是	否	String	节点内网ip
Status	是	否	String	扫描状态：WAIT: 等待扫描FAILED: 失败SCANNING: 扫描中FINISHED: 结束CANCELING: 取消中CANCELED: 已取消CANCEL_FAILED： 取消失败
StartTime	是	否	String	检测开始时间
EndTime	是	否	String	检测结束时间
RiskCnt	是	否	Uint64	风险个数
Id	是	否	String	事件id
ErrorMsg	是	否	String	错误原因:SEND_SUCCESSED: 下发成功SCAN_WAIT: agent排队扫描等待中OFFLINE: 离线SEND_FAILED:下发失败TIMEOUT: 超时LOW_AGENT_VERSION: 客户端版本过低AGENT_NOT_FOUND: 镜像所属客户端版不存在TOO_MANY: 任务过多VALIDATION: 参数非法INTERNAL: 服务内部错误MISC: 其他错误UNAUTH: 所在镜像未授权SEND_CANCEL_SUCCESSED:下发成功
NodeType	否	否	String	节点类型：NORMAL普通节点、SUPER超级节点
PublicIP	否	否	String	节点外网IP
NodeID	否	否	String	节点ID

AbnormalProcessEventTendencyInfo

待处理异常进程事件趋势

被如下接口引用：DescribeAbnormalProcessEventTendency

名称	必选	允许NULL	类型	描述
Date	是	否	Date	日期
ProxyToolEventCount	是	否	Int64	待处理代理软件事件数
TransferControlEventCount	是	否	Int64	待处理横向参透事件数
AttackCmdEventCount	是	否	Int64	待处理恶意命令事件数
ReverseShellEventCount	是	否	Int64	待处理反弹shell事件数
FilelessEventCount	是	否	Int64	待处理无文件程序执行事件数
RiskCmdEventCount	是	否	Int64	待处理高危命令事件数
AbnormalChildProcessEventCount	是	否	Int64	待处理敏感服务异常子进程启动事件数
UserDefinedRuleEventCount	是	否	Int64	待处理自定义规则事件数

ComplianceFilters

键值对过滤器，用于条件过滤查询。例如过滤ID、名称、状态等 若存在多个Filter时，Filter间的关系为逻辑与（AND）关系。 若同一个Filter存在多个Values，同一Filter下Values间的关系为逻辑或（OR）关系。

被如下接口引用：DescribeAffectedNodeList、DescribeAffectedWorkloadList、DescribeCheckItemList、DescribeClusterIngressList、DescribeClusterNameList、DescribeClusterNodeWhiteList、DescribeClusterNodes、DescribeClusterServiceList、DescribeClusterWorkloadWhiteList、DescribeClusterWorkloads、DescribeClustersNamespaces、DescribeComplianceAssetList、DescribeComplianceAssetPolicyItemList、DescribeComplianceHostList、DescribeCompliancePolicyItemAffectedAssetList、DescribeCompliancePolicyItemIgnoredAssetList、DescribeComplianceScanFailedAssetList、DescribeComplianceTaskPolicyItemSummaryList、DescribeComplianceWhitelistItemList、DescribeIACCheckResultList、DescribeNamespaceList、DescribeNetworkFirewallAuditRecord、DescribeNetworkFirewallClusterList、DescribeNetworkFirewallNamespaceLabelList、DescribeNetworkFirewallNamespaceList、DescribeNetworkFirewallPodLabelsList、DescribeNetworkFirewallPolicyList、DescribeNetworkTopologyClusterChart、DescribeNetworkTopologyFlowList、DescribeNetworkTopologyFlowSwitchList、DescribeNetworkTopologyRealFlowList、DescribeNetworkTopologyWorkLoadChart、DescribeNetworkTopologyWorkLoadDetail、DescribePodContainers、DescribeRiskList、DescribeUserCluster、DescribeUserPodList

名称	必选	允许NULL	类型	描述
Name	是	否	String	过滤键的名称
Values	是	否	Array of String	一个或者多个过滤值。
ExactMatch	否	否	Bool	是否模糊查询。默认为是。

K8sApiAbnormalRuleScopeInfo

k8s api 异常事件规则配置范围

被如下接口引用：CreateK8sApiAbnormalRuleInfo、DescribeK8sApiAbnormalEventInfo、DescribeK8sApiAbnormalEventList、DescribeK8sApiAbnormalRuleInfo、DescribeK8sApiAbnormalRuleScopeList、ModifyK8sApiAbnormalRuleInfo

名称	必选	允许NULL	类型	描述
Scope	是	否	String	范围系统事件:ANONYMOUS_ACCESS: 匿名访问ABNORMAL_UA_REQ: 异常UA请求ANONYMOUS_ABNORMAL_PERMISSION: 匿名用户权限异动GET_CREDENTIALS: 凭据信息获取MOUNT_SENSITIVE_PATH: 敏感路径挂载COMMAND_RUN: 命令执行PRIVILEGE_CONTAINER: 特权容器EXCEPTION_CRONTAB_TASK: 异常定时任务STATICS_POD: 静态pod创建ABNORMAL_CREATE_POD: 异常pod创建USER_DEFINED: 用户自定义
Action	是	否	String	动作(RULE_MODE_ALERT: 告警 RULE_MODE_RELEASE:放行)
RiskLevel	否	是	String	威胁等级 HIGH:高级 MIDDLE: 中级 LOW:低级 NOTICE:提示
Status	否	是	Bool	开关状态(true:开 false:关) 适用于系统规则
IsDelete	否	是	Bool	是否被删除 适用于自定义规则入参

NetworkAuditRecord

网络集群资产审计返回结构体

被如下接口引用：DescribeNetworkFirewallAuditRecord

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
ClusterId	是	否	String	集群id
ClusterName	是	否	String	集群名字
Region	是	否	String	集群区域
Action	是	否	String	动作
Operation	是	否	String	操作人
NetworkPolicyName	是	否	String	策略名
OperationTime	是	否	String	操作时间
AppId	是	是	Int64	操作人appid
Uin	是	否	String	操作人uin
PolicyId	否	是	Uint64	策略id

ImageInfo

基本镜像信息

被如下接口引用：CreateAssetImageRegistryScanTask、CreateAssetImageRegistryScanTaskOneKey、DescribeAssetImageRegistryRiskInfoList、DescribeAssetImageRegistryRiskListExport、DescribeAssetImageRegistryScanStatusOneKey、DescribeAssetImageRegistryVirusList、DescribeAssetImageRegistryVirusListExport、DescribeAssetImageRegistryVulList、DescribeAssetImageRegistryVulListExport、DescribeImageRegistryTimingScanTask、ModifyAssetImageRegistryScanStop、ModifyAssetImageRegistryScanStopOneKey、UpdateImageRegistryTimingScanTask

名称	必选	允许NULL	类型	描述
ImageDigest	否	否	String	镜像id
RegistryType	否	否	String	仓库类型
ImageRepoAddress	否	否	String	镜像仓库地址
InstanceId	否	否	String	实例id
InstanceName	是	否	String	实例名称
Namespace	是	否	String	命名空间
ImageName	是	否	String	镜像名称
ImageTag	是	否	String	镜像tag
Force	是	否	String	强制扫描

ImageSimpleInfo

镜像列表

被如下接口引用：DescribeImageSimpleList

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
ImageID	是	否	String	镜像id
ImageName	是	否	String	镜像名称
Size	是	否	Uint64	镜像大小
ImageType	是	否	String	类型
ContainerCnt	是	否	Int64	关联容器数

ComplianceAssetPolicyItem

表示一条检测项的信息。

被如下接口引用：DescribeComplianceAssetPolicyItemList

名称	必选	允许NULL	类型	描述
CustomerPolicyItemId	是	否	Uint64	为客户分配的唯一的检测项的ID。
BasePolicyItemId	是	否	Uint64	检测项的原始ID
Name	是	否	String	检测项的名称。
Category	是	否	String	检测项所属的类型的名称
BenchmarkStandardId	是	否	Uint64	所属的合规标准的ID
BenchmarkStandardName	是	否	String	所属的合规标准的名称
RiskLevel	是	否	String	威胁等级
CheckStatus	是	否	String	检测状态CHECK_INIT, 待检测CHECK_RUNNING, 检测中CHECK_FINISHED, 检测完成CHECK_FAILED, 检测失败
CheckResult	是	是	String	检测结果RESULT_PASSED: 通过RESULT_FAILED: 未通过
WhitelistId	是	是	Uint64	检测项对应的白名单项的ID。如果存在且非0，表示检测项被用户忽略。
FixSuggestion	是	否	String	处理建议。
LastCheckTime	是	是	String	最近检测的时间。
VerifyInfo	是	是	String	验证信息

ClusterCheckTaskItem

集群检查任务入参

被如下接口引用：CreateClusterCheckTask

名称	必选	允许NULL	类型	描述
ClusterId	是	否	String	指定要扫描的集群ID
ClusterRegion	是	否	String	集群所属地域
NodeIp	否	否	String	指定要扫描的节点IP

名称	必选	允许NULL	类型	描述
WorkloadName	否	否	String	按照要扫描的workload名字

SecLogJoinObjectInfo

安全日志接入对象详情

被如下接口引用：DescribeSecLogJoinObjectList

名称	必选	允许NULL	类型	描述
HostID	是	否	String	主机ID
HostName	是	是	String	主机名称
HostIP	是	是	String	主机IP
HostStatus	是	否	String	主机状态
ClusterID	是	是	String	集群ID
ClusterName	是	是	String	集群名称
PublicIP	是	是	String	外网IP
JoinState	是	否	Bool	接入状态(true:已接入 false:未接入)
ClusterVersion	是	是	String	集群版本
ClusterMainAddress	是	否	String	集群主节点地址

EventEscapeImageInfo

风险容器信息

被如下接口引用：DescribeEventEscapeImageList

名称	必选	允许NULL	类型	描述
ImageId	否	否	String	镜像id，用于跳转
UniqueKey	否	否	String	唯一值
EventType	否	否	String	事件类型 ESCAPE_CGROUPS：利用cgroup机制逃逸 ESCAPE_TAMPER_SENSITIVE_FILE：篡改敏感文件逃逸 ESCAPE_DOCKER_API：访问Docker API接口逃逸 ESCAPE_VUL_OCCURRED：逃逸漏洞利用 MOUNT_SENSITIVE_PTAH：敏感路径挂载 PRIVILEGE_CONTAINER_START：特权容器 PRIVILEGE：程序提权逃逸
OriginEventType	否	否	String	原始事件类型
ImageName	否	否	String	镜像名
ContainerCount	否	否	Int64	容器数量
FoundTime	否	否	Datetime	生成时间
LatestFoundTime	否	否	Datetime	最近生成时间

名称	必选	允许NULL	类型	描述
EventCount	否	否	Int64	事件数量
Status	否	否	String	状态，EVENT_UNDEAL:未处理，EVENT_DEALED:已处理，EVENT_INGNORE:忽略
Description	否	否	String	风险描述
Solution	否	否	String	解决方案

EscapeRule

容器逃逸扫描策略开关信息

被如下接口引用：DescribeEscapeRuleInfo

名称	必选	允许NULL	类型	描述
Type	是	否	String	规则类型 ESCAPE_HOST_ACESS_FILE:宿主机文件访问逃逸 ESCAPE_MOUNT_NAMESPACE:MountNamespace逃逸 ESCAPE_PRIVILEDGE:程序提权逃逸 ESCAPE_PRIVILEDGE_CONTAINER_START:特权容器启动逃逸 ESCAPE_MOUNT_SENSITIVE_PTAH:敏感路径挂载ESCAPE_SYSCALL:Syscall逃逸
Name	是	否	String	规则名称宿主机文件访问逃逸、Syscall逃逸、MountNamespace逃逸、程序提权逃逸、特权容器启动逃逸、敏感路径挂载
IsEnable	是	否	Bool	是否打开：false否 ，true是
Group	是	否	String	规则组别。RISK_CONTAINER：风险容器，PROCESS_PRIVILEGE：程序特权，CONTAINER_ESCAPE：容器逃逸

AssetClusterListItem

集群列表Item

被如下接口引用：DescribeAssetClusterList、DescribeAssetSuperNodeInfo

名称	必选	允许NULL	类型	描述
ClusterID	是	否	String	集群ID
ClusterName	是	否	String	集群名称
Status	是	否	String	集群状态CSR_RUNNING: 运行中CSR_EXCEPTION:异常CSR_DEL:已经删除
BindRuleName	是	否	String	绑定规则名称
ClusterType	是	否	String	集群类型:
CT_TKE:TKE集群;				
CT_USER_CREATE:用户自建集群;				
CT_TKE_SERVERLESS:TKE Serverless集群;				
ClusterVersion	否	否	String	集群版本

名称	必选	允许NULL	类型	描述
MemLimit	否	否	Int64	内存量
CpuLimit	否	否	Int64	cpu

ImageRegistryTypeCount

仓库类型镜像数量

被如下接口引用：DescribeAssetImageRegistrySummary

名称	必选	允许NULL	类型	描述
RegistryType	否	否	String	仓库类型
ImageCount	否	否	Int64	镜像数量

ComplianceWhitelistItem

表示一条白名单记录。

被如下接口引用：DescribeComplianceWhitelistItemList

名称	必选	允许NULL	类型	描述
WhitelistItemId	是	否	Uint64	白名单项的ID。
CustomerPolicyItemId	是	否	Uint64	客户检测项的ID。
Name	是	否	String	检测项的名称。
StandardName	是	否	String	合规标准的名称。
StandardId	是	否	Uint64	合规标准的ID。
AffectedAssetCount	是	否	Uint64	检测项影响的资产的数目。
LastUpdateTime	是	否	Datetime	最后更新的时间
InsertTime	是	否	Datetime	加入到白名单的时间

ProcessBaseInfo

运行时安全，进程基础信息

被如下接口引用：DescribeAbnormalProcessDetail、DescribeAccessControlDetail、DescribeEscapeEventDetail、DescribeReverseShellDetail、DescribeRiskSyscallDetail

名称	必选	允许NULL	类型	描述
ProcessStartUser	是	是	String	进程启动用户
ProcessUserGroup	是	是	String	进程用户组
ProcessPath	是	是	String	进程路径

名称	必选	允许NULL	类型	描述
ProcessParam	是	是	String	进程命令行参数

ContainerNetwork

容器网络信息

被如下接口引用：DescribeAssetContainerDetail

名称	必选	允许NULL	类型	描述
EndpointID	是	否	String	endpoint id
Mode	是	否	String	模式:bridge
Name	是	否	String	网络名称
NetworkID	是	否	String	网络ID
Gateway	是	否	String	网关
Ipv4	是	否	String	IPV4地址
Ipv6	是	否	String	IPV6地址
MAC	是	否	String	MAC 地址

HybridClusterItem

混合云集群信息结构体

被如下接口引用：DescribeHybridClusters

名称	必选	允许NULL	类型	描述
ClusterId	否	是	String	集群的ID
MasterIpList	否	是	String	集群主Ip列表,以;隔开
ClusterName	否	是	String	集群名称

K8sApiAbnormalEventListItem

k8sapi异常事件列表Item

被如下接口引用：DescribeK8sApiAbnormalEventList

名称	必选	允许NULL	类型	描述
ID	是	否	Uint64	事件ID
MatchRuleType	是	否	String	命中规则类型
RiskLevel	是	否	String	威胁等级
ClusterID	是	否	String	集群ID

名称	必选	允许NULL	类型	描述
ClusterName	是	否	String	集群名称
ClusterRunningStatus	是	否	String	集群运行状态
FirstCreateTime	是	否	String	初次生成时间
LastCreateTime	是	否	String	最近一次生成时间
AlarmCount	是	否	Uint64	告警数量
Status	是	否	String	状态
RuleType	是	否	String	规则类型
Desc	是	否	String	描述信息
Suggestion	是	否	String	解决方案
RuleName	是	否	String	规则名称
MatchRule	是	否	K8sApiAbnormalRuleScopeInfo	命中规则

VirusDetailInfo

运行时木马详情

被如下接口引用：

名称	必选	允许NULL	类型	描述
ImageId	是	是	String	镜像ID
ImageName	是	是	String	镜像名称
CreateTime	是	是	String	创建时间
Size	是	是	Array of Uint64	木马文件大小
FilePath	是	是	String	木马文件路径
ModifyTime	是	是	String	最近生成时间
VirusName	是	是	String	病毒名称
RiskLevel	是	是	String	风险等级 RISK_CRITICAL, RISK_HIGH, RISK_MEDIUM, RISK_LOW, RISK_NOTICE。
ContainerName	是	是	String	容器名称
ContainerId	是	是	String	容器id
HostName	是	是	String	主机名称
HostId	是	是	String	主机id
ProcessName	是	是	String	进程名称
ProcessPath	是	是	String	进程路径
ProcessMd5	是	是	String	进程md5

名称	必选	允许NULL	类型	描述
ProcessId	是	是	Array of Uint64	进程id
ProcessArgv	是	是	String	进程参数
ProcessChan	是	是	String	进程链
ProcessAccountGroup	是	是	String	进程组
ProcessStartAccount	是	是	String	进程启动用户
ProcessFileAuthority	是	是	String	进程文件权限
SourceType	是	是	Int64	来源：0：一键扫描， 1：定时扫描 2：实时监控
PodName	是	是	String	集群名称
Tags	是	是	Array of String	标签
HarmDescribe	是	是	String	事件描述
SuggestScheme	是	是	String	建议方案
Mark	是	是	String	备注
FileName	是	是	String	风险文件名称
FileMd5	是	是	String	文件MD5
EventType	是	是	String	事件类型

AbnormalProcessChildRuleInfo

容器运行时安全，子策略信息

被如下接口引用：AddEditAbnormalProcessRule、DescribeAbnormalProcessDetail、DescribeAbnormalProcessRuleDetail

名称	必选	允许NULL	类型	描述
RuleId	否	是	String	子策略id
RuleMode	是	否	String	策略模式， RULE_MODE_RELEASE: 放行 RULE_MODE_ALERT: 告警 RULE_MODE_HOLDUP: 拦截
ProcessPath	是	否	String	进程路径
RuleLevel	否	是	String	威胁等级，HIGH:高，MIDDLE:中，LOW:低

ImageRisk

容器安全镜像高危行为信息

被如下接口引用：DescribeAssetImageRegistryImageLayerDetail、DescribeAssetImageRegistryRiskInfoList

名称	必选	允许NULL	类型	描述
Behavior	是	是	Uint64	高危行为

名称	必选	允许NULL	类型	描述
Type	是	是	Uint64	种类
Level	是	是	String	风险等级
Desc	是	是	String	描述
InstructionContent	是	是	String	解决方案

AccessControlRuleInfo

容器运行时，访问控制策略信息

被如下接口引用：AddEditAccessControlRule、DescribeAccessControlRuleDetail

名称	必选	允许NULL	类型	描述
RuleId	否	是	String	策略id
IsEnable	是	否	Bool	开关,true:开启，false:禁用
ImageIds	是	否	Array of String	生效镜像id，空数组代表全部镜像
ChildRules	是	否	Array of AccessControlChildRuleInfo	用户策略的子策略数组
RuleName	是	否	String	策略名字
SystemChildRules	否	否	Array of AccessControlSystemChildRuleInfo	系统策略的子策略数组
IsDefault	否	否	Bool	是否是系统默认策略

ProcessInfo

容器安全进程列表

被如下接口引用：DescribeAssetProcessList

名称	必选	允许NULL	类型	描述
StartTime	是	否	String	进程启动时间
RunAs	是	否	String	运行用户
CmdLine	是	否	String	命令行参数
Exe	是	否	String	Exe路径
PID	是	否	Uint64	主机PID
ContainerPID	是	否	Uint64	容器内pid
ContainerName	是	否	String	容器名称
HostID	是	否	String	主机id
HostIP	是	否	String	主机ip
ProcessName	是	否	String	进程名称

名称	必选	允许NULL	类型	描述
HostName	是	否	String	主机名称
PublicIp	是	否	String	外网ip
NodeID	否	否	String	节点id
PodIP	否	否	String	podip
PodName	否	否	String	pod名称
NodeType	否	否	String	节点类型
NodeUniqueID	否	否	String	超级节点唯一id

ImageVirus

容器安全镜像病毒信息

被如下接口引用：DescribeAssetImageRegistryImageLayerDetail、DescribeAssetImageRegistryVirusList

名称	必选	允许NULL	类型	描述
Path	是	是	String	路径
RiskLevel	是	是	String	风险等级
Category	是	是	String	分类
VirusName	是	是	String	病毒名称
Tags	是	是	Array of String	标签
Desc	是	是	String	描述
Solution	是	是	String	解决方案
FileType	是	是	String	文件类型
FileName	是	是	String	文件路径
FileMd5	是	是	String	文件md5
FileSize	是	是	Uint64	大小
FirstScanTime	是	是	String	首次发现时间
LatestScanTime	是	是	String	最近扫描时间

EventType

运行时安全事件类型

被如下接口引用：

名称	必选	允许NULL	类型	描述
Type	是	否	String	事件类型, 字符串枚举，例如：ESCAPE_SYSCALL

名称	必选	允许NULL	类型	描述
EventName	是	否	String	事件名称，例如：敏感路径挂载

SecTendencyEventInfo

运行时安全事件趋势信息

被如下接口引用：DescribeSecEventsTendency

名称	必选	允许NULL	类型	描述
EventSet	是	否	Array of RunTimeTendencyInfo	趋势列表
EventType	是	否	String	事件类型：ET_ESCAPE : 容器逃逸ET_REVERSE_SHELL: 反弹shellET_RISK_SYSCALL:高危系统调用ET_ABNORMAL_PROCESS: 异常进程ET_ACCESS_CONTROL 文件篡改ET_VIRUS 木马事件ET_MALICIOUS_CONNECTION 恶意外连事件

ComplianceImageDetailInfo

表示镜像资产专属的详情。

被如下接口引用：DescribeComplianceAssetDetailInfo

名称	必选	允许NULL	类型	描述
ImageId	是	否	String	镜像在主机上的ID。
ImageName	是	否	String	镜像的名称。
ImageTag	是	否	String	镜像的Tag。
Repository	是	是	String	镜像所在远程仓库的路径。

IngressForwardConfig

Ingress转发配置

被如下接口引用：DescribeIngressForwardConfig

名称	必选	允许NULL	类型	描述
Protocol	是	否	String	协议.
ListeningPort	是	否	Uint64	监听端口
Host	是	否	String	域名
Path	是	否	String	URL路径
BackendServiceName	是	否	String	后端服务
ServicePort	是	否	Uint64	服务端口
RewriteAddress	是	否	String	重定向目标地址

名称	必选	允许NULL	类型	描述
Type	是	否	Uint64	1 ForwardConfig:转发配置,2 RewriteForwardConfig:重定向转发配置

SecLogDeliveryClsSettingInfo

安全日志-日志投递cls设置信息

被如下接口引用：DescribeSecLogDeliveryClsSetting、ModifySecLogDeliveryClsSetting

名称	必选	允许NULL	类型	描述
LogType	是	否	String	日志类型
State	是	否	Bool	投递状态(true:开启 false:关闭)
Region	是	否	String	区域
LogSet	是	否	String	日志集
TopicID	是	否	String	主题ID
LogSetName	否	是	String	日志集名称
TopicName	否	是	String	主题名称

VirusAutoIsolateSampleInfo

木马自动隔离样本信息

被如下接口引用：DescribeVirusAutoIsolateSampleList

名称	必选	允许NULL	类型	描述
MD5	是	否	String	文件MD5值
VirusName	是	否	String	病毒名
ModifyTime	是	否	Datetime_iso	最近编辑时间
AutoIsolateSwitch	是	否	Bool	自动隔离开关(true:开 false:关)

PortInfo

容器安全端口信息列表

被如下接口引用：DescribeAssetPortList

名称	必选	允许NULL	类型	描述
Type	是	否	String	类型
PublicIP	是	否	String	对外ip
PublicPort	是	否	Uint64	主机端口
ContainerPort	是	否	Uint64	容器端口

名称	必选	允许NULL	类型	描述
ContainerPID	是	否	Uint64	容器Pid
ContainerName	是	否	String	容器名
HostID	是	否	String	主机id
HostIP	是	否	String	主机ip
ProcessName	是	否	String	进程名称
ListenContainer	是	否	String	容器内监听地址
ListenHost	是	否	String	容器外监听地址
RunAs	是	否	String	运行账号
HostName	是	否	String	主机名称
PublicIp	是	否	String	外网ip
NodeID	否	否	String	节点id
PodIP	否	否	String	podip
PodName	否	否	String	pod名称
NodeType	否	否	String	节点类型
NodeUniqueID	否	否	String	超级节点唯一id

AffectedNodeItem

受影响的节点类型结构体

被如下接口引用：AddClusterNodeToWhiteList、DescribeAffectedNodeList

名称	必选	允许NULL	类型	描述
ClusterId	是	否	String	集群ID
ClusterName	是	否	String	集群名字
InstanceId	是	否	String	实例id
PrivateIpAddresses	是	否	String	内网ip地址
InstanceRole	是	否	String	节点的角色，Master、Work等
ClusterVersion	是	否	String	k8s版本
ContainerRuntime	是	否	String	运行时组件,docker或者containerd
Region	是	否	String	区域
VerifyInfo	是	否	String	检查结果的验证信息
NodeName	是	否	String	节点名称

ImageRiskInfo

镜像风险详情

被如下接口引用：DescribeAssetImageRiskList

名称	必选	允许NULL	类型	描述
Behavior	是	否	Uint64	行为
Type	是	否	Uint64	类型
Level	是	否	Uint64	级别
Desc	是	否	String	详情
InstructionContent	是	否	String	解决方案

ABTestConfig

灰度项目配置

被如下接口引用：DescribeABTestConfig

名称	必选	允许NULL	类型	描述
ProjectName	是	否	String	灰度项目名称
Status	是	否	Bool	true：正在灰度，false：不在灰度

ImageLayer

镜像层信息

被如下接口引用：DescribeAssetImageRegistryImageLayerDetail

名称	必选	允许NULL	类型	描述
LayerNum	否	是	Int64	序号
LayerId	否	是	String	层id
LayerCmd	否	是	String	层指令
Size	否	是	Int64	层大小
CriticalLevelVulCnt	否	是	Int64	漏洞严重个数
HighLevelVulCnt	否	是	Int64	漏洞高危个数
MediumLevelVulCnt	否	是	Int64	漏洞中危个数
LowLevelVulCnt	否	是	Int64	漏洞低危个数
VirusCnt	否	是	Int64	木马个数
RiskCnt	否	是	Int64	敏感信息个数
VulList	否	是	Array of ImageNewVul	漏洞列表
VirusList	否	是	Array of ImageVirus	木马列表

名称	必选	允许NULL	类型	描述
SensitiveList	否	是	Array of ImageRisk	敏感信息列表

ComplianceBenchmarkStandardEnable

表示是否启用合规标准。

被如下接口引用：ModifyCompliancePeriodTask

名称	必选	允许NULL	类型	描述
StandardId	是	否	Uint64	合规标准的ID。
Enable	是	否	Bool	是否启用合规标准

ComplianceAssetPolicySetItem

资产+检查项ids 集合单元

被如下接口引用：AddComplianceAssetPolicySetToWhitelist

名称	必选	允许NULL	类型	描述
CustomerAssetItemId	是	否	Uint64	资产ID
CustomerPolicyItemIdSet	否	否	Array of Uint64	需要忽略指定资产内的检查项ID列表，为空表示所有

K8sApiAbnormalRuleListItem

k8s api 异常请求规则列表Item

被如下接口引用：DescribeK8sApiAbnormalRuleList

名称	必选	允许NULL	类型	描述
RuleID	是	否	String	规则ID
RuleName	是	否	String	规则名称
RuleType	是	否	String	规则类型RT_SYSTEM 系统规则RT_USER 用户自定义
EffectClusterCount	是	否	Uint64	受影响集群总数
UpdateTime	是	否	String	更新时间
OprUin	是	否	String	编辑账号
Status	是	否	Bool	状态

ClusterRegionItem

集群支持的地域结构体

被如下接口引用：DescribeSupportRegions

名称	必选	允许NULL	类型	描述
Region	否	是	String	地域
RegionCode	否	是	String	地域缩写
RegionId	否	是	Uint64	地域Id
RegionName	否	是	String	地域中文名
RegionNameEn	否	是	String	地域英文名

SecLogDeliveryKafkaSettingInfo

安全日志日志投递kafka设置详情

被如下接口引用：DescribeSecLogDeliveryKafkaSetting、ModifySecLogDeliveryKafkaSetting

名称	必选	允许NULL	类型	描述
LogType	是	否	String	日志类型
TopicID	是	否	String	主题ID
TopicName	是	是	String	主题名称
State	是	否	Bool	投递状态(false:关 true:开)

AccessControlEventInfo

容器运行时安全访问控制事件信息

被如下接口引用：DescribeAccessControlEvents

名称	必选	允许NULL	类型	描述
ProcessName	是	否	String	进程名称
MatchRuleName	是	否	String	命中规则名称
FoundTime	是	否	Datetime	生成时间
ContainerName	是	否	String	容器名
ImageName	是	否	String	镜像名
Behavior	是	否	String	动作执行结果， BEHAVIOR_NONE: 无 BEHAVIOR_ALERT: 告警 BEHAVIOR_RELEASE：放行 BEHAVIOR_HOLDUP_FAILED:拦截失败 BEHAVIOR_HOLDUP_SUCCESSED：拦截失败
Status	是	否	String	状态0:未处理 “EVENT_UNDEAL”:事件未处理 "EVENT_DEALED":事件已经处理 "EVENT_INGNORE"：事件已经忽略
Id	是	否	String	事件记录的唯一id
FileName	是	否	String	文件名称
EventType	是	否	String	事件类型， FILE_ABNORMAL_READ:文件异常读取
ImageId	是	否	String	镜像id, 用于跳转

名称	必选	允许NULL	类型	描述
ContainerId	是	否	String	容器id, 用于跳转
Solution	是	否	String	事件解决方案
Description	是	否	String	事件详细描述
MatchRuleId	是	否	String	命中策略id
MatchAction	是	否	String	命中规则行为：RULE_MODE_RELEASE 放行RULE_MODE_ALERT 告警 RULE_MODE_HOLDUP 拦截
MatchProcessPath	是	否	String	命中规则进程信息
MatchFilePath	是	否	String	命中规则文件信息
FilePath	是	否	String	文件路径，包含名字
RuleExist	是	否	Bool	规则是否存在
EventCount	是	否	Int64	事件数量
LatestFoundTime	是	否	String	最近生成时间
RuleId	是	否	String	规则组id
ContainerNetStatus	是	否	String	网络状态未隔离 NORMAL已隔离 ISOLATED隔离中 ISOLATING隔离失败 ISOLATE_FAILED解除隔离中 RESTORING解除隔离失败 RESTORE_FAILED
ContainerNetSubStatus	是	否	String	容器子状态"AGENT_OFFLINE" //Agent离线"NODE_DESTROYED" //节点已销毁"CONTAINER_EXITED" //容器已退出"CONTAINER_DESTROYED" //容器已销毁"SHARED_HOST" // 容器与主机共享网络"RESOURCE_LIMIT" //隔离操作资源超限"UNKNOW" // 原因未知
ContainerIsolateOperationSrc	是	否	String	容器隔离操作来源
ContainerStatus	是	否	String	容器状态正在运行: RUNNING暂停: PAUSED停止: STOPPED已经创建: CREATED已经销毁: DESTROYED正在重启中: RESTARTING迁移中: REMOVING
NodeName	否	否	String	节点名称：如果是超级节点，展示的实质上是它的node_id
PodName	否	否	String	pod名称
PodIP	否	否	String	pod ip
NodeType	否	否	String	节点类型：NORMAL普通节点、SUPER超级节点
ClusterID	否	否	String	集群id
NodeUniqueID	否	否	String	节点的唯一id，主要是超级节点使用
PublicIP	否	否	String	节点公网IP
NodeID	否	否	String	节点id
HostID	否	否	String	uuid
HostIP	否	否	String	节点内网ip
ClusterName	否	否	String	集群名称

NetworkTopologyFlow

网络流量列表

被如下接口引用：DescribeNetworkTopologyFlowList、DescribeNetworkTopologyRealFlowList

名称	必选	允许NULL	类型	描述
Id	否	是	String	流量id
FlowTime	否	是	String	流量时间
SrcIp	否	是	String	源ip
SrcPod	否	是	String	源pod
SrcWorkLoad	否	是	String	源负载
SrcPolicy	否	是	Uint64	源关联策略
SrcLabel	否	是	String	源标签
SrcWorkLoadKind	否	是	String	源负载类型
SrcNamespace	否	是	String	源命名空间
DestIp	否	是	String	目标ip
DestPod	否	是	String	目标pod
DestWorkLoad	否	是	String	目标负载
DestWorkLoadKind	否	是	String	目标负载类型
DestNamespace	否	是	String	目标命名空间
DestPolicy	否	是	Uint64	目标关联策略
DestLabel	否	是	String	目标标签
Protocol	否	是	String	协议
Port	否	是	String	端口
Action	否	是	String	动作

SecLogAlertMsgInfo

安全日志告警信息

被如下接口引用：DescribeSecLogAlertMsg

名称	必选	允许NULL	类型	描述
MsgType	是	否	String	告警类型
MsgValue	是	否	String	告警值
State	是	否	Bool	状态(0:关闭 1:开启)

ComplianceScanFailedAsset

表示检测失败的资产的信息。

被如下接口引用：DescribeComplianceScanFailedAssetList

名称	必选	允许NULL	类型	描述
CustomerAssetId	是	否	Uint64	客户资产的ID。
AssetType	是	否	String	资产类别。
CheckStatus	是	否	String	检测状态CHECK_INIT, 待检测CHECK_RUNNING, 检测中CHECK_FINISHED, 检测完成CHECK_FAILED, 检测失败
AssetName	是	否	String	资产的名称。
FailureReason	是	否	String	资产检测失败的原因。
Suggestion	是	否	String	检测失败的处理建议。
CheckTime	是	否	Datetime	检测的时间。

ClsTopicInfo

cls主题信息

被如下接口引用：DescribeSecLogDeliveryClsOptions

名称	必选	允许NULL	类型	描述
TopicID	是	否	String	主题ID
TopicName	是	否	String	主题名称

ImageRiskTendencyInfo

运行时安全事件趋势信息

被如下接口引用：DescribeImageRiskTendency

名称	必选	允许NULL	类型	描述
ImageRiskSet	是	否	Array of RunTimeTendencyInfo	趋势列表

名称	必选	允许NULL	类型	描述
ImageRiskType	是	否	String	风险类型：IRT_VULNERABILITY：安全漏洞IRT_MALWARE_VIRUS: 木马病毒IRT_RISK:敏感信息

ProjectInfo

主机所属项目

被如下接口引用：DescribeAssetHostDetail、DescribeAssetHostList

名称	必选	允许NULL	类型	描述
ProjectName	是	否	String	项目名称
ProjectID	是	否	Int64	项目ID

SoftQuotaDayInfo

后付费详情

被如下接口引用：DescribePostPayDetail

名称	必选	允许NULL	类型	描述
PayTime	是	否	String	扣费时间
CoresCnt	是	否	Uint64	计费核数(已废弃)

AbnormalProcessEventInfo

容器运行时安全异常进程信息

被如下接口引用：DescribeAbnormalProcessEvents

名称	必选	允许NULL	类型	描述
ProcessPath	是	否	String	进程目录
EventType	是	否	String	事件类型，MALICE_PROCESS_START:恶意进程启动
MatchRuleName	是	否	String	命中规则名称，PROXY_TOOL：代理软件，TRANSFER_CONTROL：横向渗透，ATTACK_CMD：恶意命令，REVERSE_SHELL：反弹shell，FILELESS：无文件程序执行，RISK_CMD：高危命令，ABNORMAL_CHILD_PROC：敏感服务异常子进程启动，USER_DEFINED_RULE：用户自定义规则
FoundTime	是	否	Datetime	生成时间
ContainerName	是	否	String	容器名
ImageName	是	否	String	镜像名
Behavior	是	否	String	动作执行结果， BEHAVIOR_NONE: 无 BEHAVIOR_ALERT: 告警 BEHAVIOR_RELEASE：放行 BEHAVIOR_HOLDUP_FAILED:拦截失败 BEHAVIOR_HOLDUP_SUCCESSED：拦截失败

名称	必选	允许NULL	类型	描述
Status	是	否	String	状态，EVENT_UNDEAL:事件未处理 EVENT_DEALED:事件已经处理 EVENT_INGNORE：事件已经忽略
Id	是	否	String	事件记录的唯一id
ImageId	是	否	String	镜像id，用于跳转
ContainerId	是	否	String	容器id，用于跳转
Solution	是	否	String	事件解决方案
Description	是	否	String	事件详细描述
MatchRuleId	是	否	String	命中策略id
MatchAction	是	否	String	命中规则行为：RULE_MODE_RELEASE 放行RULE_MODE_ALERT 告警 RULE_MODE_HOLDUP 拦截
MatchProcessPath	是	否	String	命中规则进程信息
RuleExist	是	否	Bool	规则是否存在
EventCount	是	否	Int64	事件数量
LatestFoundTime	是	否	Datetime	最近生成时间
RuleId	是	否	String	规则组Id
MatchGroupName	是	否	String	命中策略名称：SYSTEM_DEFINED_RULE （系统策略）或 用户自定义的策略名字
MatchRuleLevel	是	否	String	命中规则等级，HIGH：高危，MIDDLE：中危，LOW：低危。
ContainerNetStatus	是	是	String	网络状态未隔离 NORMAL已隔离 ISOLATED隔离中 ISOLATING隔离失败 ISOLATE_FAILED解除隔离中 RESTORING解除隔离失败 RESTORE_FAILED
ContainerNetSubStatus	是	是	String	容器子状态"AGENT_OFFLINE" //Agent离线"NODE_DESTROYED" //节点已销毁"CONTAINER_EXITED" //容器已退出"CONTAINER_DESTROYED" //容器已销毁"SHARED_HOST" // 容器与主机共享网络"RESOURCE_LIMIT" //隔离操作资源超限"UNKNOW" // 原因未知
ContainerIsolateOperationSrc	是	是	String	容器隔离操作来源
ContainerStatus	是	否	String	容器状态正在运行: RUNNING暂停: PAUSED停止: STOPPED已经创建: CREATED已经销毁: DESTROYED正在重启中: RESTARTING迁移中: REMOVING
ClusterID	否	否	String	集群ID
NodeType	否	否	String	节点类型：NORMAL普通节点、SUPER超级节点
PodName	否	否	String	pod 名称
PodIP	否	否	String	pod ip
NodeUniqueID	否	否	String	集群id
PublicIP	否	否	String	节点公网ip
NodeName	否	否	String	节点名称

名称	必选	允许NULL	类型	描述
NodeID	否	否	String	节点id
HostID	否	否	String	uuid
HostIP	否	否	String	节点内网ip
ClusterName	否	否	String	集群名称

CompliancePeriodTaskRule

表示一个定时任务的周期设置

被如下接口引用：DescribeCompliancePeriodTaskList、DescribeComplianceTaskAssetSummary、ModifyCompliancePeriodTask

名称	必选	允许NULL	类型	描述
Frequency	是	否	Uint64	执行的频率（几天一次），取值为：1,3,7。
ExecutionTime	是	否	String	在这天的什么时间执行，格式为：HH:mm:SS。
Enable	否	是	Bool	是否开启

ConnDetectConfig

联通性检测配置

被如下接口引用：AddAssetImageRegistryRegistryDetail、UpdateAssetImageRegistryRegistryDetail

名称	必选	允许NULL	类型	描述
Quuid	否	否	String	主机quuid
Uuid	否	否	String	主机uuid

ComplianceHostInfo

合规安全自选范围中的主机列表单条记录信息

被如下接口引用：DescribeComplianceHostList

名称	必选	允许NULL	类型	描述
HostId	是	否	Uint64	主机唯一id
HostIP	是	否	String	主机ip
HostName	是	否	String	主机名称
HostStatus	是	否	String	主机状态 ASSET_OFFLINE 回收 ASSET_ABNORMAL 离线 ASSET_NORMAL 正常
ImageCnt	是	否	Uint64	镜像数量
ContainerCnt	是	否	Uint64	容器数量
Checked	是	是	Bool	是否为已选项

名称	必选	允许NULL	类型	描述
InstanceId	是	是	String	主机实例id

VulDefenceEvent

漏洞防御事件详情

被如下接口引用：DescribeVulDefenceEvent

名称	必选	允许NULL	类型	描述
CVEID	是	否	String	漏洞CVEID
VulName	是	否	String	漏洞名称
PocID	是	否	String	漏洞PocID
EventType	是	否	String	入侵状态
SourceIP	是	否	String	攻击源IP
City	是	否	String	攻击源ip地址所在城市
EventCount	是	否	Int64	事件数量
ContainerID	是	否	String	容器ID
ContainerName	是	否	String	容器名称
ImageID	是	否	String	镜像ID
ImageName	是	否	String	镜像名称
Status	是	否	String	处理状态
EventID	是	否	Int64	事件ID
CreateTime	是	是	String	首次发现时间
ContainerNetStatus	是	否	String	隔离状态未隔离 NORMAL已隔离 ISOLATED隔离中 ISOLATING隔离失败 ISOLATE_FAILED解除隔离中 RESTORING解除隔离失败 RESTORE_FAILED
MergeTime	是	是	String	最近发现时间
ContainerStatus	是	是	String	容器状态正在运行: RUNNING暂停: PAUSED停止: STOPPED已经创建: CREATED已经销毁: DESTROYED正在重启中: RESTARTING迁移中: REMOVING
ContainerNetSubStatus	是	是	String	容器子状态"AGENT_OFFLINE" //Agent离线 "NODE_DESTROYED" //节点已销毁 "CONTAINER_EXITED" //容器已退出 "CONTAINER_DESTROYED" //容器已销毁 "SHARED_HOST" // 容器与主机共享网络 "RESOURCE_LIMIT" //隔离操作资源超限 "UNKNOW" // 原因未知
ContainerIsolateOperationSrc	是	是	String	容器隔离操作来源
QUUID	是	是	String	主机QUUID/超级节点ID
HostIP	是	是	String	主机内网IP
HostName	是	是	String	主机名称/超级节点名称

名称	必选	允许NULL	类型	描述
NodeType	否	否	String	节点类型[NORMAL:普通节点|SUPER:超级节点]
PublicIP	否	否	String	外网IP
NodeUniqueID	否	否	String	超级节点唯一ID
NodeID	否	否	String	超级节点ID
ClusterID	否	否	String	集群ID
ClusterName	否	否	String	集群名称

RaspInfo

漏洞防御插件 rasp信息

被如下接口引用：DescribeVulDefenceEventDetail

名称	必选	允许NULL	类型	描述
Name	是	否	String	rasp名称
Value	是	否	String	rasp 描述

ImageVirusInfo

容器安全镜像病毒信息

被如下接口引用：DescribeAssetImageVirusList

名称	必选	允许NULL	类型	描述
Path	是	是	String	路径
RiskLevel	是	是	Uint64	风险等级
VirusName	是	是	String	病毒名称
Tags	是	是	Array of String	标签
Desc	是	是	String	描述
Solution	是	是	String	修护建议
Size	是	是	Uint64	大小
FirstScanTime	是	是	String	首次发现时间
LatestScanTime	是	是	String	最近扫描时间
Md5	是	是	String	文件md5
FileName	是	是	String	文件名称
CheckPlatform	是	是	Array of String	检测平台1: 云查杀引擎2: tav3: binaryAi4: 异常行为5: 威胁情报

VulDefenceEventTendency

漏洞防御攻击事件趋势

被如下接口引用：DescribeVulDefenceEventTendency

名称	必选	允许NULL	类型	描述
Date	是	否	Date	日期
EventCount	是	否	Int64	事件数量

HostInfo

容器安全主机列表

被如下接口引用：DescribeAssetHostList

名称	必选	允许NULL	类型	描述
HostID	否	否	String	主机id
HostIP	否	否	String	主机ip即内网ip
HostName	否	否	String	主机名称
Group	否	否	String	业务组
DockerVersion	否	否	String	docker 版本
DockerFileSystemDriver	否	否	String	docker 文件系统类型
ImageCnt	否	否	Uint64	镜像个数
ContainerCnt	否	否	Uint64	容器个数
Status	否	否	String	agent运行状态
IsContainerd	否	否	Bool	是否是Containerd
MachineType	否	否	String	主机来源：["CVM", "ECM", "LH", "BM"] 中的之一为腾讯云服务器；["Other"]之一非腾讯云服务器；
PublicIp	否	否	String	外网ip
Uuid	否	否	String	主机uuid
InstanceID	否	否	String	主机实例ID
RegionID	否	否	Int64	地域ID
Project	否	是	ProjectInfo	所属项目
Tags	否	是	Array of TagInfo	标签
ClusterID	否	否	String	集群id
ClusterName	否	否	String	集群名称
ClusterAccessedStatus	否	否	String	集群接入状态

名称	必选	允许NULL	类型	描述
ChargeCoresCnt	否	否	Uint64	计费核数
DefendStatus	否	否	String	防护状态:
已防护: Defended				
未防护: UnDefended				

ComplianceBenchmarkStandard

表示一个合规标准的信息。

被如下接口引用：DescribeCompliancePeriodTaskList

名称	必选	允许NULL	类型	描述
StandardId	是	否	Uint64	合规标准的ID
Name	是	否	String	合规标准的名称
PolicyItemCount	是	否	Uint64	合规标准包含的数目
Enabled	是	否	Bool	是否启用此标准
Description	是	否	String	标准的描述

AbnormalProcessSystemChildRuleInfo

异常进程系统策略的子策略信息

被如下接口引用：AddEditAbnormalProcessRule、DescribeAbnormalProcessRuleDetail

名称	必选	允许NULL	类型	描述
RuleId	是	否	String	子策略Id
IsEnable	是	否	Bool	子策略状态，true为开启，false为关闭
RuleMode	是	否	String	策略模式, RULE_MODE_RELEASE: 放行 RULE_MODE_ALERT: 告警 RULE_MODE_HOLDUP:拦截
RuleType	是	否	String	子策略检测的行为类型PROXY_TOOL： 代理软件TRANSFER_CONTROL：横向渗透ATTACK_CMD： 恶意命令REVERSE_SHELL：反弹shellFILELESS：无文件程序执行RISK_CMD：高危命令ABNORMAL_CHILD_PROC: 敏感服务异常子进程启动
RuleLevel	否	是	String	威胁等级，HIGH:高，MIDDLE:中，LOW:低

MaliciousConnectionRuleInfo

恶意外连黑白名单信息

被如下接口引用：DescribeMaliciousConnectionBlackList、DescribeMaliciousConnectionWhiteList

名称	必选	允许NULL	类型	描述
RuleType	是	否	String	枚举：IP: 表示ipv4或者ipv6DOMAIN: 表示域名

名称	必选	允许NULL	类型	描述
Address	是	否	String	自定义黑白名单的域名/IP
CreatedTime	是	否	String	创建时间
UpdateTime	是	否	String	更新时间
Remark	是	否	String	备注
RuleID	是	否	Uint64	规则ID

VulIgnoreRegistryImage

漏洞扫描忽略的仓库镜像

被如下接口引用：DescribeVulIgnoreRegistryImageList

名称	必选	允许NULL	类型	描述
ID	是	否	Int64	记录ID
RegistryName	是	否	String	仓库名称
ImageVersion	是	否	String	镜像版本
RegistryPath	是	否	String	仓库地址
ImageID	是	否	String	镜像ID
PocID	是	否	String	漏洞PocID

ModifyIgnoreVul

漏洞扫描新增和取消忽略漏洞入参

被如下接口引用：AddIgnoreVul、DeleteIgnoreVul

名称	必选	允许NULL	类型	描述
PocID	是	否	String	漏洞PocID
ImageIDs	否	否	Array of String	忽略的镜像ID，空表示全部
ImageType	否	否	String	当有镜像时镜像类型: LOCAL 本地镜像 REGISTRY 仓库镜像

ScanIgnoreVul

扫描忽略的漏洞

被如下接口引用：DescribeScanIgnoreVulList

名称	必选	允许NULL	类型	描述
VulName	是	否	String	漏洞名称
CVEID	是	否	String	漏洞CVEID

名称	必选	允许NULL	类型	描述
PocID	是	否	String	漏洞PocID
RegistryImageCount	是	否	Int64	忽略的仓库镜像数
UpdateTime	是	否	String	更新时间
IsIgnoreAll	是	否	Int64	是否忽略所有镜像：0：否/1：是
LocalImageCount	是	否	Int64	忽略的本地镜像数

VulAffectedRegistryImageInfo

漏洞影响的仓库镜像列表

被如下接口引用：DescribeVulRegistryImageList

名称	必选	允许NULL	类型	描述
ImageID	是	否	String	镜像ID
ImageName	是	否	String	镜像名称
ImageTag	是	否	String	镜像版本
Namespace	是	否	String	镜像命名空间
ImageRepoAddress	是	否	String	镜像地址
ComponentList	是	否	Array of VulAffectedImageComponentInfo	组件列表
IsLatestImage	是	否	Bool	是否为镜像的最新版本
ImageAssetId	是	否	Int64	内部镜像资产ID

ImageVulLayerInfo

漏洞列表中的层信息

被如下接口引用：DescribeAssetImageRegistryVulList

名称	必选	允许NULL	类型	描述
LayerId	否	是	String	层id
LayerCmd	否	是	String	层cmd

ComplianceK8SDetailInfo

表示K8S资产专属的详情。

被如下接口引用：DescribeComplianceAssetDetailInfo

名称	必选	允许NULL	类型	描述
ClusterName	是	是	String	K8S集群的名称。

名称	必选	允许NULL	类型	描述
ClusterVersion	是	是	String	K8S集群的版本。

VulAffectedImageComponentInfo

受漏洞影响的组件信息

被如下接口引用：DescribeVulImageList、DescribeVulRegistryImageList

名称	必选	允许NULL	类型	描述
Name	是	是	String	组件名称
Version	是	是	String	组件版本
FixedVersion	是	是	String	组件修复版本
Path	是	是	String	组件路径

ClusterPodInfo

集群的pod详细信息

被如下接口引用：DescribeUserPodList

名称	必选	允许NULL	类型	描述
PodName	否	否	String	Pod名称.
Status	否	否	String	Pod状态
PodIP	否	否	String	Pod IP
NodeLanIP	否	否	String	节点内网Ip
WorkloadName	否	否	String	所属的工作负载名字
WorkloadKind	否	否	String	所属工作负载类型
ClusterName	否	否	String	所属集群名字
ClusterId	否	否	String	所属集群ID
Namespace	否	否	String	所属命名空间
Region	否	否	String	所属地域
Age	否	否	String	运行时间
StartTime	否	否	String	创建时间
Restarts	否	否	Uint64	重启次数
ServiceName	否	否	String	关联的service名字
ServiceCount	否	否	Uint64	关联的service数量
ContainerName	否	否	String	关联的容器名字

名称	必选	允许NULL	类型	描述
ContainerCount	否	否	Uint64	关联的容器数量
CPU	否	否	Uint64	CPU占用率
Memory	否	否	Uint64	内存占用量
Labels	否	否	String	Pod标签
ClusterStatus	否	否	String	集群状态
WorkloadLabels	否	否	String	工作负载标签
ContainerId	否	否	String	容器Id
HostName	否	否	String	主机名称
HostId	否	否	String	主机Id
ClusterType	否	否	String	集群类型
NodeName	否	否	String	abc
NodeType	否	否	String	NORMAL：普通节点 SUPER：超级节点
ChargeCoresCnt	否	否	Uint64	计费核数

EscapeEventTendencyInfo

待处理逃逸事件趋势

被如下接口引用：DescribeEscapeEventTendency

名称	必选	允许NULL	类型	描述
RiskContainerEventCount	是	否	Int64	待处理风险容器事件总数
ProcessPrivilegeEventCount	是	否	Int64	待处理程序特权事件总数
ContainerEscapeEventCount	是	否	Int64	待处理容器逃逸事件总数
Date	是	否	Date	日期

EscapeEventDescription

运行时容器逃逸事件描述信息

被如下接口引用：DescribeEscapeEventDetail

名称	必选	允许NULL	类型	描述
Description	是	否	String	事件规则
Solution	是	否	String	解决方案
Remark	是	是	String	事件备注信息
OperationTime	是	是	String	事件最后一次处理的时间

AccessControlEventDescription

运行时容器访问控制事件描述信息

被如下接口引用：DescribeAccessControlDetail

名称	必选	允许NULL	类型	描述
Description	是	否	String	事件规则
Solution	是	否	String	解决方案
Remark	是	是	String	事件备注信息
MatchRule	是	否	AccessControlChildRuleInfo	命中规则详细信息
RuleName	是	否	String	命中规则名字
RuleId	是	否	String	命中规则id
OperationTime	是	是	String	事件最后一次处理的时间

ImageDenyEventTendency

镜像拦截事件趋势

被如下接口引用：DescribeImageDenyEventTendency

名称	必选	允许NULL	类型	描述
Date	是	否	Date	日期
EventCount	是	否	Int64	事件数量

NetworkPolicyInfoItem

网络集群策略返回的结构体

被如下接口引用：DescribeNetworkFirewallPolicyList

名称	必选	允许NULL	类型	描述
Name	是	否	String	网络策略名
Description	是	是	String	网络策略描述
PublishStatus	是	否	String	发布状态：开启待确认：PublishedNoConfirm开启已确认：PublishedConfirmed关闭中：unPublishing开启中：Publishing待开启：unPublishEdit
PolicySourceType	是	否	String	策略类型：自动发现：System手动添加：Manual
Namespace	是	否	String	策略空间
PolicyCreateTime	是	否	String	策略创建日期
NetworkPolicyPlugin	是	否	String	策略类型kube-router：KubeRoutercilium：Cilium
PublishResult	是	是	String	策略发布结果

名称	必选	允许NULL	类型	描述
FromPolicyRule	是	否	Int64	入站规则全部允许：1全部拒绝 ：2自定义：3
ToPolicyRule	是	否	Int64	入站规则全部允许：1全部拒绝 ：2自定义：3
PodSelector	是	是	String	作用对象
Id	是	否	Uint64	网络策略Id

SearchTemplate

快速搜索模板

被如下接口引用：CreateSearchTemplate、DescribeSearchTemplates

名称	必选	允许NULL	类型	描述
Id	否	否	Uint64	规则ID
Name	是	否	String	检索名称
LogType	是	否	String	检索索引类型
Condition	是	否	String	检索语句
TimeRange	是	否	String	时间范围
Query	是	否	String	转换的检索语句内容
Flag	是	否	String	检索方式。输入框检索：standard,过滤，检索：simple
DisplayData	是	否	String	展示数据

CKafkaTopicInfo

Ckafka topic信息

被如下接口引用：DescribeSecLogDeliveryKafkaOptions

名称	必选	允许NULL	类型	描述
TopicID	是	否	String	主题ID
TopicName	是	否	String	主题名称

RuleBaseInfo

运行时安全，策略基本信息

被如下接口引用：DescribeAbnormalProcessRules、DescribeAccessControlRules

名称	必选	允许NULL	类型	描述
IsDefault	是	否	Bool	true: 默认策略，false:自定义策略
EffectImageCount	是	否	Uint64	策略生效镜像数量

名称	必选	允许NULL	类型	描述
RuleId	是	否	String	策略Id
UpdateTime	是	是	String	策略更新时间, 存在为空的情况
RuleName	是	否	String	策略名字
EditUserName	是	否	String	编辑用户名称
IsEnable	是	否	Bool	true: 策略启用，false：策略禁用

SuperNodePodListItem

超级节点Pod列表Item信息

被如下接口引用：DescribeSuperNodePodList

名称	必选	允许NULL	类型	描述
PodName	否	否	String	pod名称
PodIP	否	否	String	podIP
NodeUniqueID	否	否	String	节点唯一id
Status	否	否	String	运行状态
CpuRequest	否	否	Int64	cpu需求核数
CpuLimit	否	否	Int64	cpu限制核数
MemRequest	否	否	Int64	内存需求大小
MemLimit	否	否	Int64	内存限制大小
Namespace	否	否	String	命名空间
DeploymentName	否	否	String	工作负载名称
DeploymentID	否	否	String	工作负载id
StartTime	否	否	String	启动时间
CreateTime	否	否	String	创建时间
RelateContainerCount	否	否	Uint64	关联容器个数
RunningTime	否	否	String	运行时间
PodUid	否	否	String	PodUid
ChargeCoresCnt	否	否	Uint64	计费核数
DefendStatus	否	否	String	防护状态

RegistryConnDetectResult

镜像仓库联通性检测结果

被如下接口引用：DescribeAssetImageRegistryRegistryDetail、DescribeAssetImageRegistryRegistryList、ImageRegistryConnDetect

名称	必选	允许NULL	类型	描述
Quuid	否	否	String	联通性检测的主机quuid 或者 backend
Uuid	否	否	String	联通性检测的主机uuid 或者 backend
ConnDetectStatus	否	否	String	检测结果状态
ConnDetectMessage	否	否	String	检测结果信息
Solution	否	否	String	失败的解决方案
FailReason	否	否	String	失败原因

VulDefenceHost

漏洞防御的主机信息

被如下接口引用：DescribeVulDefenceHost

名称	必选	允许NULL	类型	描述
HostName	是	否	String	主机名称/超级节点名称
HostIP	是	否	String	主机ip即内网ip
HostID	是	否	String	主机QUUID/超级节点ID
Status	是	否	String	插件状态，正常：SUCCESS，异常：FAIL， NO_DEFENDED:未防御
PublicIP	是	否	String	外网ip
CreateTime	是	否	String	首次开启时间
ModifyTime	是	否	String	更新时间
NodeType	否	否	String	节点类型[NORMAL:普通节点|SUPER:超级节点]
NodeSubNetName	否	否	String	超级节点子网名称
NodeSubNetCIDR	否	否	String	超级节点子网网段
NodeSubNetID	否	否	String	超级节点子网ID
NodeUniqueID	否	否	String	超级节点唯一ID
NodeID	否	否	String	超级节点ID
PodIP	否	否	String	Pod Ip
PodName	否	否	String	Pod 名称

RunTimeFilters

容器安全 描述键值对过滤器，用于条件过滤查询。例如过滤ID、名称、状态等 若存在多个Filter时，Filter间的关系为逻辑与（AND）关系。 若同一个Filter存在多个Values，同一Filter下Values间的关系为逻辑或（OR）关系。

被如下接口引用：CreateAbnormalProcessRulesExportJob、CreateAccessControlsRuleExportJob、CreateDefenceVulExportJob、CreateEmergencyVulExportJob、CreateEscapeEventsExportJob、CreateEscapeRegexpWhiteListExportJob、CreateEscapeWhiteListExportJob、CreateEventEscapeImageExportJob、CreateImageDenyEventExportJob、

CreateImageDenyRuleExportJob、CreateImageExportJob、CreateK8sApiAbnormalEventExportJob、CreateK8sApiAbnormalRuleExportJob、CreateReverseShellRegexpWhiteListExportJob、CreateReverseShellWhiteListsExportJob、CreateRiskDnsEventExportJob、CreateSystemVulExportJob、CreateVulContainerExportJob、CreateVulDefenceEventExportJob、CreateVulDefenceHostExportJob、CreateVulImageExportJob、CreateWebVulExportJob、DeleteImageDenyEvent、DeleteImageDenyRule、DescribeAbnormalProcessEvents、DescribeAbnormalProcessEventsExport、DescribeAbnormalProcessRules、DescribeAbnormalProcessRulesExport、DescribeAccessControlEvents、DescribeAccessControlEventsExport、DescribeAccessControlRules、DescribeAccessControlRulesExport、DescribeAssetClusterList、DescribeAssetContainerPortList、DescribeAssetImageBindRuleInfo、DescribeAssetSuperNodeList、DescribeEmergencyVulList、DescribeEscapeEventInfo、DescribeEscapeEventsExport、DescribeEscapeRegexpWhiteList、DescribeEscapeWhiteList、DescribeEventEscapeImageList、DescribeExportJobManageList、DescribeImageDenyEventList、DescribeImageDenyRuleList、DescribeImageSimpleList、DescribeK8sApiAbnormalEventList、DescribeK8sApiAbnormalRuleList、DescribeK8sApiAbnormalRuleScopeList、DescribeMaliciousConnectionBlackList、DescribeMaliciousConnectionWhiteList、DescribeReverseShellEvents、DescribeReverseShellEventsExport、DescribeReverseShellRegexpWhiteList、DescribeReverseShellWhiteLists、DescribeRiskDnsList、DescribeRiskSyscallEvents、DescribeRiskSyscallEventsExport、DescribeRiskSyscallWhiteLists、DescribeScanIgnoreVulList、DescribeSecLogJoinObjectList、DescribeSecLogJoinSuperObjectList、DescribeSuperNodeInstallTaskDetail、DescribeSuperNodeInstallTaskList、DescribeSuperNodePodList、DescribeSupportDefenceVul、DescribeSystemVulList、DescribeVirusAutoIsolateSampleList、DescribeVirusList、DescribeVirusTaskList、DescribeVulContainerList、DescribeVulDefenceEvent、DescribeVulDefenceHost、DescribeVulDefencePlugin、DescribeVulImageList、DescribeVulScanLocalImageList、DescribeVulSummary、DescribeWebVulList、ExportVirusList

名称	必选	允许NULL	类型	描述
Name	是	否	String	过滤键的名称
Values	是	否	Array of String	一个或者多个过滤值。
ExactMatch	否	否	Bool	是否模糊查询

PromotionActivityContent

促销活动内容

被如下接口引用：DescribePromotionActivity

名称	必选	允许NULL	类型	描述
MonthNum	是	否	Uint64	月数
CoresCountLimit	是	否	Uint64	核数最低限量
ProfessionalDiscount	是	否	Uint64	专业版折扣
ImageAuthorizationNum	是	否	Uint64	附赠镜像数

TagInfo

主机标签信息

被如下接口引用：DescribeAssetHostDetail、DescribeAssetHostList

名称	必选	允许NULL	类型	描述
TagKey	是	否	String	标签键
TagValue	是	否	String	标签值

ImageNewVul

容器安全镜像漏洞信息

被如下接口引用：DescribeAssetImageRegistryImageLayerDetail

名称	必选	允许NULL	类型	描述
CVEID	否	是	String	漏洞id
POCID	否	是	String	观点验证程序id
Name	否	是	String	漏洞名称
Components	否	是	Array of ComponentsInfo	涉及组件信息
Category	否	是	String	分类
CategoryType	否	是	String	分类2
Level	否	是	String	风险等级
Des	否	是	String	描述
OfficialSolution	否	是	String	解决方案
Reference	否	是	Array of String	引用
DefenseSolution	否	是	String	防御方案
SubmitTime	否	是	String	提交时间
CvssScore	否	是	String	Cvss分数
CvssVector	否	是	String	Cvss信息
IsSuggest	否	是	String	是否建议修复
FixedVersions	否	是	String	修复版本号
Tag	否	是	Array of String	漏洞标签:"CanBeFixed","DynamicLevelPoc","DynamicLevelExp"
Component	否	是	String	组件名
Version	否	是	String	组件版本
AttackLevel	否	是	Int64	攻击热度 0-3
LayerCmds	否	是	Array of String	镜像层指令列表
LayerIds	否	是	Array of String	镜像层id列表

ClusterInfoItem

集群资产返回的结构体

被如下接口引用：DescribeUserCluster

名称	必选	允许NULL	类型	描述
ClusterId	否	否	String	集群id

名称	必选	允许NULL	类型	描述
ClusterName	否	否	String	集群名字
ClusterVersion	否	否	String	集群版本
ClusterOs	否	否	String	集群操作系统
ClusterType	否	否	String	集群类型
ClusterNodeNum	否	否	Uint64	集群节点数
Region	否	否	String	集群区域
DefenderStatus	否	否	String	监控组件的状态，为Defender_Uninstall、Defender_Normal、Defender_Error、Defender_Installing
ClusterStatus	否	否	String	集群状态
ClusterCheckMode	否	否	String	集群的检测模式，为Cluster_Normal或者Cluster_Actived.
ClusterAutoCheck	否	否	Bool	是否自动定期检测
DefenderErrorReason	否	否	String	防护容器部署失败原因，为UserDaemonSetNotReady时,和UnreadyNodeNum转成"N个节点防御容器为就绪"，其他错误直接展示
UnreadyNodeNum	否	否	Uint64	防御容器没有ready状态的节点数量
SeriousRiskCount	否	否	Int64	严重风险检查项的数量
HighRiskCount	否	否	Int64	高风险检查项的数量
MiddleRiskCount	否	否	Int64	中风险检查项的数量
HintRiskCount	否	否	Int64	提示风险检查项的数量
CheckFailReason	否	否	String	检查失败原因
CheckStatus	否	否	String	检查状态,为Task_Running, NoRisk, HasRisk, Uncheck, Task_Error
TaskCreateTime	否	否	String	任务创建时间,检查时间
AccessedStatus	否	是	String	接入状态:
未接入: AccessedNone				
已防护: AccessedDefended				
未防护: AccessedInstalled				
部分防护: AccessedPartialDefence				
接入异常: AccessedException				
卸载异常: AccessedUninstallException				
接入中: AccessedInstalling				
卸载中: AccessedUninstalling				
AccessedSubStatus	否	是	String	接入失败原因

名称	必选	允许NULL	类型	描述
NodeCount	否	是	Uint64	节点总数
OffLineNodeCount	否	是	Uint64	离线节点数
UnInstallAgentNodeCount	否	是	Uint64	未安装agent节点数
ChargeCoresCnt	否	是	Uint64	计费核数

ComplianceContainerDetailInfo

表示容器资产专属的详情。

被如下接口引用：DescribeComplianceAssetDetailInfo

名称	必选	允许NULL	类型	描述
ContainerId	是	否	String	容器在主机上的ID。
PodName	是	是	String	容器所属的Pod的名称。

RiskSyscallEventInfo

容器安全运行时高危系统调用信息

被如下接口引用：DescribeRiskSyscallEvents

名称	必选	允许NULL	类型	描述
ProcessName	是	否	String	进程名称
ProcessPath	是	否	String	进程路径
ImageId	是	否	String	镜像id
ContainerId	是	否	String	容器id
ImageName	是	否	String	镜像名
ContainerName	是	否	String	容器名
FoundTime	是	否	String	生成时间
Solution	是	否	String	事件解决方案
Description	是	否	String	事件详细描述
SyscallName	是	否	String	系统调用名称
Status	是	否	String	状态，EVENT_UNDEAL:事件未处理 EVENT_DEALED:事件已经处理 EVENT_INGNORE：事件已经忽略 EVENT_ADD_WHITE：时间已经加白
EventId	是	否	String	事件id
NodeName	是	否	String	节点名称
PodName	是	否	String	pod(实例)的名字
Remark	是	否	String	备注

名称	必选	允许NULL	类型	描述
RuleExist	是	否	Bool	系统监控名称是否存在
EventCount	是	否	Int64	事件数量
LatestFoundTime	是	否	String	最近生成时间
ContainerNetStatus	是	否	String	网络状态未隔离 NORMAL已隔离 ISOLATED隔离中 ISOLATING隔离失败 ISOLATE_FAILED解除隔离中 RESTORING解除隔离失败 RESTORE_FAILED
ContainerNetSubStatus	是	否	String	容器子状态"AGENT_OFFLINE" //Agent离线"NODE_DESTROYED" //节点已销毁"CONTAINER_EXITED" //容器已退出"CONTAINER_DESTROYED" //容器已销毁"SHARED_HOST" // 容器与主机共享网络"RESOURCE_LIMIT" //隔离操作资源超限"UNKNOW" // 原因未知
ContainerIsolateOperationSrc	是	否	String	容器隔离操作来源
ContainerStatus	是	否	String	容器状态正在运行: RUNNING暂停: PAUSED停止: STOPPED已经创建: CREATED已经销毁: DESTROYED正在重启中: RESTARTING迁移中: REMOVING
NodeType	否	否	String	节点类型：NORMAL普通节点、SUPER超级节点
ClusterID	否	否	String	集群I'D
PodIP	否	否	String	pod ip
NodeUniqueID	否	否	String	节点唯一id
PublicIP	否	否	String	节点公网ip
NodeID	否	否	String	节点id
HostID	否	否	String	uuid
HostIP	否	否	String	节点内网ip
ClusterName	否	否	String	集群名称

RunTimeEventBaseInfo

运行时安全事件基本信息

被如下接口引用：DescribeAbnormalProcessDetail、DescribeAccessControlDetail、DescribeEscapeEventDetail、DescribeReverseShellDetail、DescribeRiskSyscallDetail

名称	必选	允许NULL	类型	描述
EventId	否	否	String	事件唯一ID
FoundTime	否	否	Datetime	事件发现时间
ContainerId	否	否	String	容器id
ContainerName	否	否	String	容器名称
ImageId	否	否	String	镜像id
ImageName	否	否	String	镜像名称
NodeName	否	否	String	节点名称

名称	必选	允许NULL	类型	描述
Status	否	否	String	状态，“EVENT_UNDEAL”:事件未处理 "EVENT_DEALED":事件已经处理 "EVENT_INGNORE"：事件已经忽略
EventName	否	否	String	事件名称：宿主机文件访问逃逸、Syscall逃逸、MountNamespace逃逸、程序提权逃逸、特权容器启动逃逸、敏感路径挂载恶意进程启动文件篡改
EventType	否	否	String	事件类型 ESCAPE_HOST_ACESS_FILE:宿主机文件访问逃逸 ESCAPE_MOUNT_NAMESPACE:MountNamespace逃逸 ESCAPE_PRIVILEDGE:程序提权逃逸 ESCAPE_PRIVILEDGE_CONTAINER_START:特权容器启动逃逸 ESCAPE_MOUNT_SENSITIVE_PTAH:敏感路径挂载 ESCAPE_SYSCALL:Syscall逃逸
EventCount	否	否	Int64	事件数量
LatestFoundTime	否	否	String	最近生成时间
HostIP	否	是	String	内网ip
ClientIP	否	是	String	外网ip
ContainerNetStatus	否	是	String	网络状态未隔离 NORMAL已隔离 ISOLATED隔离中 ISOLATING隔离失败 ISOLATE_FAILED解除隔离中 RESTORING解除隔离失败 RESTORE_FAILED
ContainerNetSubStatus	否	是	String	容器子状态"AGENT_OFFLINE" //Agent离线"NODE_DESTROYED" //节点已销毁"CONTAINER_EXITED" //容器已退出"CONTAINER_DESTROYED" //容器已销毁"SHARED_HOST" // 容器与主机共享网络"RESOURCE_LIMIT" //隔离操作资源超限"UNKNOW" // 原因未知
ContainerIsolateOperationSrc	否	是	String	容器隔离操作来源
NodeID	否	否	String	节点ID
NodeType	否	否	String	节点类型:NORMAL:普通节点;SUPER:超级节点
NodeSubNetID	否	否	String	节点子网ID
NodeSubNetName	否	否	String	节点子网名称
NodeSubNetCIDR	否	否	String	节点子网网段
PodName	否	否	String	pod名称
PodIP	否	否	String	podIP
PodStatus	否	否	String	pod状态
ClusterID	否	否	String	集群id
ClusterName	否	否	String	集群名称
NodeUniqueID	否	否	String	节点唯一id
HostID	否	否	String	uuid
Namespace	否	否	String	Namespace
WorkloadType	否	否	String	WorkloadType

VulnerabilityFocusRuleTags

重点漏洞关注标签组

被如下接口引用：DescribeVulnerabilityFocusRuleDetail、ModifyVulnerabilityFocusRule

名称	必选	允许NULL	类型	描述
VulnerabilityFocusRuleTagValues	否	是	Array of String	漏洞重点关注标签数组

NetworkClusterSwitchListItem

网络集群拓扑开关

被如下接口引用：DescribeNetworkTopologyFlowSwitchList

名称	必选	允许NULL	类型	描述
ClusterId	否	是	String	集群Id
Region	否	是	String	区域
ClusterName	否	是	String	集群名称
ClusterType	否	是	String	集群类型
ClusterVersion	否	是	String	集群版本
ClusterOs	否	是	String	集群OS信息
ClusterStatus	否	是	String	集群状态
FlowSwitch	否	是	String	集群流量开关 ON:打开，OFF关闭
ClusterNodeNum	否	是	Uint64	集群拥有节点个数
FlowSupport	否	是	String	集群流量支持Enable支持，Disable不支持
FlowUnsupportReason	否	是	String	集群流量不支持原因

ReverseShellWhiteListInfo

反弹shell白名单信息

被如下接口引用：AddEditReverseShellWhiteList、DescribeReverseShellWhiteListDetail

名称	必选	允许NULL	类型	描述
DstIp	是	否	String	目标IP
DstPort	是	否	String	目标端口

名称	必选	允许NULL	类型	描述
ProcessName	是	否	String	目标进程
ImageIds	是	否	Array of String	镜像id数组，为空代表全部
Id	否	否	String	白名单id，如果新建则id为空

RegionInfo

地域信息

被如下接口引用：DescribeSecLogDeliveryClsOptions、DescribeSecLogDeliveryKafkaOptions

名称	必选	允许NULL	类型	描述
Region	是	否	String	地域标识
RegionName	是	否	String	地域名称

ClusterCustomParameters

集群自定义参数

被如下接口引用：DescribeAgentDaemonSetCmd

名称	必选	允许NULL	类型	描述
Name	是	否	String	参数名
Values	是	否	Array of String	参数值

RiskSyscallWhiteListBaseInfo

高危系统调用白名单信息

被如下接口引用：DescribeRiskSyscallWhiteLists

名称	必选	允许NULL	类型	描述
Id	是	否	String	白名单id
ImageCount	是	否	Uint64	镜像数量
ProcessPath	是	否	String	连接进程路径
SyscallNames	是	否	Array of String	系统调用名称列表
CreateTime	是	否	Datetime	创建时间
UpdateTime	是	否	Datetime	更新时间
IsGlobal	是	否	Bool	是否是全局白名单，true全局
ImageIds	是	否	Array of String	镜像id数组

K8sApiAbnormalTendencyItem

k8sapi异常请求趋势Item

被如下接口引用：DescribeK8sApiAbnormalTendency

名称	必选	允许NULL	类型	描述
Date	是	否	String	日期
ExceptionUARequestCount	是	否	Uint64	异常UA请求事件数
AnonymousUserRightCount	是	否	Uint64	匿名用户权限事件数
CredentialInformationObtainCount	是	否	Uint64	凭据信息获取事件数
SensitiveDataMountCount	是	否	Uint64	敏感数据挂载事件数
CmdExecCount	是	否	Uint64	命令执行事件数
AbnormalScheduledTaskCount	是	否	Uint64	异常定时任务事件数
StaticsPodCreateCount	是	否	Uint64	静态Pod创建数
DoubtfulContainerCreateCount	是	否	Uint64	可疑容器创建数
UserDefinedRuleCount	是	否	Uint64	自定义规则事件数
AnonymousAccessCount	是	否	Uint64	匿名访问事件数
PrivilegeContainerCount	是	否	Uint64	特权容器事件数

AbnormalProcessEventDescription

运行时容器访问控制事件描述信息

被如下接口引用：DescribeAbnormalProcessDetail

名称	必选	允许NULL	类型	描述
Description	是	否	String	事件规则
Solution	是	否	String	解决方案
Remark	是	是	String	事件备注信息
MatchRule	是	否	AbnormalProcessChildRuleInfo	命中规则详细信息
RuleName	是	否	String	命中规则名称，PROXY_TOOL：代理软件，TRANSFER_CONTROL：横向渗透，ATTACK_CMD：恶意命令，REVERSE_SHELL：反弹shell，FILELESS：无文件程序执行，RISK_CMD：高危命令，ABNORMAL_CHILD_PROC：敏感服务异常子进程启动，USER_DEFINED_RULE：用户自定义规则
RuleId	是	否	String	命中规则的id
OperationTime	是	是	String	事件最后一次处理的时间
GroupName	是	是	String	命中策略名称：SYSTEM_DEFINED_RULE（系统策略）或 用户自定义的策略名字

RiskSyscallWhiteListInfo

高危系统调用白名单信息

被如下接口引用：AddEditRiskSyscallWhiteList、DescribeRiskSyscallWhiteListDetail

名称	必选	允许NULL	类型	描述
SyscallNames	否	否	Array of String	系统调用名称，通过DescribeRiskSyscallNames接口获取枚举列表
ProcessPath	否	否	String	目标进程
ImageIds	是	否	Array of String	镜像id数组，为空代表全部
Id	否	否	String	白名单id，如果新建则id为空

UpgradeAgentInfo

升级agent信息

被如下接口引用：DescribeUpgradeAgentList

名称	必选	允许NULL	类型	描述
HostName	是	否	String	主机名称
InnerIp	是	否	String	内部ip
PublicIp	是	否	String	外网ip
CurrentVersion	是	否	String	升级前版本
UpgradeVersion	是	否	String	升级后的版本
Status	是	否	String	升级状态， 成功：SUCCESSED, 失败：FAILED, 升级中：UPGRADING
HostID	是	否	String	唯一id

NetworkClusterNamespaceLabelInfo

网络集群网络空间标签返回的结构体

被如下接口引用：DescribeNetworkFirewallNamespaceLabelList

名称	必选	允许NULL	类型	描述
Labels	是	否	String	网络空间标签
Name	是	否	String	网络空间名字

错误码

最近更新时间: 2024-09-03 18:49:52

功能说明

如果返回结果中存在 Error 字段，则表示调用 API 接口失败。例如：

```
{
"Response": {
"Error": {
"Code": "AuthFailure.SignatureFailure",
"Message": "The provided credentials could not be validated. Please check your signature is correct."
},
"RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
}
}
```

Error 中的 Code 表示错误码，Message 表示该错误的具体信息。

错误码列表

公共错误码

错误码	说明
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）。
AuthFailure.MFAFailure	MFA 错误。
AuthFailure.SecretIdNotFound	密钥不存在。 请在控制台检查密钥是否已被删除或者禁用，如状态正常，请检查密钥是否填写正确，注意前后不得有空格。
AuthFailure.SignatureExpire	签名过期。Timestamp 和服务器时间相差不得超过五分钟，请检查本地时间是否和标准时间同步。
AuthFailure.SignatureFailure	签名错误。 签名计算错误，请对照调用方式中的接口鉴权文档检查签名计算过程。
AuthFailure.TokenFailure	token 错误。
AuthFailure.UnauthorizedOperation	请求未 CAM 授权。
DryRunOperation	DryRun 操作，代表请求将会是成功的，只是多传了 DryRun 参数。
FailedOperation	操作失败。
InternalError	内部错误。
InvalidAction	接口不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
NoSuchVersion	接口版本不存在。

错误码	说明
RequestLimitExceeded	请求的次数超过了频率限制。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
UnauthorizedOperation	未授权操作。
UnknownParameter	未知参数错误。
UnsupportedOperation	操作不支持。
UnsupportedProtocol	http(s)请求协议错误，只支持 GET 和 POST 请求。
UnsupportedRegion	接口不支持所传地域。

业务错误码

错误码	说明
FailedOperation.ErrAlreadyScanning	
InvalidParameterValue.LengthLimit	
ResourceUnavailable	
LimitExceeded	
FailedOperation.ErrRuleNotFind	
FailedOperation.DataValueNotCorrect	
RequestLimitExceeded	
InternalError.ErrRoleNotExist	
MissingParameter	
FailedOperation	
FailedOperation.AuthorizedNotEnough	
InvalidParameterValue	
InternalError	
InvalidParameter	
FailedOperation.NotifyPolicyChangeFailed	
UnauthorizedOperation	
InvalidParameter.MissingParameter	
ResourceInsufficient	
InvalidParameter.RegexRuleError	

错误码	说明
InvalidParameter.ReverShellKeyFieldAllEmpty	
InvalidParameter.InvalidFormat	
ResourceNotFound	
InvalidParameter.PortNoValid	
OperationDenied	
FailedOperation.RuleNameRepeat	
UnknownParameter	
InvalidParameter.ErrIpNoValid	
InvalidParameter.ParsingError	
FailedOperation.RuleNotFind	
FailedOperation.AgentOffline	
AuthFailure	
InternalError.MainDBFail	
InvalidParameterValue.DataRange	
FailedOperation.RuleInfoRepeat	
InvalidParameter.RuleInfoInValid	
UnsupportedOperation	
ResourceInUse	
InvalidParameterValue.DataNotFound	
FailedOperation.RuleSelectImageOutRange	
FailedOperation.RuleConfigTooMany	