主机安全（CWP）

产品文档



腾讯云TCE

目录

主机安全（CWP） 7
- 产品简介 7
  - 产品概述 7
  - 产品优势 9
  - 基本概念 10
- 快速入门 11
  - 快速入门 11
- 产品架构 13
  - 产品架构 13
- 操作指南 15
  - 安全概览 15
  - 资产概览 20
  - 主机列表 23
  - 资产指纹 27
  - 文件查杀 35
  - 异常登录 41
  - 密码破解 47
  - 恶意请求 50
  - 本地提权 56
  - 反弹Shell 61
  - 高危命令 66
  - 网络攻击 72
  - Java内存马 76
  - 核心文件监控 80
  - 漏洞管理 84
  - 安全基线 91
  - 常用操作 97
    - 未防护主机安装agent 97
    - 单台主机漏洞扫描 99
    - 单台主机基线扫描 100
- 故障处理 104
  - Linux入侵类问题排查思路 104
  - Windows入侵类问题排查思路 108
  - Linux 客户端离线排查 111
  - Windows 客户端离线排查 113
  - 异常登录的消息提醒 114
- 实践教程 117
  - 漏洞自动修复 117
- 常见问题 122
  - 功能相关 122
  - 入侵相关 126
- 软件相关说明 130
  - 功能行为描述 130
  - 客户端进程说明 132
  - 安全基线检测列表 134
- API文档 136
  - 主机安全（cwp） 136
    - 版本（2018-02-28） 136
      - API 概览 136
      - 调用方式 154
        - 接口签名v1 154
        - 接口签名v3 161
        - 请求结构 170
        - 返回结果 171
        - 公共参数 174
      - 专家服务相关接口 176
        - 应急响应列表 176
        - 安全管家月巡检报告下载 178
      - 入侵检测-反弹shell相关接口 180
        - 删除反弹Shell规则 180
        - 删除反弹Shell事件 182
        - 删除反弹Shell规则 184
        - 删除反弹Shell规则 186
        - 获取反弹Shell规则列表 188
        - 获取反弹Shell列表 190
        - 获取反弹Shell规则列表 193
        - 获取反弹Shell规则列表 195
        - 查询反弹shell系统策略配置 197
        - 查询反弹shell策略列表 199
        - 导出反弹Shell事件 201
        - 编辑反弹Shell规则（支持多服务器选择） 203
        - 修改反弹shell系统策略配置 206
        - 编辑反弹shell策略开关 208
      - 入侵检测-密码破解相关接口 210
        - 删除暴力破解记录 210
        - 获取爆破阻断模式 212
        - 获取阻断地域 214
        - 获取阻断按钮状态 216
        - 获取阻断白名单列表 218
        - 获取密码破解列表 220
        - 获取爆破破解规则 223
        - 导出密码破解记录 225
        - 修改爆破阻断模式 227
        - 设置阻断开关状态 229
        - 修改暴力破解规则 231
        - 不再提醒爆破阻断提示弹窗 233
      - 入侵检测-异常登录相关接口 234
        - 删除异地登录白名单规则 234
        - 删除异地登录记录 236

- 获取登录审计列表 238
- 获取异地登录白名单合并后列表 241
- 获取异地登录白名单列表 243
- 查询常用登录地 245
- 导出异地登录记录 247
- 入侵检测-恶意请求相关接口 249
- 删除恶意请求记录 249
- 查询恶意请求白名单列表 251
- 获取恶意请求列表 253
- 导出下载恶意请求文件 255
- 入侵检测-文件查杀相关接口 257
- 创建网络攻击白名单 257
- 文件查杀检测 259
- 入侵管理-终止扫描任务 262
- 删除木马记录 264
- 删除网络攻击白名单 266
- 查询java内存马事件列表 268
- 获取木马列表 270
- 获取木马文件下载地址 272
- 查看恶意文件详情 274
- 风险预警提示 276
- 查询定时扫描配置 278
- 获取网络攻击白名单列表 281
- 查询木马扫描进度 283
- 获文件查杀概览信息 285
- 导出木马记录 287
- 定时扫描设置 289
- 编辑网络攻击白名单 292
- 恢复木马文件 294
- 隔离木马 296
- 信任木马文件 298
- 取消信任木马 300
- 入侵检测-本地提权相关接口 302
- 删除本地提权事件 302
- 删除本地提权规则 304
- 获取本地提权事件列表 306
- 获取本地提权规则列表 309
- 导出本地提权事件 311
- 入侵检测-高危命令相关接口 313
- 校验高危命新增用户规则参数 313
- 删除高危命令事件 315
- 删除高危命令规则 317
- 获取高危命令列表 319
- 获取高危命令列表(新) 322
- 获取高危命令规则列表 325
- 新增或修改高危命令规则（支持多服务器选择） 327
- 导出高危命令事件 330
- 设置高危命令事件状态 332
- 切换高危命令规则状态 334
- 其他接口 336
- 下发登录许可 336
- 修改日志cls投递配置 338
- 停止扫描任务 340
- 查询资产管理环境变量列表 342
- 获取客户端异常事件 345
- 查询cls账户状态 347
- 查询cls日志集列表 349
- 查询cls日志集列表 351
- 查询客户信息 353
- 获取主机相关统计 355
- 获取cls投递信息 358
- 获取是否创建客户 360
- 获取日志存储量记录 362
- 检查用户是否有指定主机登录权限 364
- 获取机器信息 366
- 获取主机登录方式 368
- 获取主机登录方式状态 370
- 查询资源订单列表 372
- 获取概览统计数据 374
- 获取专业版概览信息 376
- 获取专业版状态 378
- 查询推荐购买防护核数 380
- 查询扫描状态 382
- 查询扫描任务详情 385
- 获取安全事件动态消息 388
- 获取安全事件统计 390
- 获取安全事件数统计数据 393
- 获取安全事件统计数据 396
- 获取任务下发时长 399
- 查询主机安全授权试用报告(仅限控制台申领的) 401
- 用于查询用户自定义配置 403
- 获取专业版和基础版机器数 405
- 获取漏洞态势信息 407
- 导出扫描任务详情 409
- 导出风险趋势 411
- 异步导出任务 413
- 修改网络攻击事件状态 415
- 修改日志cls投递配置 418
- 修改某个日志类型的cls投递开关 420
- 修改日志存储配置 422
- 修改主机登录方式 424

- 新购/变配 订单 426
- 用于创建/修改用户自定义配置 428
- 安全中心漏洞防御、网络攻击开关修改 430
- 基线管理相关接口 432
  - 修改事件忽略状态 432
  - 创建基线策略 434
  - 删除基线策略 437
  - 基线策略概览统计数据查询 439
  - 查询基线基础信息 441
  - 查询基线详情 443
  - 基线影响主机列表 445
  - 服务器风险top接口 447
  - 查询基线列表 449
  - 查询基线检测项信息 451
  - 基线检测进度查询 453
  - 查询基线策略详情 455
  - 用户基线策略列表查询 458
  - 基线检测项TOP 460
  - 查询忽略检测项信息 462
  - 查询忽略检测项影响主机列表 464
  - 根据策略名查询策略是否存在 466
  - 基线影响主机列表导出 468
  - 导出基线列表 470
  - 已忽略基线检测项导出 472
  - 忽略检测项影响主机列表导出 474
  - 更新基线策略信息 476
- 安全运营相关接口 479
  - 添加历史搜索记录 479
  - 添加检索模板 481
  - 删除检索模板 483
  - 获取ES字段聚合结果 485
  - 查询日志检索服务信息 487
  - 获取索引列表 489
  - 获取日志检索容量使用统计 491
  - 导出ES查询文档列表 493
  - 获取历史搜索记录 495
  - 获取快速检索列表 497
- 新版基线管理相关接口 499
  - 删除基线策略配置 499
  - 删除基线规则 500
  - 删除基线忽略规则 502
  - 删除基线弱口令 504
  - 获取基线检测详情记录 506
  - 获取基线检测概览 508
  - 获取基线下载列表 510
  - 获取基线修复列表 512
  - 获取基线检测主机列表 514
  - 获取忽略规则主机列表 516
  - 获取基线服务器风险TOP5 518
  - 获取基线检测项的列表 520
  - 获取忽略规则项列表 522
  - 获取基线检测项信息 524
  - 获取基线项检测结果列表 526
  - 获取基线检测项TOP5 528
  - 获取基线策略列表 530
  - 获取基线分类列表 532
  - 获取基线规则检测列表 534
  - 获取基线忽略规则列表 536
  - 获取基线规则列表 538
  - 获取基线弱口令列表 540
  - 获取全网热点漏洞 542
  - 获取一键忽略受影响的检测项和主机信息 544
  - 获取漏洞库列表 546
  - 导出修复列表 549
  - 导出基线主机检测 551
  - 导出基线检测项 553
  - 导出检测项结果列表 555
  - 导出基线检测规则 557
  - 导出弱口令配置列表 559
  - 修复基线检测 561
  - 修改或新增基线策略设置 563
  - 修改或新增基线策略状态 565
  - 修改或新增基线检测规则 567
  - 修改或新增基线忽略规则 569
  - 修改或新增弱口令 571
  - 检测基线 573
  - 停止基线检测 575
  - 同步基线检测进度概要 577
- 漏洞管理相关接口 579
  - 取消漏洞忽略 579
  - 应急漏洞扫描 581
  - 应急漏洞列表 583
  - 查询java内存马和rasp的是否注入风险服务配置 586
  - 查询检测进度 588
  - 定期检测配置查询 590
  - 获取指定漏洞分类统计数 592
  - 获取近日指定类型的漏洞数量和主机数量 594
  - 获取漏洞防御策略和事件统计 596
  - 查询漏洞防御设置列表 598
  - 漏洞影响主机列表 600
  - 获取待处理漏洞数+影响主机数 603

- 获取服务器风险top列表 605
- 漏洞详情 607
- 查询漏洞数量等级分布统计 610
- 漏洞列表 612
- 获取漏洞top统计 615
- 导出本次漏洞检测Excel 617
- 导出漏洞检测报告 619
- 导出漏洞影响主机列表 621
- 漏洞管理-导出漏洞列表 623
- 忽略漏洞 625
- 是否注入风险服务开关，包括内存马、rasp都是这个接口，容器rasp的开关在容器服务里 627
- 一键检测 629
- 漏洞管理-重新检测接口 632
- 定期扫描漏洞设置 634

• 设置中心相关接口 636
- 创建安装主机安全agent任务 636
- 创建授权订单 638
- 删除授权记录 641
- 获取机器安装结果 643
- 获取ageng安装任务完成情况 645
- 获取修改中的主机列表 647
- 查看授权绑定列表 649
- 查询授权绑定进度 651
- 授权概览信息 653
- 获取授权订单列表 656
- 更新用户告警设置 658
- 获取当前用户告警列表 660
- 获取告警服务IP名单 662
- 销毁订单 664
- 导出授权详情 666
- 修改主机防护状态 668
- 设置自动开通配置 670
- 授权批量绑定 672
- 编辑《主机安全-按量计费》授权订单 674
- 授权批量解绑 676
- 编辑订单属性 678
- 修改告警设置 680

• 资产管理相关接口 682
- 对旗舰版机器单次触发事件调查及告警回溯 682
- 删除AK配置 684
- 卸载云镜客户端 686
- 删除服务器关联的标签 688
- 删除标签 690
- 获取帐号统计列表数据 692
- 查询应用列表 694
- 获取软件关联进程列表 697
- 获取内核模块详情 699
- 查询资产管理内核模块列表 701
- 获取资产管理数据库详情 704
- 查询资产管理数据库列表 706
- 获取主机所有资源数量 709
- 获取资产数量概况 711
- 查询资产管理启动服务列表 714
- 获取Jar包详情 717
- 查询Jar包列表 719
- 获取资产管理主机资源详细信息 722
- 获取资源监控列表 724
- 查询资产管理计划任务列表 727
- 获取资产管理端口列表 730
- 获取资产管理进程列表 733
- 获取主机概况趋势 736
- 获取资产管理系统安装包列表 738
- 获取主机账号详情 740
- 获取账号列表 742
- 获取资产管理Web应用列表 745
- 获取资产管理Web应用插件列表 748
- 获取资产管理Web框架列表 750
- 获取Web站点详情 753
- 获取Web站点列表 755
- 查询资产管理Web服务列表 758
- 获取Web服务关联进程列表 761
- 获取用户添加的云厂商AK列表 763
- 获取组件统计列表 765
- 本接口 (DescribeComponents) 用于获取组件列表数据。 767
- 导出区域主机列表 769
- 获取帐号变更历史列表 771
- 查询批量导入机器信息 773
- 获取机器详情 775
- 查询机器操作系统列表 779
- 查询主机地域列表 781
- 获取机器地域列表 783
- 获取区域主机列表 785
- 获取端口统计列表 787
- 获取进程统计列表 789
- 获取指定标签关联的服务器信息 791
- 获取所有主机标签 793
- 新增或编辑标签 795
- 导出资产管理内核模块列表 797
- 导出资产管理Web服务列表 799
- 修改主机备注信息 801
- 资产指纹启动扫描 803

- 同步资产扫描信息 805
- 关联机器标签列表 807
- 高级防御相关接口 809
- 创建微告警负载标签 809
- 添加网站防护服务器 811
- 删除网络攻击日志 813
- 删除微告警访问事件 815
- 删除微告警自定义白名单 817
- 删除微告警标签 819
- 删除微告警自学习子策略 821
- 删除微告警全局白名单 823
- 删除防护网站 825
- 删除事件记录 827
- 网络攻击事件详情 829
- 按分页形式展示网络攻击检测事件列表 831
- 网络攻击日志详情 833
- 网络攻击日志列表 836
- 网络攻击数据统计 838
- 网络攻击top5数据列表 840
- 网络攻击趋势数据 842
- 获取网络攻击威胁类型列表 844
- 获取微告警访问事件 846
- 获取微告警自定义白名单 848
- 获取微告警全局配置 850
- 获取微告警主机列表 852
- 获取微告警标签信息 854
- 获取微告警标签列表 856
- 获取微告警标签来源列表 858
- 获取微告警POD列表 860
- 获取微告警自学习策略 862
- 获取微告警自学习子策略列表 864
- 获取微告警整体概要 866
- 获取微告警全局白名单设置 869
- 获取微告警负载标签 871
- 获取微告警负载列表 873
- 网页防篡改获取区域主机列表 875
- 查询网络攻击设置 877
- 防护目录列表 879
- 查询防护目录关联服务器 881
- 查询服务器关联目录详情 883
- 查询篡改事件列表 885
- 查询网页防篡改概览信息 887
- 查询网页防篡改防护统计 889
- 查询网站防篡改服务信息 891
- 关闭微告警自学习 893
- 导出网络攻击事件 895
- 导出网络攻击日志 897
- 导出微告警访问事件 899
- 导出微告警自定义白名单 901
- 导出微告警主机列表 903
- 导出微告警POD列表 905
- 导出微告警自学习子策略 907
- 导出微告警全局白名单 909
- 导出防护目录列表 911
- 导出篡改事件列表 913
- 更改微告警访问事件类型，可实现取消加白 915
- 创建或者更改微告警自定义白名单 917
- 更微告警自定义白名单状态 919
- 修改微告警全局配置 921
- 新增或更改标签信息 923
- 配置自学习策略 925
- 更改微告警全局白名单设置 927
- 更改微告警全局白名单状态 929
- 更改微告警负载标签 931
- 更改微告警负载监控 933
- 编辑或者创建java内存马白名单 935
- 修改网络攻击设置 937
- 创建网站防护目录 939
- 修改网站防护设置 941
- 网站防护设置开关 943
- 数据结构 945
- 错误码 1031

产品简介
产品概述

什么是主机安全

主机安全是一款针对overlay、underlay主机的安全防护产品，基于海量威胁数据，利用机器学习为您提供黑客入侵检测和漏洞风险预警等安全防护服务，主要包括密码破解拦截、异常登录提醒、木马文件检测、高危漏洞检测等安全功能，解决当前服务器面临的主要网络安全风险，帮助企业构建服务器安全防护体系。

为什么需要主机安全

服务器一旦被黑客入侵，企业面临以下安全风险：

- 业务被中断：数据库、文件被篡改或删除，导致服务无法访问，系统瘫痪。
- 数据被窃取：黑客窃取企业数据后公开售卖，客户隐私数据被泄漏，造成企业品牌受损和客户流失。
- 被加密勒索：黑客入侵服务器后通过植入不可逆的加密勒索软件对数据进行加密，对企业进行金钱勒索。
- 服务不稳定：黑客在服务器中运行挖矿程序，并通过 DDoS 木马程序获取经济利益，消耗大量的系统资源，导致服务器不能提供正常服务。

使用主机安全可以有效预防以上问题，保障企业主机安全。

主机安全主要功能

文件查杀

网站后门木马又叫 Webshell，一般是黑客通过漏洞入侵网站后放置的 ASP、PHP、JSP 等动态脚本。黑客可以通过后门木马持续控制服务器，进行文件上传下载、执行命令等各种破坏行为，对网站安全危害极大。
基于机器学习的网站后门检测技术并依托全网恶意文件样本收集能，主机安全可以实时准确的检测各类木马恶意文件，同时提供恶意文件检测和一键隔离等功能，保护您服务的安全。

异常登录

基于常用登录源 IP、登录用户名、登录时间、登录地四个维度对服务器登录日志进行分析，以识别出登录流水中异常登录的行为，根据智能算法将异常登录记录标记为“可疑”或“高危”，并向您提供实时告警通知。

密码破解

您的云服务器可通过互联网登录，给了不法之徒进行暴力破解尝试入侵您云服务器的机会。主机安全通过多维度多种手段检测云服务器是否被尝试暴力破解其密码。若检测有异常，会通过站内信或者短信等渠道对您进行告知。

恶意请求

主机安全通过对外界请求行为的实时监控及处理能力，实现对恶意请求行为的有效识别。若检测到恶意请求行为，主机安全系统会向您提供实时告警通知。

高危命令

基于安全技术及多维度多种手段，对系统中命令实现实时监控，并且可通过配置规则对命令危险程度进行等级划分。若检测出高危命令，主机安全系统会向您提供实时告警通知。

本地提权

若出现以低权限进入系统，并通过某些手段提升权限，获取到高权限的事件，很有可能为黑客的攻击行为，该行为会危害到云服务器的安全。主机安全的本地提权功能可实时监控您服务器上的提权事件，并能对提权事件详情进行查看和处理，同时也支持白名单创建功能，用于设置被允许的提权行为。

反弹 Shell

反弹 Shell 功能是基于安全技术及多维度多种手段，对服务器上的 Shell 反向连接行为进行识别记录，为您的云服务器提供反弹 Shell 行为的实时监控能力。

漏洞管理

主机安全对云服务器上存在的高危漏洞风险进行实时预警并提供修复方案，包括应急漏洞、Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞，帮助企业快速应对漏洞风险。

基线管理

主机安全支持对基线检测项的定期检测和一键检测、支持对指定主机上的指定基线项进行检测、支持通过检测策略了解基线通过率及风险情况，同时可提供基线和检测项的风险等级和修复建议，同时提供默认基线策略，有助于您更好的管理服务器中的基线安全。

高级防御

实时监控网络攻击行为，支持检测的威胁类型包括：Webshell 探测、Struts 漏洞利用、代码仓库拉取、代码注入攻击、命令注入攻击及机器批量控制利用等。

产品优势

主机安全与其他主机安全产品的优势比较如下表所示：

优势	主机安全	其他主机安全产品
黑客行为检测	基于平台全网威胁数据源，实时检测黑客攻击行为。	基于单一主机行为数据进行判断，检测能力弱，无法快速响应。
木马文件检测	后端集成电脑管家新一代 TAV 反病毒引擎及哈勃分析系统，极速响应未知风险。基于机器学习的 WebShell 检测引擎，有效对抗加密变形类恶意脚本。	可执行恶意文件的检测能力缺失，基于正则、字符逻辑匹配方式对 WebShell 进行检测，误报、漏报风险高。
免安装、维护	自动关联平台服务器运维信息，开通云服务器即可使用相关信息。安全策略云端自动更新，无需人工维护各种安全检测脚本文件。	需要用户登录服务器手动安装，且需要一定安全技术能力的人进行安全策略配置。
集中运维	安全事件可在控制台统一管理，省去登录多台服务器的麻烦。主机资产集中管理，快速构建安全可视化运维平台。	需要登录到服务器上，对单个安全事件进行处理。
低资源占用	轻量级 Agent，绝大部分计算和防护在云端进行，对服务器的资源消耗占用低。平均 CPU 小于5%，静默状态平均内存小于30M。	软件客户端内存占用高，普遍消耗在100M以上，业务峰期会影响服务器性能。

基本概念

安全基线

安全基线（Security Baseline）指为了满足安全要求，相关系统和服务安全配置必须达到的一定标准和基本要求。通过对不同配置和策略的具体项目来评估产品是否达到安全基线，包括账号配置安全、口令配置安全、授权配置、日志配置、网络配置等。安全基线评估结果在一定程度上，反映了服务器的安全性。

木马病毒

木马病毒是指隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和 DDoS 攻击等特殊功能的后门程序。

WebShell

WebShell 就是以 ASP、PHP、JSP 或 CGI 等网页文件形式存在的一种命令执行环境，也称为一种网页后门。黑客在入侵了一个网站后，通常会将 ASP 或 PHP 后门文件与网站服务器 Web 目录下正常的网页文件混在一起，然后使用浏览器来访问 ASP 或者 PHP 后门，得到一个命令执行环境，以达到控制网站服务器的目的。

主机漏洞检测

主机漏洞检测（Host Vulnerability Detection）指基于主机 Agent 在主机内部发现漏洞的一种方式。将漏洞检测模块运行于主机内部，直接进行验证或者采集信息，来判断主机是否存在漏洞。

未授权访问

未授权访问（Unauthorized Access）是不满足安全基线导致的一类问题，主要指相关服务没有对服务的访问条件进行限制，例如设置密码、限制访问来源等，导致任何人都可以直接连接服务进行操作，从而产生安全问题。

异常登录

通过采集服务器上 RDP、SSH 登录日志，上报登录源 IP、登录用户名、登录时间、登录地等信息到云端进行风险评定，对非法登录进行实时告警通知。

隔离文件

通过隔离技术把存在恶意行为的木马、病毒文件进行隔离存储，避免恶意文件持续扩散。

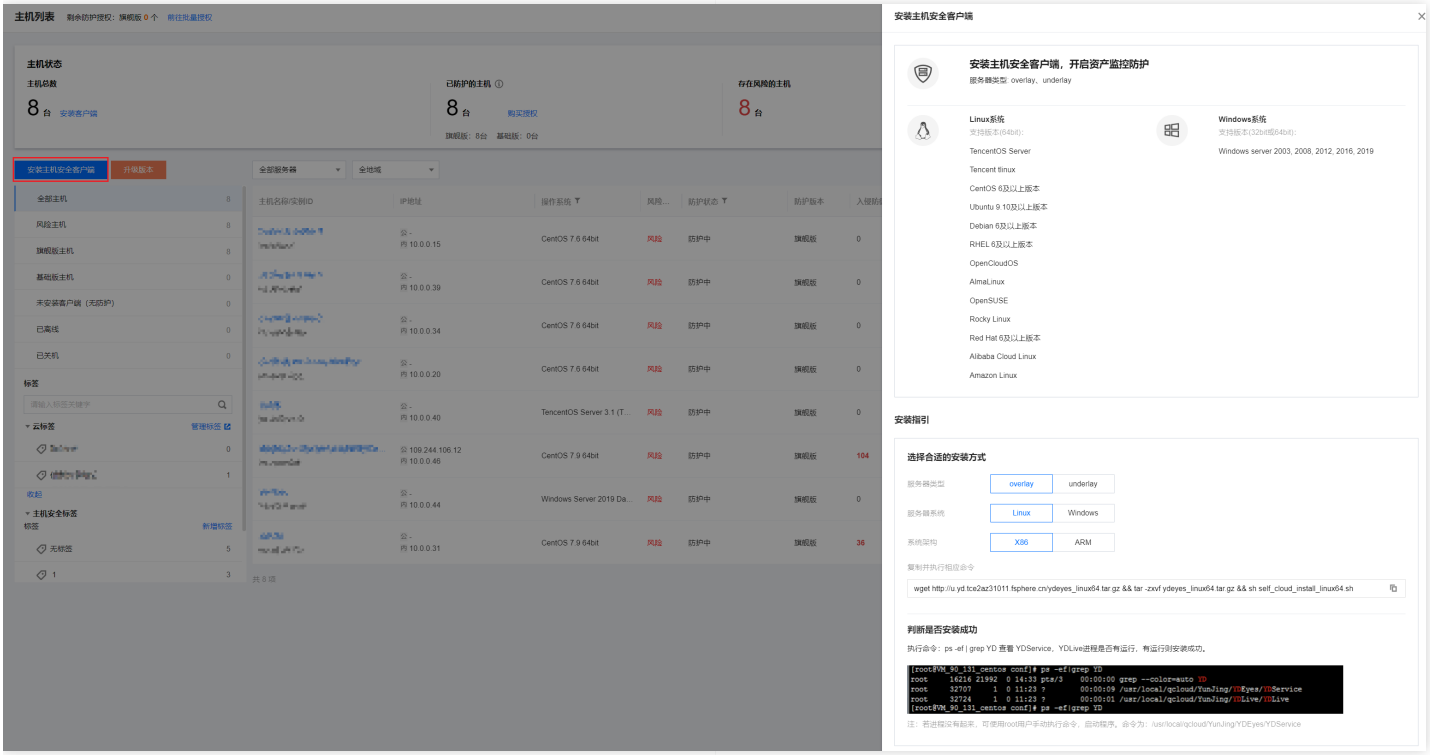
快速入门
快速入门

步骤1：安装主机安全

主机安全客户端是主机安全提供的防护插件，使用主机安全功能须先安装该插件。

1.登录租户端控制台，选择【产品管理】 > 【安全】 > 【主机安全】，进入主机安全租户端控制台。

2.在左侧导航中选择【资产管理】>【主机列表】，单击 安装主机安全客户端 可查看安装指引。



步骤2：操作主机安全

主机安全租户端支持展示主机的安全风险事件，支持对木马文件进行检测及隔离、漏洞检测、对可疑的登录行为进行检测识别及加白名单处理、支持对密码破解行为进行阻断设置、同时支持告警设置等操作，详情请参见 操作指南。

步骤3：故障排除

若主机遭遇入侵，可根据入侵类问题排查指南进行问题排查，恢复网站或系统的正常运行，详情请参见 Linux 入侵类问题排查思路 或 Windows 入侵类问题排查思路。

步骤4：卸载主机安全

若您不再需要主机安全防护，可将主机安全客户端进行卸载，主机安全共有控制台卸载与系统卸载两种方式，下面将为您详细介绍：

控制台中卸载
1.登录主机安全租户端控制台，在左侧导航栏，选择【资产管理】>【主机列表】，查看自己的云服务器是否已安装主机安全。
2.在服务器列表中，选择需要卸载主机安全客户端的服务器，单击右侧操作栏的【卸载】即可。



进入系统卸载

- Windows 系统：依照路径 C:\Program Files\QCloud\YunJing\uninst.exe ，找到 uninst.exe 文件，双击即可卸载。
- Linux 系统：输入命令： if [-w '/usr']; then /usr/local/qcloud/YunJing/uninst.sh ; else /var/lib/qcloud/YunJing/uninst.sh ; fi 即可卸载。

常见问题

防火墙拦截

建议防火墙策略放过主机安全后台服务器访问地址

overlay域名	s.yd.tce2az31011.fsphere.cn; l.yd.tce2az31011.fsphere.cn; u.yd.tce2az31011.fsphere.cn	overlay端口	5574、8080、80、9080
underlay域名	s.yd.tce2az31011.fsphere.cn; l.yd.tce2az31011.fsphere.cn; u.yd.tce2az31011.fsphere.cn	underlay端口	5574、8080、80、9080

产品架构
产品架构

下图是云镜的产品架构示意图：



云镜Agent

Agent是一个常驻在云主机操作系统中的轻量化进程，部署在需要保护的云主机上，主要功能是根据用户配置的安全策略上报服务器上存在的安全风险数据和新增的安全事件数据，同时响应用户和云镜云端防护中心的指令，实现对云主机上的安全威胁清除和恶意攻击拦截。

云镜防护引擎

基于云平台的大数据处理能力，云端防护中心接收全网Agent上报云主机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，云端防护中心是云镜的中枢神经系统，相关安全威胁的识别算法依赖于云服务商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。

用户操作控制台

提供给用户使用的网页版本控制台，主要功能包括云主机资产管理、安全威胁数据处理、安全策略配置、安全报表查看等供用户操作和查看的功能。

操作指南
安全概览

本文档将为您介绍安全概览各模块功能及操作步骤。

概述

主机安全的安全概览实时展示您的主机安全评分、待处理风险、安全防护状态、风险趋势以及主机安全的实时动态；提供帮助文档和主机安全升级服务建议，帮助您抵御黑客入侵风险及攻击威胁，保障企业主机安全。

操作指南

1.登录主机安全租户端控制台。
2.在左侧导航中，选择【安全概览】，可查看安全概览信息和相关处理操作，各模块说明如下。

安全状态

1. 在【安全状态】中，展示了您的主机安全评分和以下3类安全风险情况，并提供快捷处理入口。
   - 入侵防御：包括入侵检测模块的7个功能，即文件查杀、异常登录、密码破解、恶意请求、反弹 Shell、本地提权、高危命令，合并统计待处理风险数和受影响主机数。
   - 漏洞风险：包括 Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞，合并统计待处理风险数和受影响主机数。
   - 基线风险：只统计基线待处理风险数和受影响主机数。

   立即处理
2. 单击 ，将打开风险处理详情弹框，可以查看入侵防御、漏洞管理、基线管理具体详情。单击对应风险卡片，页面将跳转至相对应的风险处理界面。



主机安全状态划分为3个等级：

等级	体检评分	字体颜色	状态说明
优	90分 - 100分	绿色	资产安全状态较好，需继续保持，定期巡检。
中危	60分 - 89分	橙色	资产存在较多安全风险，建议您及时处理安全事件。
高危	20分 - 59分	红色	资产存在严重安全风险，请您尽快处理安全事件。

> 说明：
>
> 主机安全状态体检评分最低分数为 20分。

按安全事件分类计算扣分项，安全事件等级分类及扣分规则：

安全事件（按事件数计算）	扣分/个	叠加最大扣分
严重	木马、病毒、暴破成功。	50分
高危	高危漏洞、高危基线、异地登录、本地提权、反弹 Shell、高危命令。	10分
中危	中危漏洞、中危基线。	3分
低危	低危漏洞、低危基线。	2分
其他	基础版（非防护状态）。	1分

安全防护

1. 在【安全防护】中，展示主机安全应对入侵攻击提供的（预防-防御-检测-响应）全流程解决方案，并细化展示各阶段所需的安全防护项。若各防护项均开启，可直观了解您当前主机安全的情况，并提供安全风险快捷处理入口。



防护详情

在【防护详情】中，可查看目前主机总数、在线主机总数量、未防护主机数、已防护主机数、专业版或旗舰版主机数、基础版主机数，同时提供资产更新时间、病毒库更新时间、漏洞库更新时间以及安全引擎防护等信息。

> 说明：
>
> 由于基础版主机防护程度相对较弱，“防护主机数”仅包含专业版或旗舰版主机。

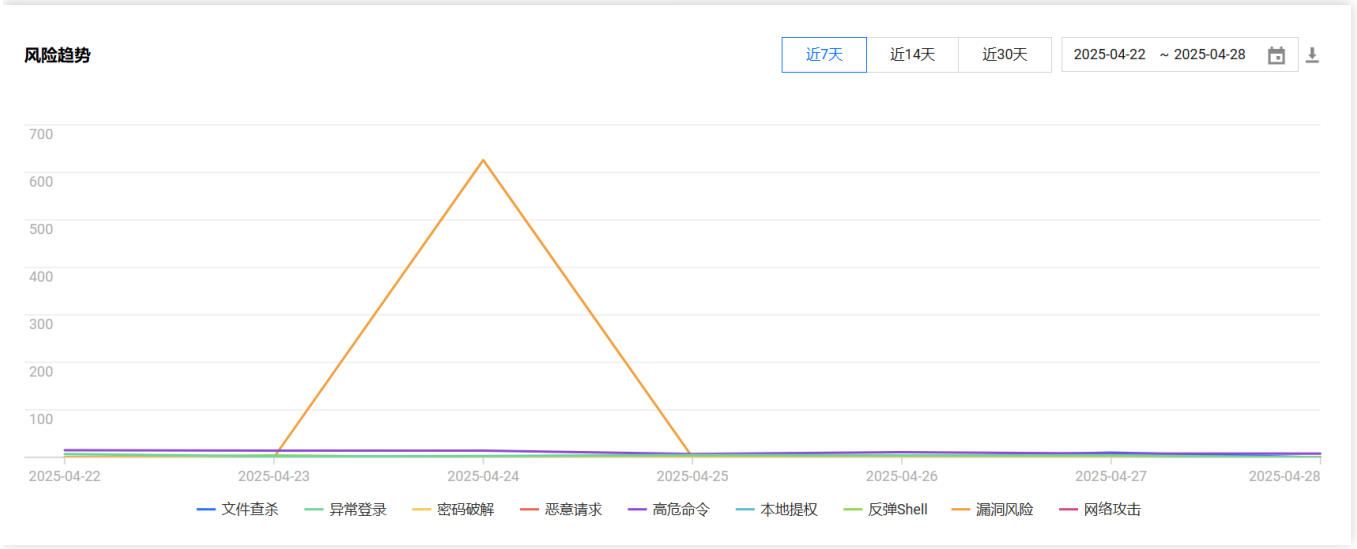


风险趋势

风险趋势功能通过折线图，为您展示近7天、近14天或近30天的安全风险和威胁发生趋势，并且支持按时间段筛选查看。将

鼠标在趋势图中悬停，将显示该日期文件查杀、密码破解、异常登录、漏洞风险、网络攻击等安全事件数。单击右上角，支持将所选中日期的安全事件数下载至本地。

> 说明：
>
> 数据来源为当日新增待处理事件数，每小时更新一次，历史事件数将保留，不再变更。



实时动态

实时动态功能按照时间倒序实时展示发现的主机风险及威胁事件。单击蓝色字段的主机 IP，将跳转至【主机详情】中，可查看该主机安全各类风险情况；单击【查看详情】，将跳转至相应事件处理页面。

实时动态

告警行为	威胁等级	发现时间	操作
异常登录 主机10.0.0.46被113.108.77.63异常登录	可疑	2024-08-22 …	查看详情
异常登录 主机10.0.0.46被119.147.10.183异常登录	可疑	2024-08-16 …	查看详情
异常登录 主机10.0.0.46被113.108.77.62异常登录	可疑	2024-08-15 …	查看详情
异常登录 主机10.0.0.46被113.108.77.62异常登录	可疑	2024-08-14 …	查看详情
异常登录 主机10.0.0.46被119.147.10.186异常登录	可疑	2024-08-08 …	查看详情

共 30 条

版权所有：TCloudFinanceZone

资产概览

本文档将为您介绍资产概览各功能模块及操作。

概述

资产概览是从资产维度对主机及关键资产指纹数据进行统计盘点、可视化呈现，便于用户了解主机资产情况。

前提条件

仅专业版或旗舰版主机支持资产指纹数据采集和同步，基础版或未防护主机则不支持。

背景信息

各版本支持采集的资产指纹如下：

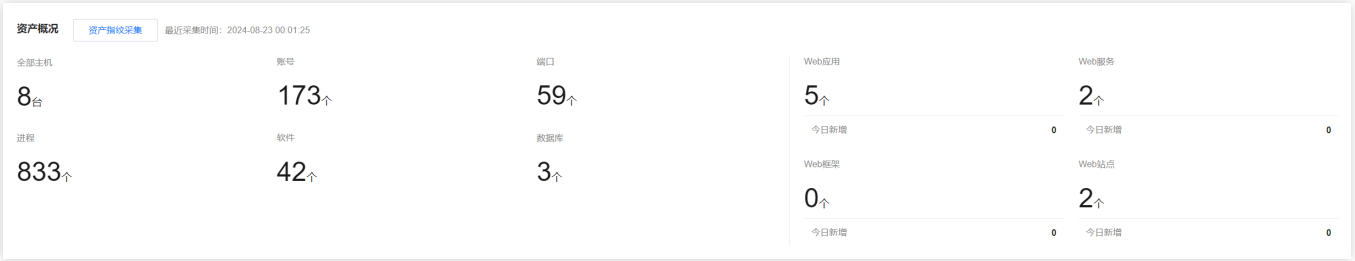
主机安全防护版本	采集的资产指纹项
专业版	10项：资源监控、账号、端口、进程、软件应用、数据库、Web应用、Web服务、Web框架、Web站点
旗舰版	16项：资源监控、账号、端口、进程、软件应用、数据库、Web应用、Web服务、Web框架、Web站点、Jar包、启动服务、计划任务、环境变量、内核模块

> 说明：
>
> 资产指纹数据每隔8小时自动采集一次，支持手动采集。

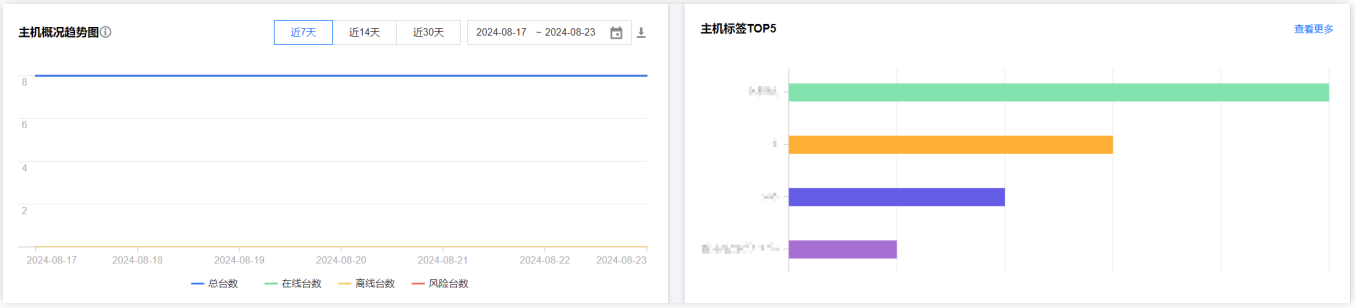
概览

登录主机安全租户端控制台，在左侧导航栏，选择【资产管理】>【概览】，进入概览页面。

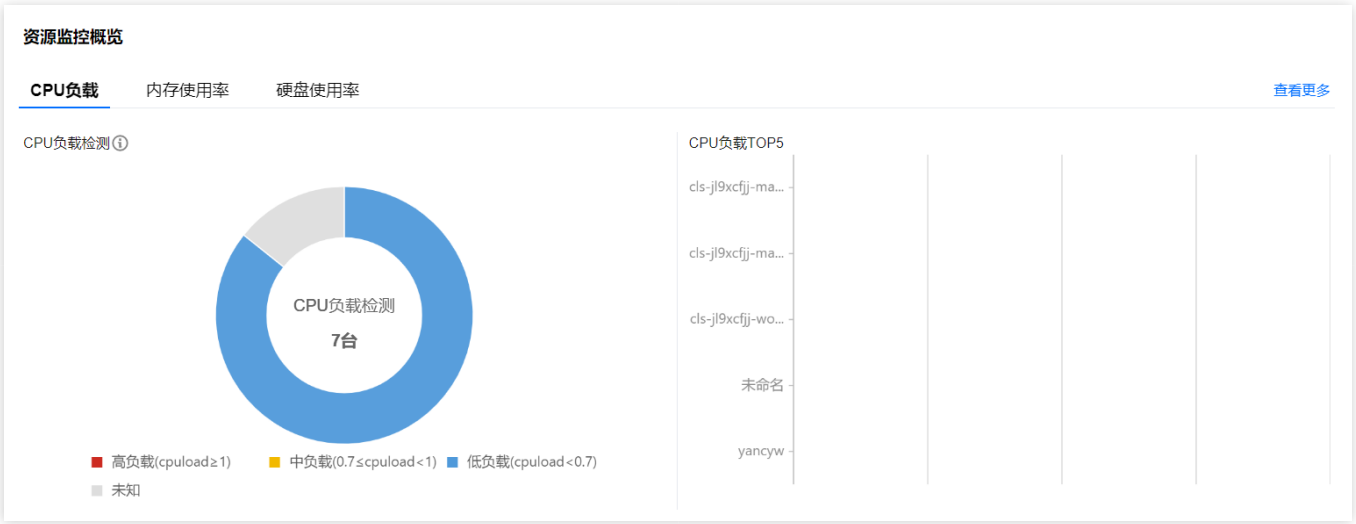
1. 资产概况面板，可查看全部主机及各项资产指纹的统计情况。



2. 主机概况趋势图（总台数、在线台数、离线台数、风险台数）支持最长不超过近3个月时间段的查询，支持下载导出；主机标签 TOP 5，可查看所有主机中使用最多的前5个标签。

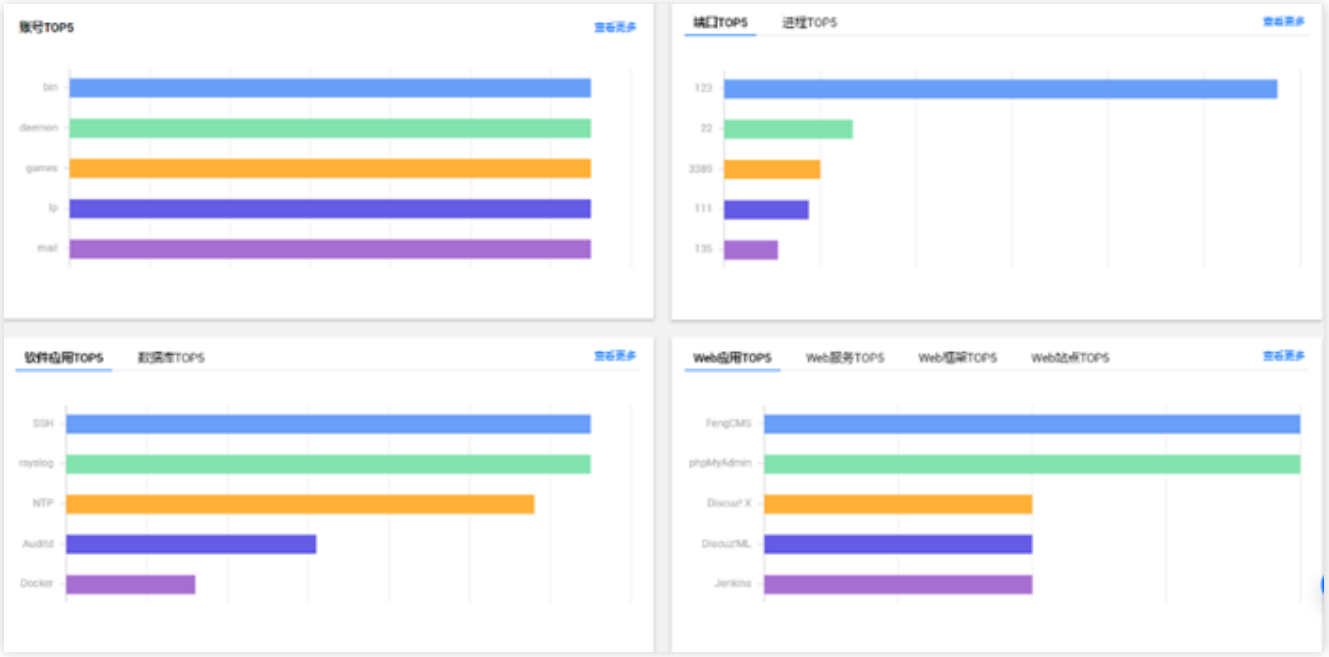


3. 资源监控概览，可查看CPU负载、内存使用率、硬盘使用率的分布情况及相应TOP 5。



> 说明：
>
> 关于CPU负载，目前仅支持获取Linux系统的服务器CPU负载，Windows系统暂认定为未知。

4. 查看账号TOP 5、端口TOP5、进程TOP 5、软件应用TOP 5、数据库TOP5、Web应用TOP 5、Web服务TOP5、Web框架TOP 5、Web站点TOP5。



> 说明：
>
> 各资产指纹TOP 5是根据指纹（账号、端口、进程、软件应用、数据库、Web应用、Web服务、Web框架、Web站点）所属服务器数量降序排列后，取排名前5项的数据。

主机列表

本文档将为您介绍主机列表各功能模块及操作。

概述

主机列表可查看目前已接入主机安全的所有服务器的信息，帮助您全面了解资产的安全状态。

相关限制

可接入主机安全的主机范围：

主机类型	Linux系统	Windows系统
overlay主机	支持架构：x86、arm	支持架构：x86
underlay主机	支持架构：x86、arm	支持架构：x86

操作步骤

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【资产管理】>【主机列表】。
2. 在主机列表页面，可以查询资产状态、安装/卸载主机安全客户端等操作。

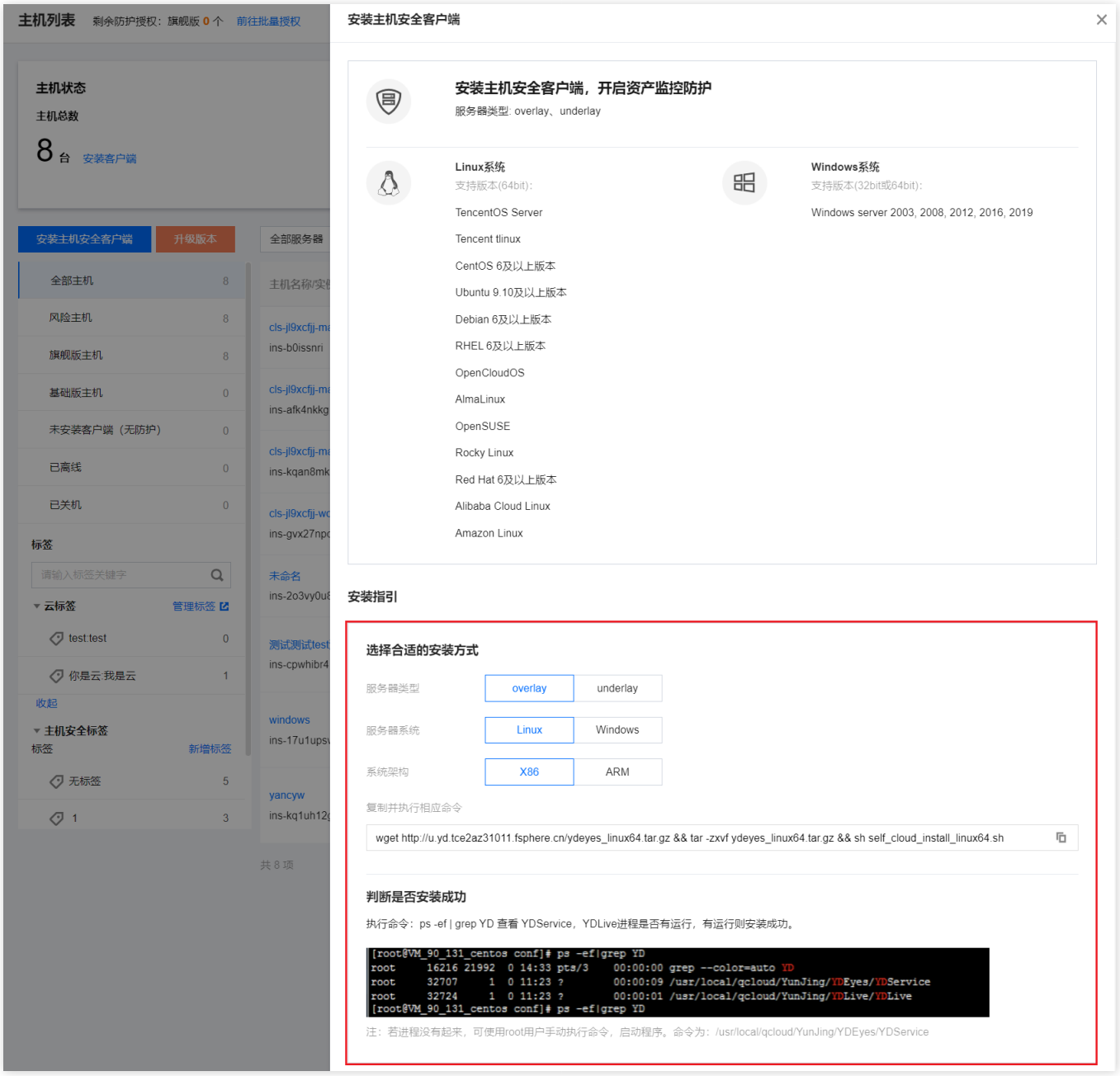
主机状态

在【主机状态】中，可查看目前主机总数、已防护的主机（由于基础版主机防护程度相对较弱，此处仅包含专业版或旗舰版主机数）、存在风险的主机数、无防护的主机数和授权即将到期的主机数。



安装主机安全客户端

单击【安装主机安全客户端】展示主机安全客户端的安装指引，选择服务器类型和操作系统进行正确安装，可接入overlay、underlay服务器，安装完成后，须验证是否安装成功。


主机列表
剩余防护授权：旗舰版 0 个
前往批量授权
主机状态
主机总数
8 台
安装客户端
安装主机安全客户端
升级版本
全部服务器
全部主机 8
风险主机 8
旗舰版主机 8
基础版主机 0
未安装客户端（无防护） 0
已离线 0
已关机 0
标签
请输入标签关键字
云标签
管理标签
test:test 0
你是云:我是云 1
收起
主机安全标签
标签
新增标签
无标签 5
1 3
共 8 项
安装主机安全客户端
安装主机安全客户端，开启资产监控防护
服务器类型: overlay、underlay
Linux系统
支持版本(64bit):
TencentOS Server
Tencent tlinux
CentOS 6及以上版本
Ubuntu 9.10及以上版本
Debian 6及以上版本
RHEL 6及以上版本
OpenCloudOS
AlmaLinux
OpenSUSE
Rocky Linux
Red Hat 6及以上版本
Alibaba Cloud Linux
Amazon Linux
Windows系统
支持版本(32bit或64bit):
Windows server 2003, 2008, 2012, 2016, 2019
安装指引
选择合适的安装方式
服务器类型
overlay
underlay
服务器系统
Linux
Windows
系统架构
X86
ARM
复制并执行相应命令
wget http://u.yd.tce2az31011.fsphere.cn/ydeyes_linux64.tar.gz && tar -zxvf ydeyes_linux64.tar.gz && sh self_cloud_install_linux64.sh
判断是否安装成功
执行命令：ps -ef | grep YD 查看 YDService，YDLive进程是否有运行，有运行则安装成功。
[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
注：若进程没有起来，可使用root用户手动执行命令，启动程序。命令为：/usr/local/qcloud/YunJing/YDEyes/YDService

">

升级版本

单击【升级版本】将跳转至【授权管理】页，您可为基础版主机绑定专业版或旗舰版授权，即可开启专业版或旗舰版防护。

筛选导出

- 支持筛选服务器专区、地域、主机状态（全部主机、风险主机、旗舰版或专业版主机、基础版主机、未安装客户端、已离线、已关机）、标签及服务器 IP 或名称搜索。

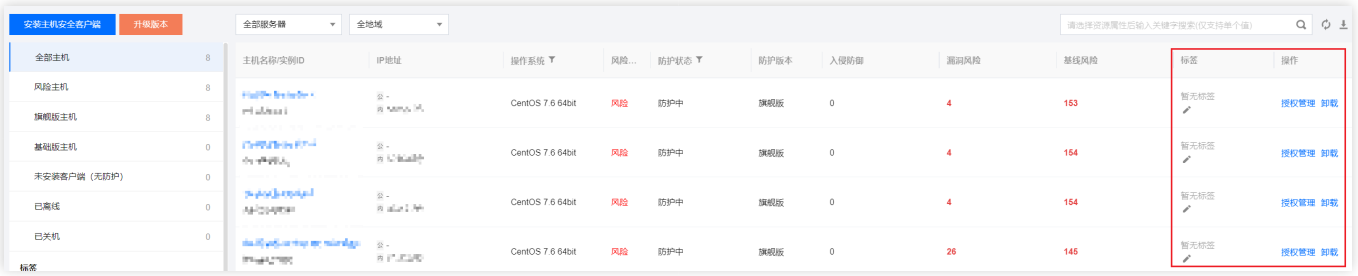


- 单击 导出按钮，可对当前筛选出来的机器进行数据导出。



列表操作

- 支持设置标签、关联标签。
- 支持卸载主机安全客户端、授权管理，单击【授权管理】，将跳转至授权管理页，支持授权绑定、解绑、扩容、缩容等操作。



- 单击入侵防御、漏洞风险、基线风险的【数值】可跳转查看风险详情。



资产指纹

本文档将为您介绍如何查看资产指纹统计数据。

概述

资产指纹数据采集，可帮助您快速了解资产的概况和运行状态。

相关限制

仅专业版或旗舰版主机才可采集资产指纹数据。
各版本支持采集的资产指纹如下：

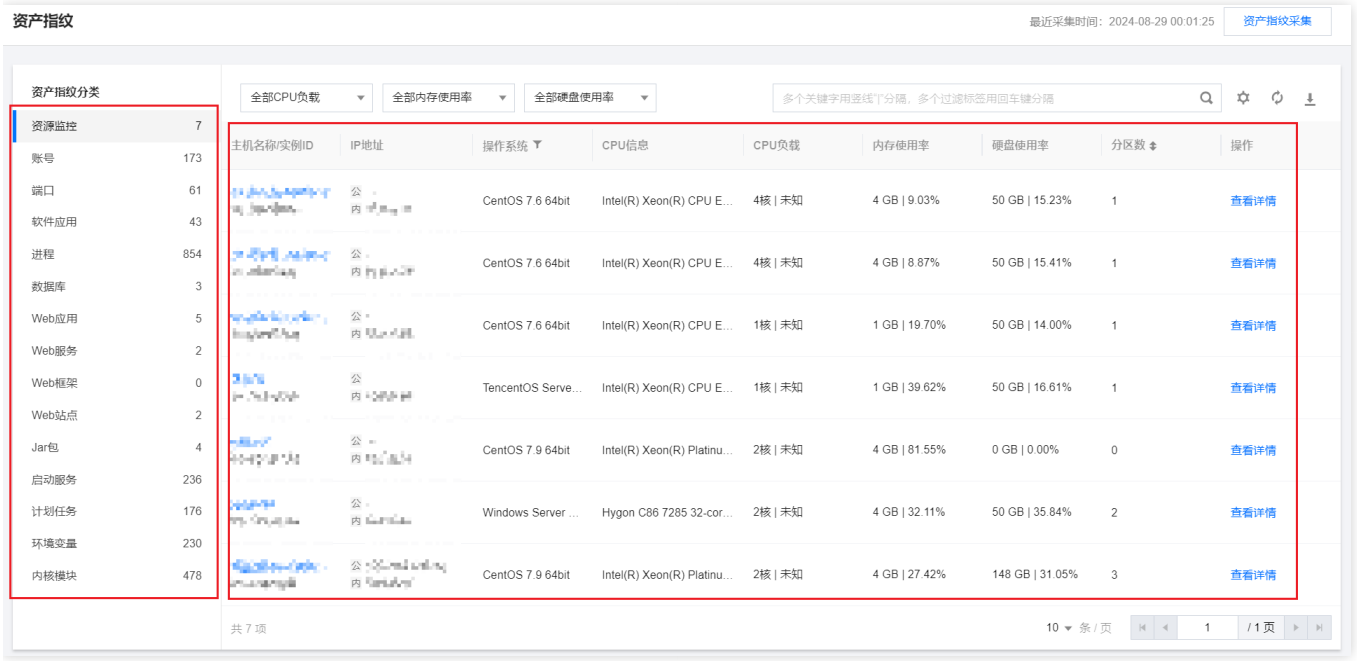
主机安全防护版本	采集的资产指纹项
专业版	10项：资源监控、账号、端口、进程、软件应用、数据库、Web应用、Web服务、Web框架、Web站点
旗舰版	16项：资源监控、账号、端口、进程、软件应用、数据库、Web应用、Web服务、Web框架、Web站点、Jar包、启动服务、计划任务、环境变量、内核模块

> 说明：
>
> 资产指纹数据每隔8小时自动采集一次，支持手动采集。

操作步骤

1. 登录主机安全租户端控制台，在左侧导航栏，选择【资产管理】 >【资产指纹】。
2. 在【资产指纹】中，展示了资产指纹分类列表，包括各资产指纹项及其对应服务器数量。在左侧资产指纹分类列表中选中一项后，右侧将展示该指纹详情，支持对指纹数据的查询和导出。

   > 说明：
   >
   > 各资产指纹搜索功能均支持模糊搜索。

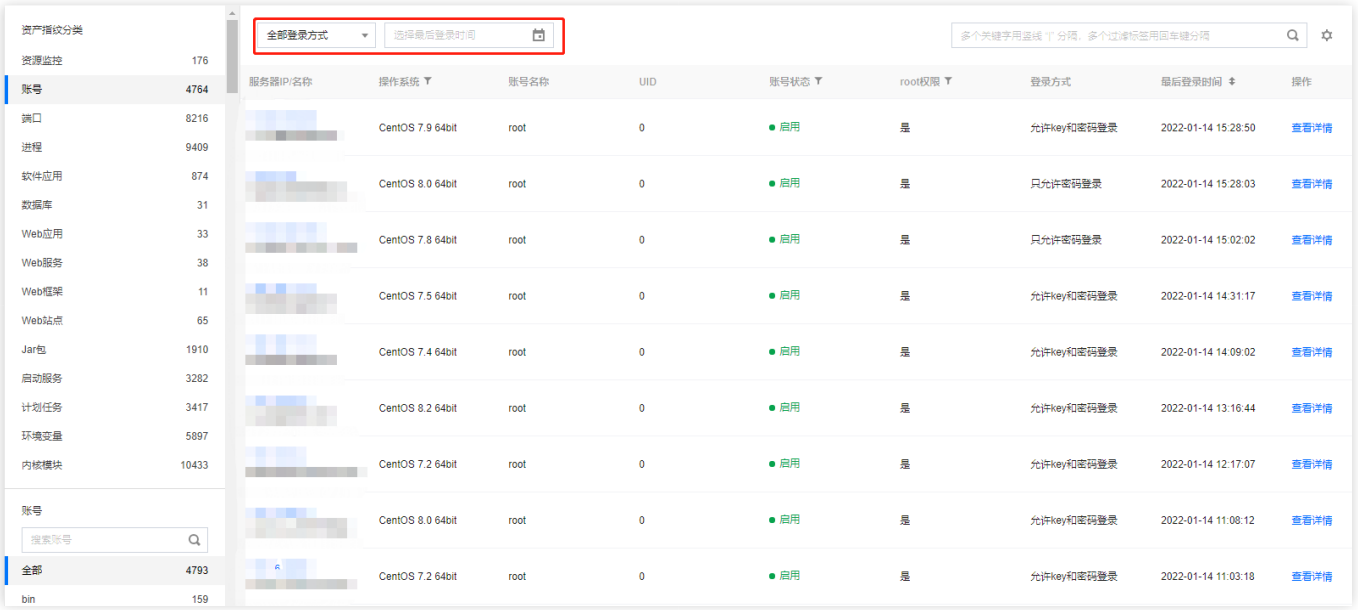


资产指纹分类说明：

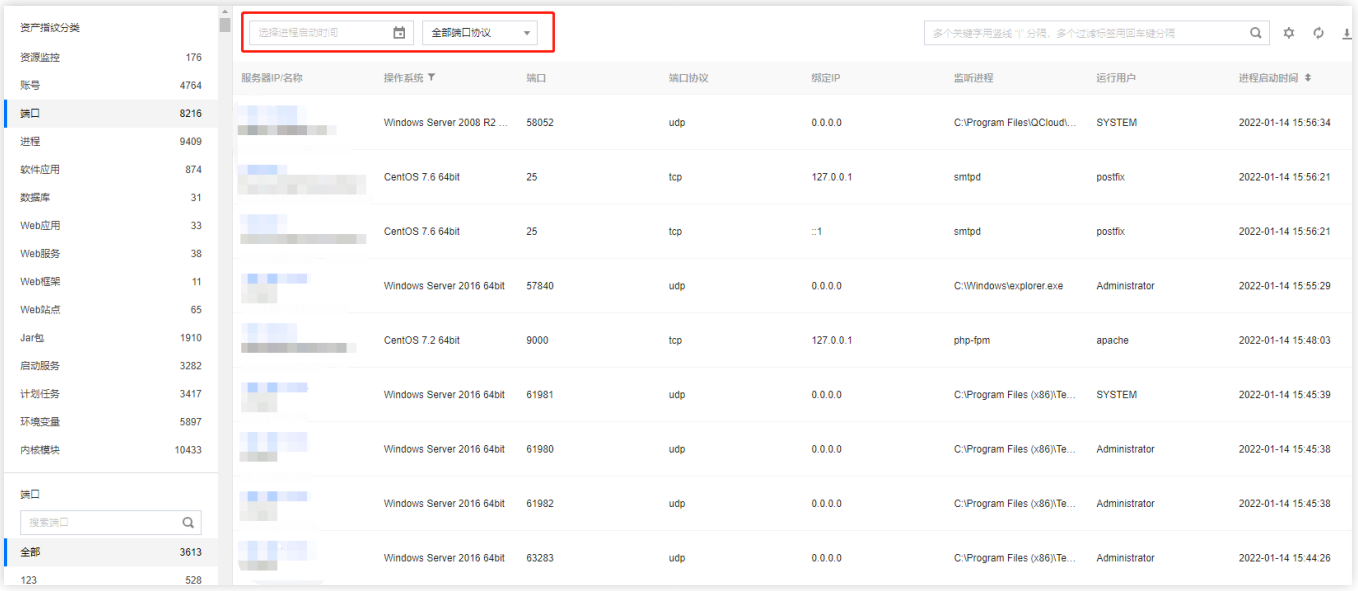
- 资源监控：对服务器CPU负载、内存使用、硬盘使用进行数据采集。



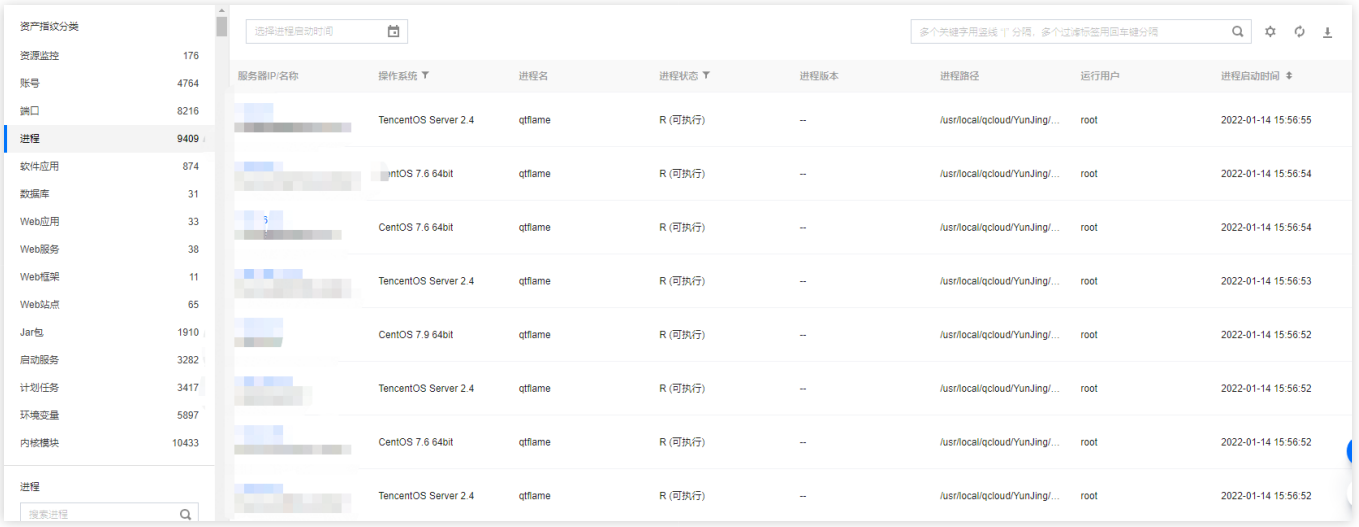
- 账号：对服务器所有账号进行采集。



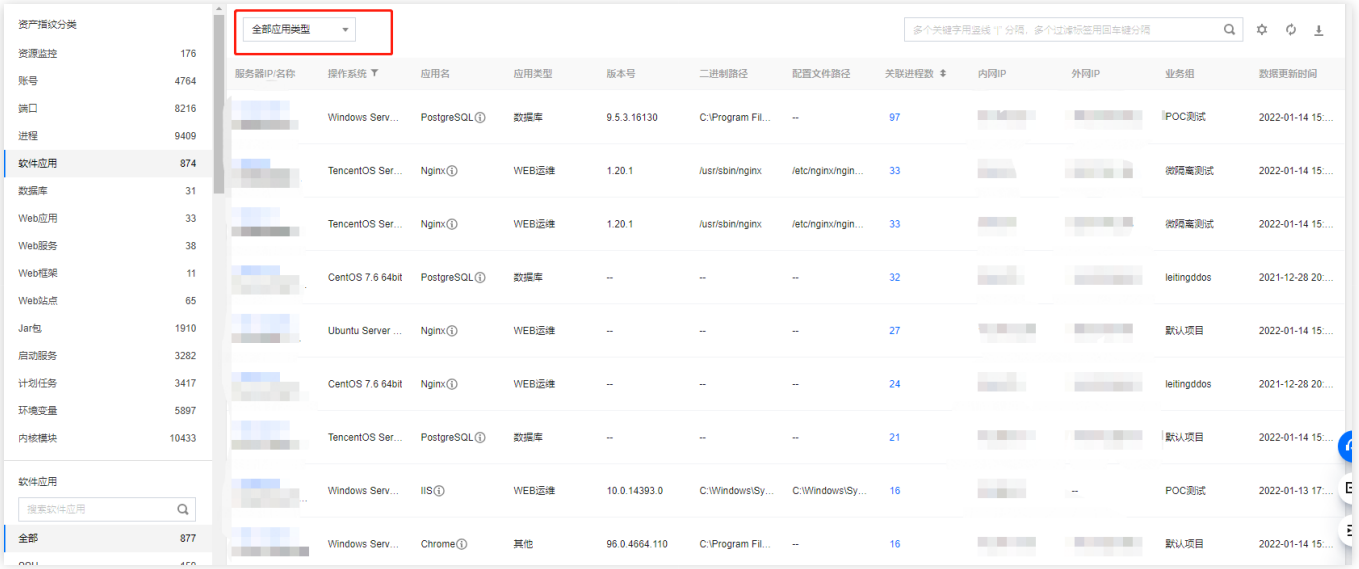
- 端口：对服务器所有已使用端口进行采集。



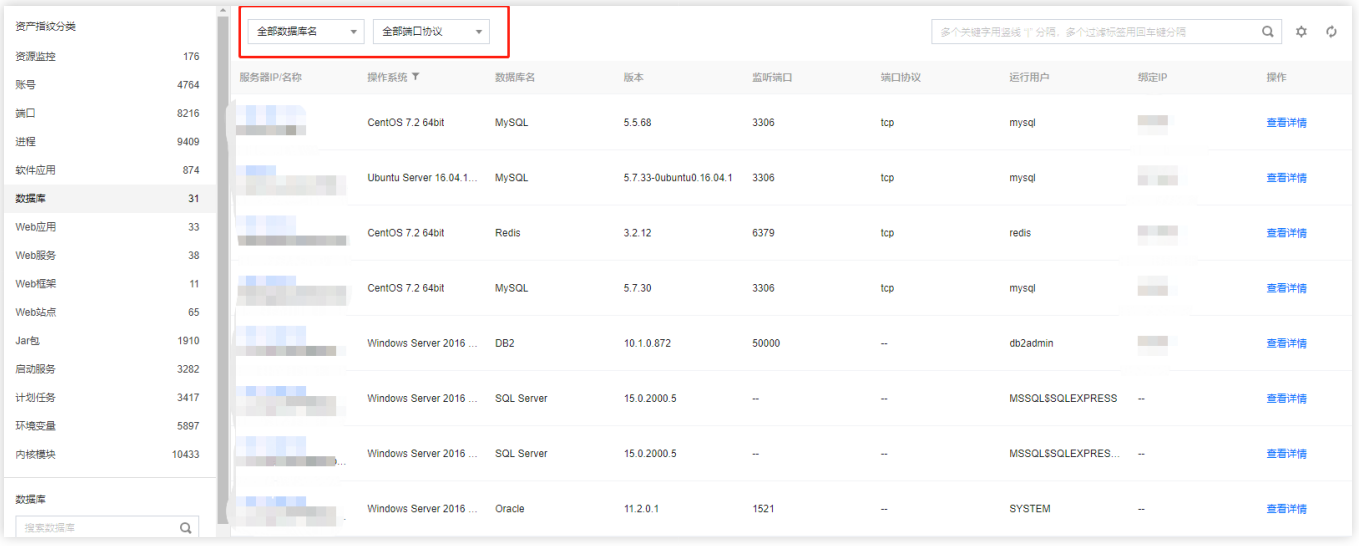
- 进程：对服务器的所有运行进程进行采集。



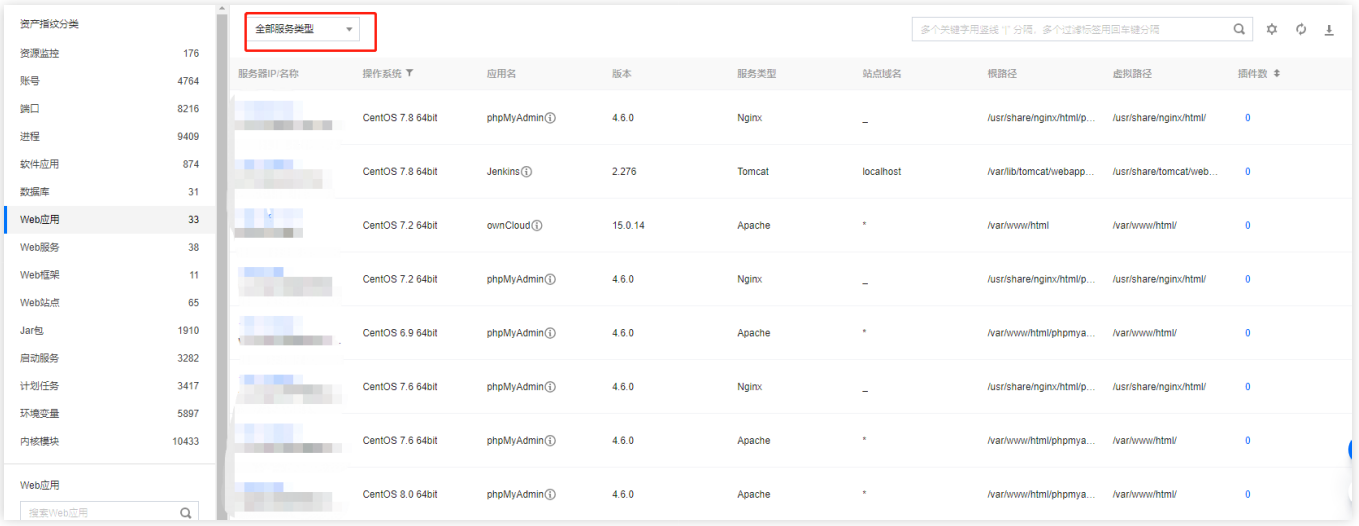
- 软件应用：对服务器所有运行中的软件应用进行采集。



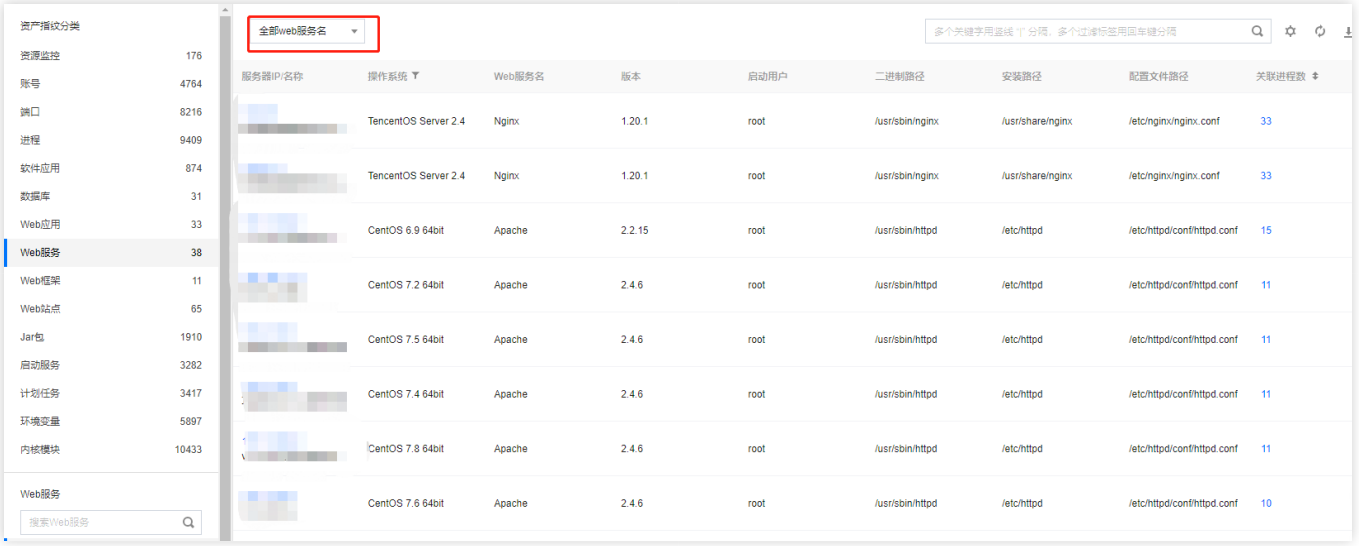
- 数据库：对服务器所有运行的数据库进行采集。



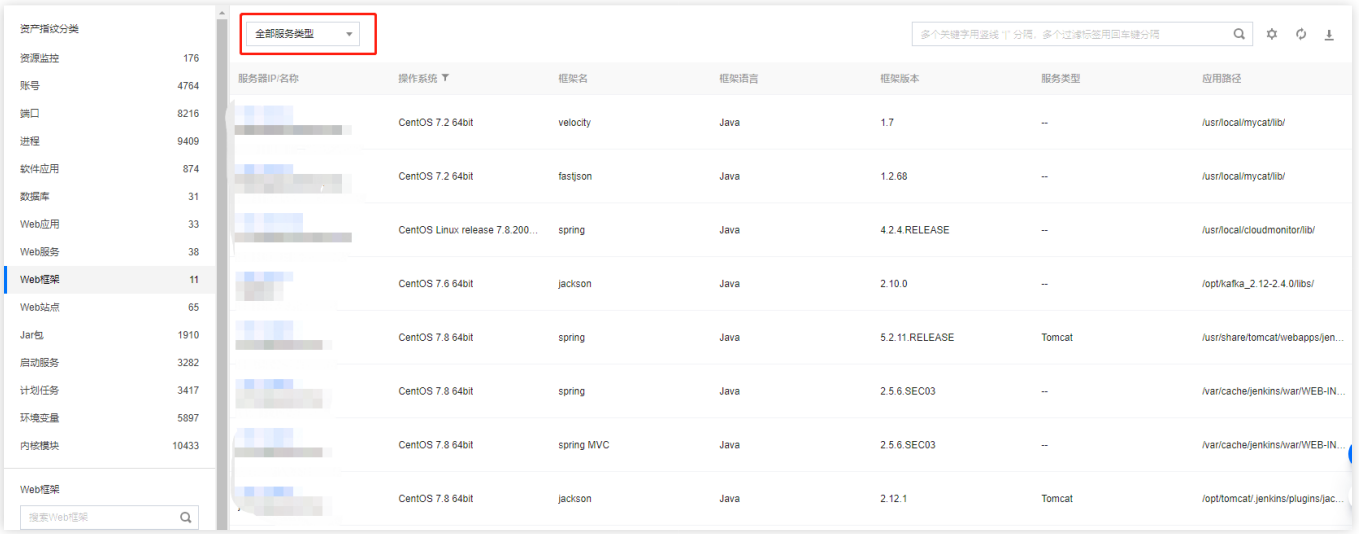
- Web 应用：对服务器所有运行的 Web 应用进行采集。



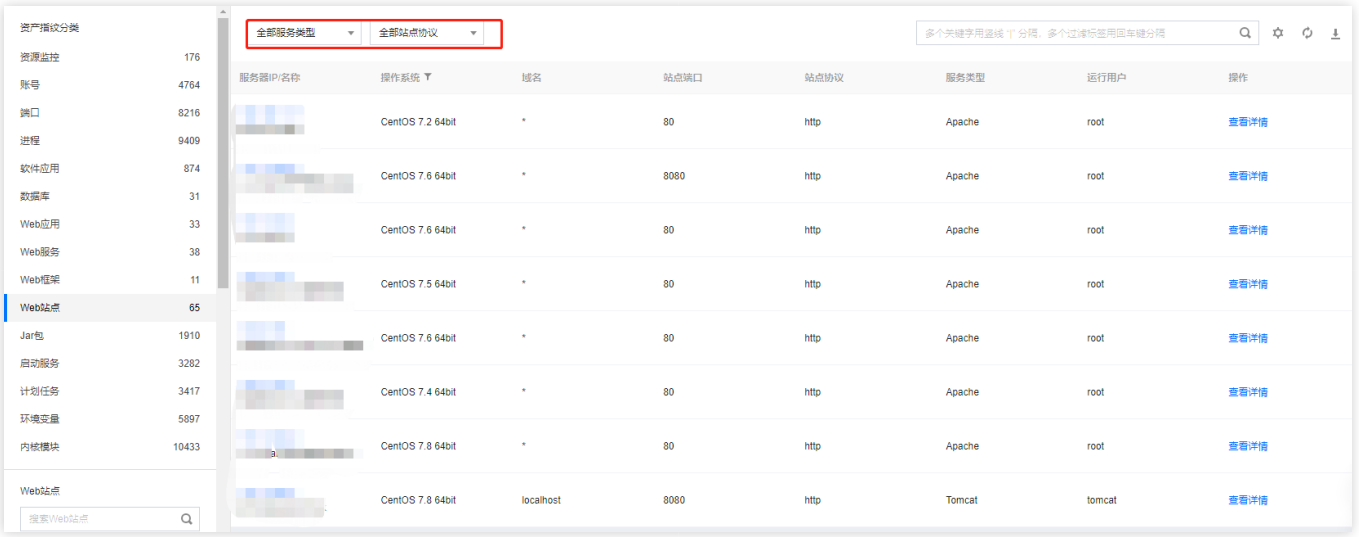
- Web 服务：对服务器所有运行的 Web 服务进行采集。



- Web 框架：对服务器所有应用的 Web 框架进行采集。



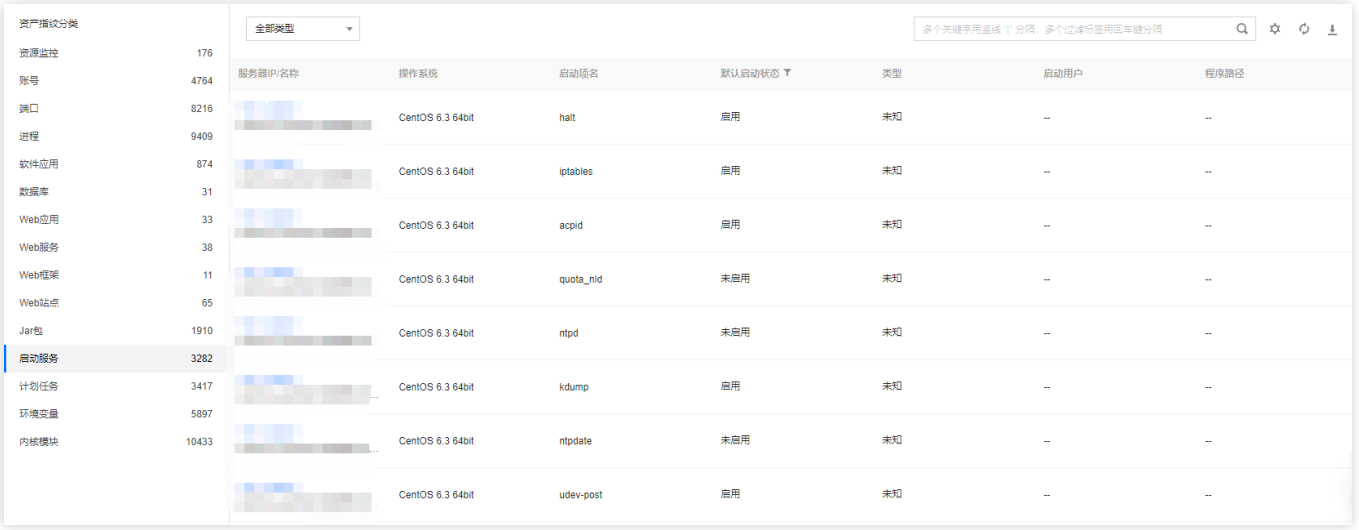
- Web站点：对服务器所有部署的Web站点进行采集。



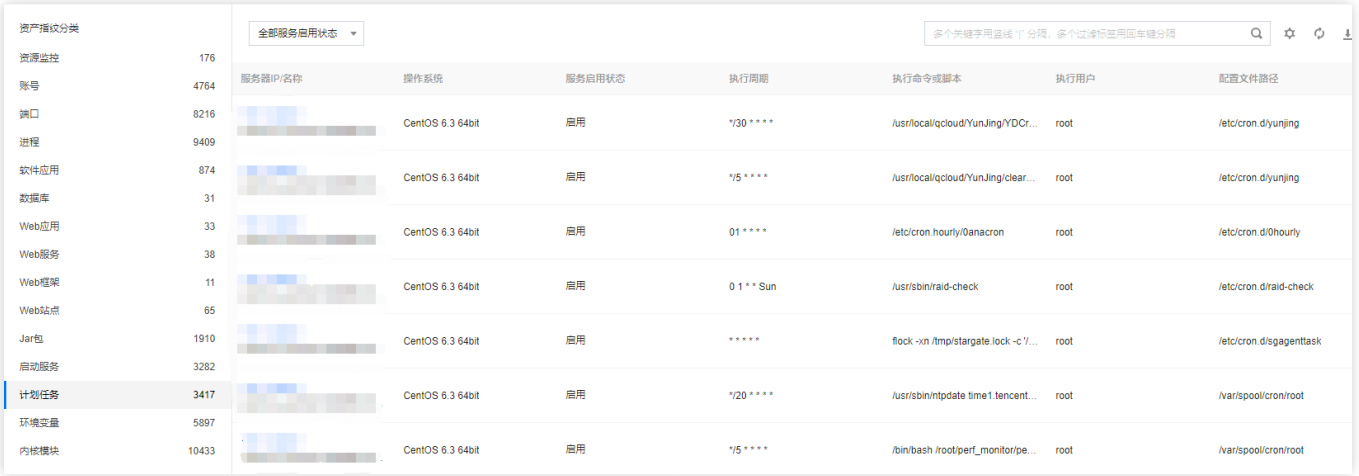
- Jar 包：对服务器所有的 Jar 包进行采集。



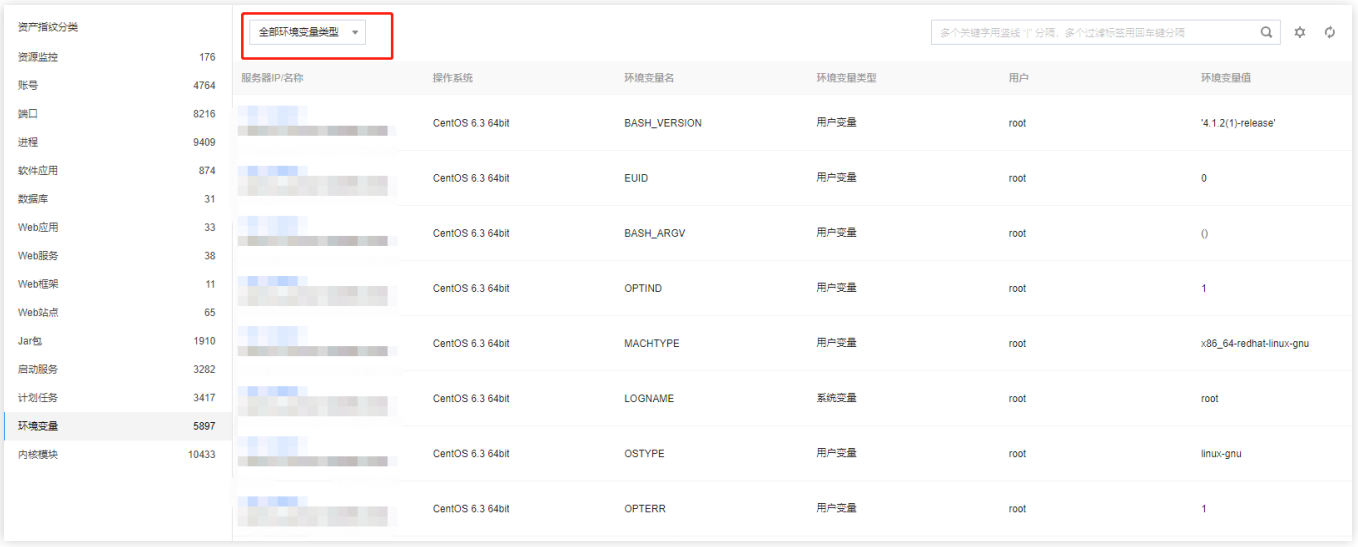
- 启动服务：对服务器所有的启动服务进行采集。



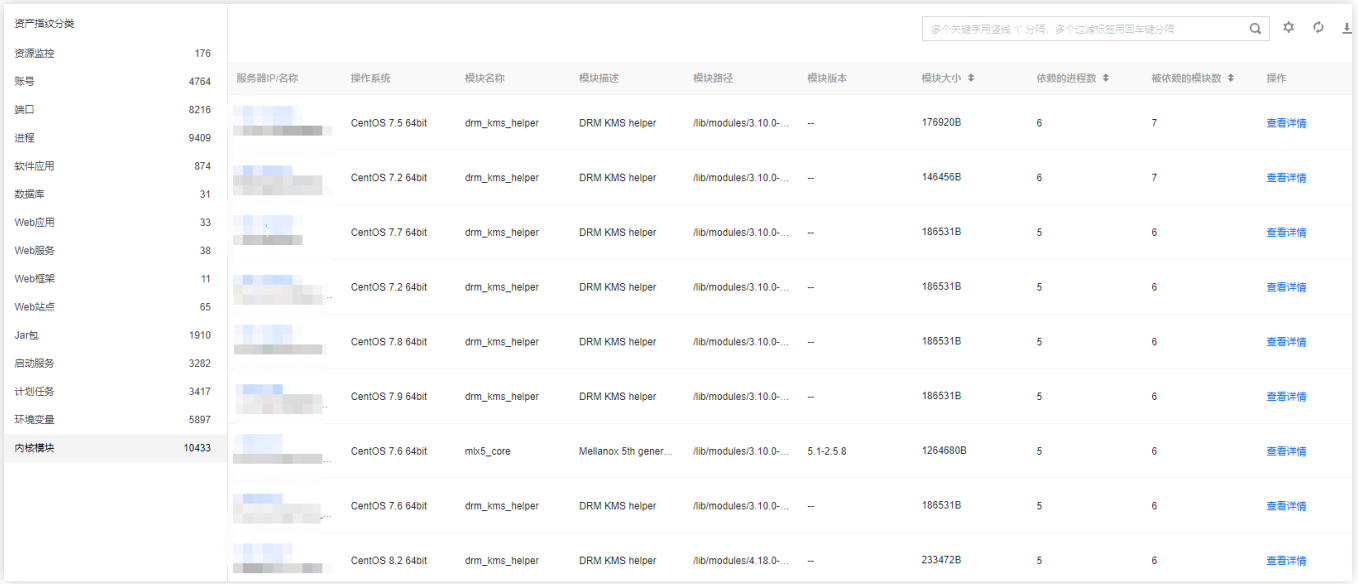
- 计划任务：对服务器所有的计划任务进行采集。



- 环境变量：对服务器所有的环境变量进行采集。



- 内核模块：对服务器的内核模块进行采集。



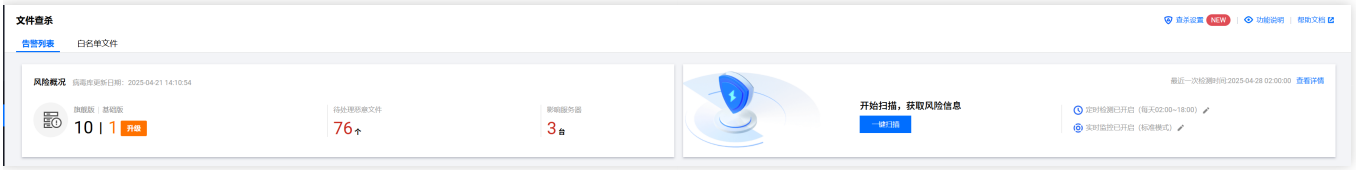
文件查杀

本文档将指导您如何在主机安全控制台对木马文件进行操作处理。

文件查杀设置

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵防御】>【文件查杀】。
2. 在文件查杀中，单击右上角处【查杀设置】，右侧弹出查杀设置页面，可对查杀模式进行设置。

> 说明：
>
> - 常见的木马文件检测有以下两种：
> - Webshell 检测：提供常用的 Web 网站类脚本木马后门检测，包含 ASP/PHP/JSP/Python 等脚本语言。
> - 二进制检测：提供对二进制可执行类的病毒木马检测，例如 DDoS 木马、远控、挖矿类软件等，文件类型包括 exe、dll、bin 等，并告警用户。



3. 在【查杀设置】中，支持定时扫描、实时监控、自动隔离设置。

- 定时扫描：单击开启【定时扫描】，设置检测模式、周期和检测范围后，单击【保存】，可定期扫描主机木马病毒文件，增强安全性。



字段说明：

- 检测模式：包括快速检测模式和全盘检测模式，可对运行中进程、关键目录、驱动加载等进行检测。其中全盘检测的时长与服务器磁盘文件数量相关，推荐选择4小时以上，避免出现扫描不完整或超时情况。
- 检测周期：可选择每天、每隔3天或每隔7天检测周期。

    - 检测范围：支持选择全部专业版或旗舰版服务器、自选服务器。
- 实时监控：单击开启【实时监控】，并选择监控模式后，单击**【保存】**，可实时监控 Web 目录、系统关键目录，查杀木马病毒文件。



字段说明：

- 监控模式：
    - 标准：监控并扫描检测常见目录下增量文件。
    - 深度：监控并扫描检测所有目录下增量文件。

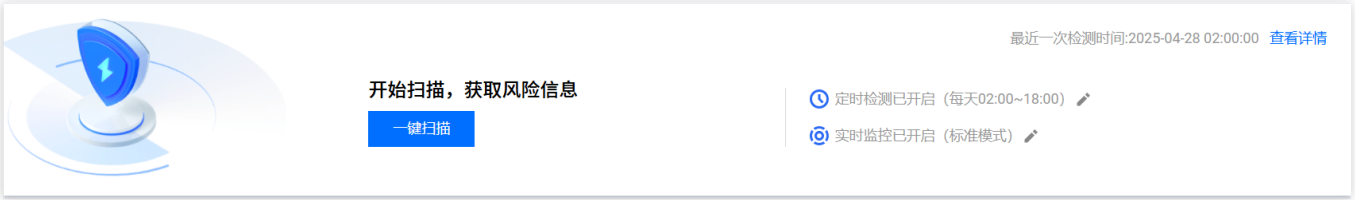
- 自动隔离：单击开启【自动隔离】>【保存】，将自动隔离检测出的恶意文件，部分恶意文件仍需用户手动确认隔离，建议检查文件查杀列表中所有安全事件，确保已全部处理。

> 说明：
>
> 若出现误隔离，请在已隔离列表中对文件进行恢复。开启或关闭自动隔离，均需要进行配置，实际生效存在几分钟延迟。



检测设置概览

1. 登录主机安全租户端控制台 ，在左侧导航栏中，选择【入侵防御】>【文件查杀】。
2. 在文件查杀页面，单击【一键扫描】，开始设置手动检测模式。



3. 在【一键检测设置】弹窗中，确定检测模式、引擎模式、主机范围后，还可配置超时时间（检测可能会因为文件、目录过多等原因导致耗时较长）。



4. 单击【开始检测】后将按检测设置进行检测，单击【查看详情】可查看检测详情。





检测详情列表字段说明：

- 影响服务器 ：服务器的 IP 及名称。
- 操作系统 ：服务器的操作系统。
- 检测状态：检测完成、检测中、检测失败（原因：可能是检测超时失败，建议增加超时时间后重新检测；可能是客户端已离线，建议重启或重新安装客户端后重新检测）。
- 待处理风险：服务器检出待处理的风险文件数量。
- 检测开始时间：此次检测开始的时间。
- 检测结束时间：服务器检测结束的时间。
- 操作：
  - 重新检测：若想对检测状态处于检测完成、检测停止和检测失败的服务器再次检测，您可以单击【重新检测】。
  - 停止检测：若想对检测状态处于检测中的服务器停止检测，您可以单击【停止检测】，服务器将不会被检测，可能存在的风险，请谨慎操作。
- 查看详情：若想查看目标服务器的检测结果，您可以单击【查看详情】。

查看告警列表

1. 登录主机安全租户端控制台 ，在左侧导航栏中，选择【入侵防御】>【文件查杀】。
2. 在文件查杀页面，可查看当前受防护的服务器中木马文件的检测情况，如下图所示：



告警列表字段说明：

- 主机名称/实例ID：被检测的服务器名称和实例ID。
- IP地址 ：被检测的服务器IP地址。
- 路径：风险文件路径，单击 复制文件路径、单击 下载风险文件样本。
- 病毒名/检出引擎：入侵风险文件的病毒名。
- 首次发现时间：首次检出该风险文件的时间。
- 最近检测时间：最近一次检出该风险文件的时间。
- 处理状态：风险文件的处理状态，待处理状态的事件会提示最近一次检测该文件时，文件和进程的存在情况。
- 操作：
  - 详情：可查看恶意文件详情。
  - 隔离：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。（注意：windows系统下，若该文件正在运行中，会导致隔离失败），支持隔离并杀掉该文件相关进程，建议勾选。
  - 标记已处理：建议您参照告警详情中的“修复建议”进行处理，处理后可将该告警标记为已处理。
  - 加入白名单：若您确认该进程运行属于正常行为，可将该进程添加白名单放行规则，后续再出现该进程运行，将直接放行不再拦截/告警。
  - 忽略：仅将本次告警进行忽略，若再有相同情况发生依然会进行告警。
  - 删除记录：删除该告警记录，控制台将不再显示，无法恢复记录，请慎重操作。

常见问题

木马文件为什么隔离失败？

木马文件隔离失败，一般是由于木马文件对抗安全软件导致的，建议先自行删除服务器中的告警文件。若仍无法处理，请联系技术支持工程师进行处理，Windows 系统也可尝试使用电脑管家进行查杀。

后续步骤

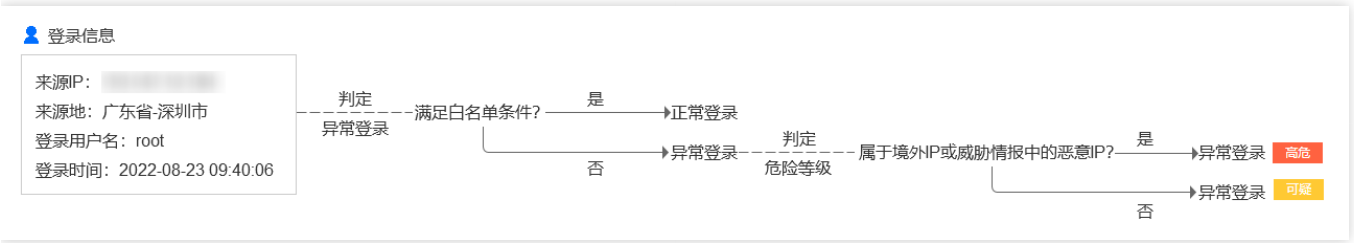
- Linux 入侵类问题排查指南，请参见 Linux 入侵类问题排查思路。
- Windows 入侵类问题排查指南，请参见 Windows 入侵类问题排查思路。

异常登录

本文将为您介绍异常登录的功能和操作。

概述

当检测到存在不满足白名单（常用来源 IP、常用用户名、常用登录地、常用登录时间）的服务器登录行为，将产生异常登录告警。若异常登录来源 IP 属于威胁情报中的恶意 IP，将被标记为“高危”，反之则标记为“可疑”。



限制说明

- 已安装主机安全客户端的主机（客户端在线），均会实时监控异常登录行为。
- 主机安全控制台仅保留近6个月的异常登录事件，过期的事件数据将不再展示。

操作指南

1. 登录主机安全租户端控制台。
2. 左侧导航中，选择【入侵防御】>【 异常登录】，各功能说明如下。

告警列表

在告警列表页面中，可查看并处理主机安全监测到的异常登录风险。



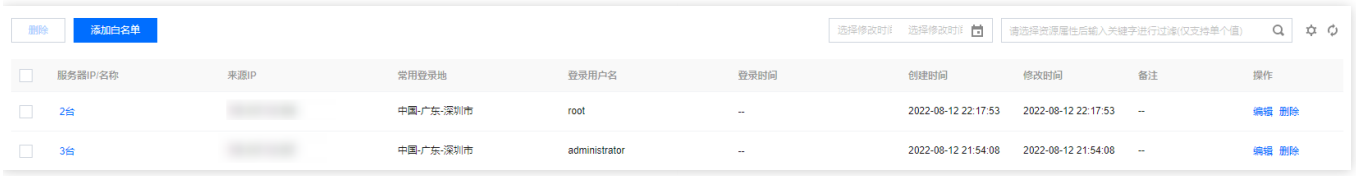
字段说明：

- 主机名称/实例ID：被异常登录的服务器。

- IP地址：被异常登录的服务器IP地址。
- 来源 IP：登录来源 IP，一般是公司网络出口 IP 或网络代理 IP。
- 来源地：登录来源 IP 所在的地域。
- 登录用户名：成功登录服务器时使用的登录用户名。
- 登录时间：成功登录服务器的时间（服务器上的时区时间）。
- 危险等级：可疑/高危。
- 状态
  - 异常登录：本次登录存在异常地域、异常用户名、异常登录时间或异常来源 IP 登录。
  - 已加入白名单：登录来源 IP 已被添加至白名单（登录源 IP、登录用户名、登录时间、常用登录地、生效范围的组合构成白名单判定规则）。
  - 已处理：用户已手动处理，并将该事件标记为已处理。
  - 已忽略：用户已忽略本次告警事件。
- 操作
  - 处理
    - 标记已处理：若您已人工对该风险事件进行处理，可将事件标记为已处理。
    - 加入白名单：加入白名单操作后，当再次发生相同事件时将不再进行告警，请谨慎操作。
    - 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。
    - 删除记录：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。

白名单管理

在白名单管理页面中，可增/删/改/查异常登录的白名单。



字段说明：

- 服务器 IP/名称：该白名单生效的服务器。
- 来源 IP：加白名单的登录来源 IP。
- 常用登录地：加白名单的登录地。
- 登录用户名：加白名单的用户名。
- 登录时间：加白名单的登录时间段。
- 创建时间：该白名单的创建时间。
- 修改时间：最近一次修改白名单的时间。
- 操作
  - 编辑：可重新编辑登录源 IP、登录用户名、登录时间、常用登录地、生效范围等。
  - 删除：可对白名单进行删除操作。

热点问题

收到异常登录告警后该如何处理？

判断该登录行为是否自己操作。

- 若是自己的登录行为，且您不希望再看到告警，请单击【处理】选择【加入白名单】操作，对常见登录源 IP、登录用户名、登录地、登录时间、生效范围进行设置。



登录源 IP 为空：代表所有来源 IP 对服务器进行登录，均不产生告警。
登录用户名为空：代表对服务器的任何用户名进行登录，均不产生告警。
登录地为空：代表不论登录地域在哪，均不产生告警。
登录时间为空：代表不论何时登录，均不产生告警。

> 注意：
>
> 登录源IP、登录用户名、登录地、登录时间不能同时为空。

- 若不是自己的登录行为，请立即修改服务器登录密码（建议修改为10位以上，包含大小写字母和特殊字符的强密码）。
  服务器被异常登录，登录者很有可能已经入侵您的服务器并留下恶意文件。建议您立即进行文件查杀、漏洞检测、基

线检测以加固您的服务器安全。

白名单怎么设置可以满足大部分用户需求？

- 场景1：固定 IP 网段登录源可以使用任一用户名对服务器进行登录，而不产生异常登录告警。
  您可在登录源 IP 中输入 IP 段，选择生效服务器范围即可。



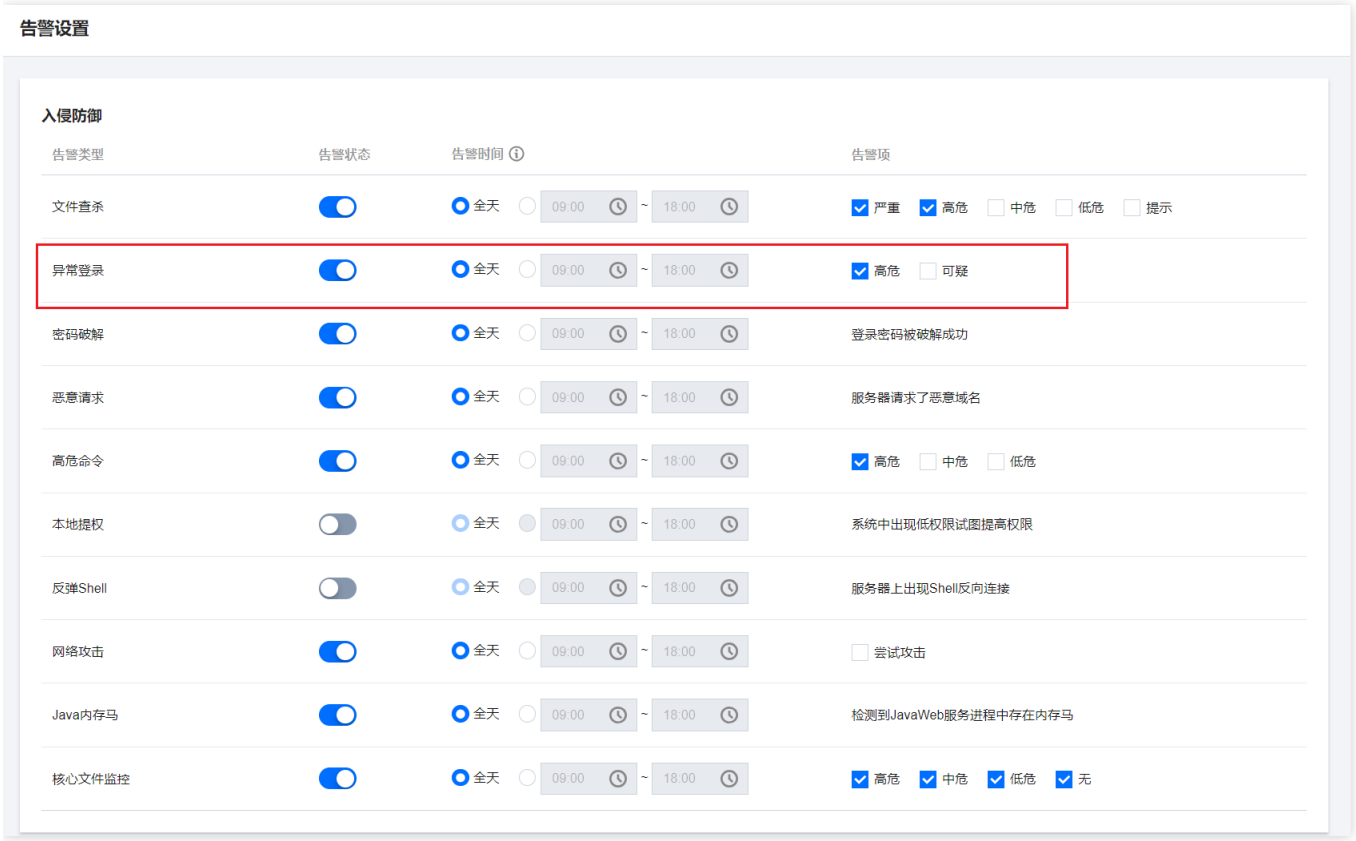
- 场景2：登录源 IP 是动态变化的，要支持登录地是中国香港地区的 IP 随时都可以使用任一用户名对服务器进行登录，而不产生异常登录告警。
  您可在常用登录地中选择香港特别行政区，选择生效服务器范围即可。



> 说明：
>
> 登录条件支持组合。

如何关闭异常登录告警？

请前往【设置中心】>【告警设置】对异常登录的告警开关进行关闭。若保持告警开关开启，建议勾选高危选项，仅告警高危的异常登录行为即可。


告警设置
入侵防御
告警类型
告警状态
告警时间
告警项
文件查杀
全天 09:00 ~ 18:00
严重 高危 中危 低危 提示
异常登录
全天 09:00 ~ 18:00
高危 可疑
密码破解
全天 09:00 ~ 18:00
登录密码被破解成功
恶意请求
全天 09:00 ~ 18:00
服务器请求了恶意域名
高危命令
全天 09:00 ~ 18:00
高危 中危 低危
本地提权
全天 09:00 ~ 18:00
系统中出现低权限试图提高权限
反弹Shell
全天 09:00 ~ 18:00
服务器上出现Shell反向连接
网络攻击
全天 09:00 ~ 18:00
尝试攻击
Java内存马
全天 09:00 ~ 18:00
检测到JavaWeb服务进程中存在内存马
核心文件监控
全天 09:00 ~ 18:00
高危 中危 低危 无

密码破解

主机安全密码破解基于网络安全防御和主机入侵检测能力，为主机提供密码暴力破解行为实时监控。

操作指南

查看密码破解事件

登录主机安全租户端控制台，在左侧导航中，选择【入侵防御】>【密码破解】，进入密码破解页面，可查看密码破解事件列表。



字段说明：

- 主机名称/实例ID：检测到存在密码破解行为的服务器名称和实例ID。
- IP地址：检测到存在密码破解行为的服务器IP地址。
- 来源 IP：攻击来源 IP 地址。
- 来源地：攻击来源 IP 所在地域。
- 协议：攻击者通过的协议，含 ssh/rdp。
- 登录用户名：攻击者登录使用的用户名。
- 端口：攻击者登录使用的端口。
- 首次攻击时间：主机安全首次监控到密码破解行为的时间。
- 最近攻击时间：该事件最近再次发生的时间。
- 尝试次数：攻击 IP 尝试密码破解的次数统计。
- 破解状态：破解成功、破解失败。
- 阻断状态：阻断、未阻断。
- 告警状态：待处理、已加入白名单、已处理、已忽略。
- 操作：
    - 标记已处理：若您已人工对该告警进行处理，可将告警标记为已处理。
    - 加入白名单：对当前告警的域名创建放行策略，当再次发生相同攻击时将不再进行告警，同时当前告警状态将变更为“已加白”。
    - 忽略：仅将本次告警进行忽略，若再有相同情况发生依然会进行告警。
    - 删除记录：删除该告警记录，控制台将不再显示，无法恢复记录，请慎重操作。

配置白名单

配置白名单后，属于白名单来源 IP 的密码破解行为将不会被阻断与告警，操作步骤如下：

1. 登录主机安全租户端控制台，在左侧导航中，选择【入侵检测 】> 【密码破解】，进入密码破解页面。
2. 在密码破解页面，单击【白名单管理】，进入白名单管理页面。
3. 在白名单管理页面，单击【添加白名单】，进入创建白名单页面中。



4. 在右侧弹出窗中，填写来源 IP 及生效范围。

> 注意：
>
> 添加白名单后，该来源 IP 的密码破解行为将不会被阻断与告警，请慎重操作。若有非白名单来源 IP 尝试登录，并命中暴力破解规则时，系统将自动发出异常告警或阻断。



字段说明：

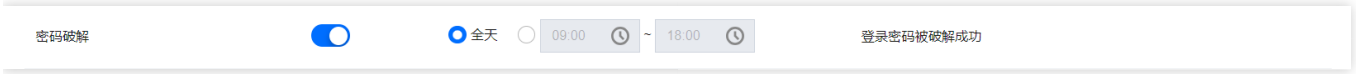
- 来源 IP：支持填写单个 IP、IP 范围（如1.1.1.1-1.1.1.10）或 IP 段（如1.1.1.0/24）。
- 生效范围：

- 全部服务器（请谨慎选择）：将对用户 AppID 下所有服务器添加信任该白名单条件。
- 自定义服务器范围：自定义选择添加信任该白名单条件的服务器范围。

- 备注：建议您输入相关规则备注。

开启告警通知

登录主机安全租户端控制台，在左侧导航中，选择【设置中心】>【告警设置】，在告警设置中，开启告警通知开关，当前产生密码破解事件时，会以站内信、短信、邮件、企业微信等方式进行通知。



密码破解事件处置指引

1. 当用户接收密码破解事件告警时，登录主机安全租户端控制台，在左侧导航中，选择【入侵防御】>【密码破解】，进入密码破解页面。
2. 查看告警事件列表中的对应攻击来源 IP。

- 若确认是可信来源 IP，用户需在该事件右侧操作栏中，单击【处理】 >【加入白名单】，设置白名单条件和生效范围（请谨慎添加白名单）。配置成功后，预计5分钟内生效，后续来自该来源 IP 的密码破解行为将不再进行告警或者阻断。



- 若确认是不可信来源 IP，且服务器已被攻击者密码破解成功。
  针对已被密码破解入侵的服务器，建议用户立即重新设置复杂密码（大写+小写+特殊字符+数字组成的12-16位的复杂密码），并检查账号列表中是否存在陌生账号，若存在陌生账号，需将陌生账号删除或者禁用，同时排查系统异常情况。

恶意请求

本文档将为您介绍如何查看并操作恶意请求告警列表及策略配置。

背景信息

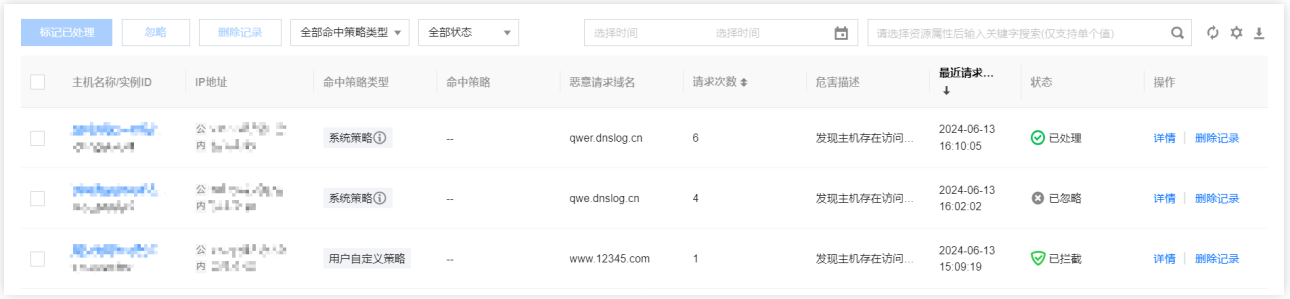
恶意请求功能提供对外界请求行为进行实时监控及处理的能力，有效识别恶意请求行为。若主机向恶意域名发起请求会被识别并记录，检测到此类恶意请求行为，系统会为您提供实时告警。

限制说明

- 恶意请求监测支持专业版、旗舰版主机。
- 恶意请求拦截仅支持 Linux 系统的旗舰版主机，且仅支持拦截服务器做 DNS 查询，不支持拦截流量上的转发。

告警列表

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵防御】 > 【恶意请求】，进入恶意请求页面。
2. 在恶意请求页面，可查看恶意请求告警列表，并进行相关操作。



- 筛选：支持按命中策略类型、状态、最近请求时间、搜索框输入主机名称、实例 ID、IP 地址、恶意请求域名进行筛选。
- 自定义展示列：单击 ，可设置告警列表展示字段。
- 导出：单击 ，可导出告警列表详细信息。
- 字段说明：
  - 主机名称/实例 ID：对恶意域名发起请求的主机名称及实例 ID
  - IP 地址：对恶意域名发起请求的主机IP
  - 命中策略类型：
    - 系统策略：系统策略为主机安全运营专家与算法专家经过多模型的规则配置，适用于大部分的恶意请求检测。
    - 用户自定义策略：用户根据业务情况对相关域名设置告警/拦截/放行动作。

- 命中策略：主机请求恶意域名所命中的策略名称。
- 恶意请求域名：域名或IP 地址
- 请求次数：主机请求次数
- 危害描述：请求该恶意域名可能造成的危害。
- 最近请求时间：最近一次请求该恶意域名的时间。
- 状态：待处理、已加白、已处理、已忽略、已拦截。
- 详情：可查看该恶意请求事件的详细情况，含风险主机信息、恶意请求详情、危险描述、修复建议。
- 处理：标记已处理、加入白名单、创建拦截策略、忽略、删除记录。


恶意请求详情
待处理
标记已处理
加入白名单
创建拦截策略
忽略
删除记录
风险主机
主机名称
客户端在线
实例 ID
公
首次请求时间 2025-03-03 11:30:55
最近请求时间 2025-03-03 11:31:12
恶意请求详情
命中策略名称 tecs
命中策略类型 用户自定义策略
恶意请求域名
标签特征
进程
命令行
MD5
请求次数
PID
危害描述
告警描述 发现主机存在访问恶意IP/域名的行为，您的主机可能已经失陷。
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。
修复建议
建议方案 1.检查恶意进程及非法端口，删除可疑的启动项和定时任务；
2.隔离或者删除相关的木马文件；
3.对系统进行风险排查，并进行安全加固，详情可参考如下链接：
参考链接 暂无



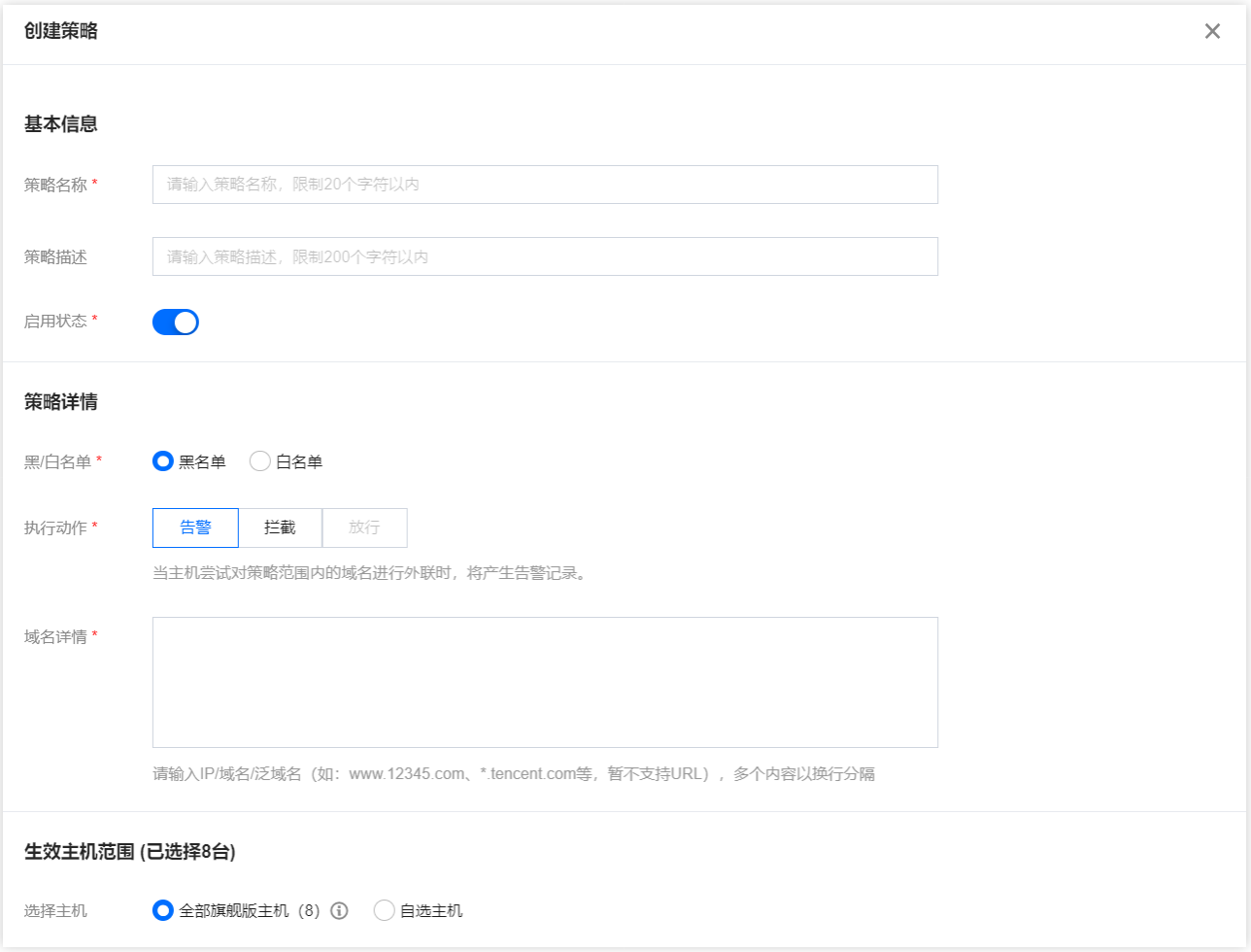
策略配置

管理策略

在恶意请求页面上方选择【策略配置】，进入策略配置页面。



- 筛选：支持按策略类型、执行动作、生效状态、关键字进行筛选。
- 自定义展示列：单击  ，可设置策略列表展示字段。
- 导出：单击  ，可导出策略列表的详细信息。
- 字段说明：
  - 策略名称：系统策略固定名称，分别为：系统规则（重保）、系统规则（标准）；用户自定义策略则为用户所设置的策略名称。
  - 策略类型：系统策略、用户自定义策略。
  - 黑/白名单：该策略属于白名单/黑名单。
  - 域名详情：IP/域名或泛域名。
  - 生效主机：该策略生效的主机范围。
  - 更新时间：最近一次更新策略的时间。
  - 执行动作：请求访问域名时命中策略将自动执行的动作（放行/告警/拦截）。
  - 生效状态：策略是否生效。
  - 编辑：对策略进行编辑。
  - 删除：删除该策略。
- 创建策略：
  - 黑名单：当主机请求了黑名单中的域名，将执行告警/拦截动作。
  - 白名单：当主机请求了白名单中的域名，将执行放行动作。



注意：

- 系统策略是内置策略，不支持新增、编辑和删除，仅支持开关。
- 系统策略（标准）建议保持开启状态，系统策略（重保）建议在重保期间按需开启。
- 用户自定义策略中，拦截策略仅对旗舰版主机生效。

本地提权

本文档将为您介绍如何对提权事件详情进行查看和处理，同时指导您如何创建白名单，用于设置被允许的提权行为。

背景信息

若出现以低权限进入系统，通过某些手段提升权限，获取到高权限的事件，很有可能为黑客的攻击行为，该行为会危害到主机安全。本地提权功能可实时监控您云服务器上的提权事件，并能对提权事件详情进行查看和处理，同时也支持白名单创建功能，用于设置被允许的提权行为。

操作步骤

告警列表

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵防御 】>【本地提权】，进入本地提权的事件列表标签页。
2. 在本地提权的【告警列表】标签页，可查看本地提权事件列表，并进行相关操作。
3. 在【告警列表】标签页，可查看发生提权事件的主机名称/实例ID、 IP地址、提权用户、父进程、父进程所属用户、发现时间、状态、操作等信息，列表展示字段支持自定义。

- 筛选事件：本地提权事件列表支持选择日期查看相应的事件，支持按关键字及标签查询（多个关键字用竖线 “|” 分隔，多个过滤标签用回车键分隔）事件，同时支持按状态、筛选事件。



- 自定义设置列表字段：在本地提权告警列表上方，单击设置图标，可设置列表展示字段，选择完成后，单击确定，即可设置成功。



- 事件导出：在本地提权告警列表上方，单击 ，可将本地提权告警列表导出。
- 详情：在本地提权事件的右侧操作栏，单击【详情】，可查看本地提权事件详情。



- 标记已处理：若您已人工对该告警进行处理，可将告警标记为已处理。
- 加入白名单：对当前告警服务器添加白名单提权进程，后续再检测到相同提权行为将不再告警。
- 忽略：仅将本次告警进行忽略，若有相同情况发生依然会进行告警。
- 删除记录：删除该告警记录，控制台将不再显示，无法恢复记录，请谨慎操作。

白名单管理

本地提权功能支持添加白名单，通过设置白名单提权条件，将满足条件的事件标记为白名单。

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵防御】>【本地提权】，进入本地提权页面。
2. 在本地提权页面，选择【白名单管理】>【添加白名单】。



3. 在添加白名单弹窗中，设置提权条件，包括：带 S 权限的进程、自定义提权进程（支持多个进程名，以英文逗号分隔，例如 123.exe,test.exe），同时选择该条件覆盖的服务器范围，单击【确定】。

> 注意：
>
> - s 权限： 设置使文件在执行阶段具有文件所有者的权限，相当于临时拥有文件所有者的身份。
> - 勾选两个条件时，需要同时满足才能命中白名单。
> - 若服务器范围选择全部服务器，将对用户 APPID 下所有服务器添加信任该白名单条件，请谨慎操作。



4. 设置完成后，可在白名单管理列表查看该条件，告警列表中满足该条件的事件即会被标记为白名单事件。
5. 在白名单管理页面，可对白名单进行筛选删除等操作。

- 筛选：已配置的白名单支持按关键字及标签查询（多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔）筛选，同时支持按是否带 S 权限进行筛选。



- 自定义设置列表字段：在白名单列表上方，可设置列表展示字段，选择完成后，单击【确定】，即可设置成功。



- 编辑：在目标白名单的右侧操作栏，单击【编辑】，可对已创建的白名单进行编辑。



- 删除：在白名单列表中，支持对已配置的白名单进行删除。



反弹Shell

本文档将为您介绍如何对反弹 Shell 详情进行查看和处理，同时指导您如何创建白名单，用于设置被允许的反向连接行为。

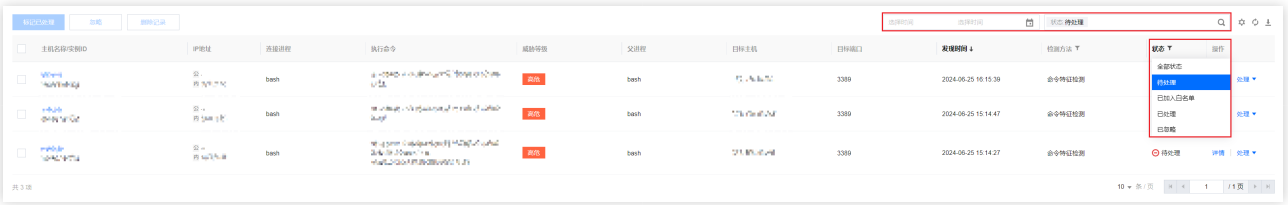
背景信息

反弹 Shell 功能是基于多维度多手段，对服务器上的 Shell 反向连接行为进行识别记录，为您的云服务器提供反弹 Shell 行为的实时监控能力。

操作步骤

告警列表

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵防御】>【反弹 Shell】，进入反弹 Shell 告警列表页。
2. 在反弹 Shell 【告警列表】标签页面，可查看反弹 Shell 事件列表，并进行相关操作。
   可查看发生反弹 Shell 的主机名称/实例ID、IP地址、连接进程等信息，列表展示字段支持自定义。
   - 筛选：反弹 Shell 告警列表支持选择日期查看相应事件，支持按关键字及标签查询（多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔）事件，同时支持按状态（全部、待处理及已确认）筛选告警。



   - 自定义设置列表字段：在反弹 Shell 告警列表上方，单击 ，可设置列表展示字段，选择完成后，单击【确定】，即可设置成功。



- 事件导出：在反弹 Shell 告警列表上方，单击 ，可将反弹 Shell 告警列表导出。
- 详情：在目标反弹 Shell 事件的右侧操作栏，单击【详情】，可查看反弹 Shell 事件详情。



- 标记已处理：建议您参照告警详情中的“修复建议”，人工对该告警进行处理，处理后可将告警标记为已处理。
- 加入白名单：加入白名单操作后，当再次发生相同情况时将不再进行告警，请谨慎操作。
- 忽略：仅将本次告警进行忽略，若再有相同情况发生依然会进行告警。
- 删除记录：删除该告警记录，控制台将不再显示，无法恢复记录，请慎重操作。

白名单管理

反弹 Shell 支持添加白名单，通过设置白名单条件，将满足条件的事件标记为白名单。

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵防御】>【反弹 Shell】 ，进入反弹 Shell 页面。
2. 在反弹 Shell 页面，选择【白名单管理】 > 【添加白名单】。



3. 在添加白名单弹窗中，设置反弹 Shell 条件，包括：目标主机、自定义连接进程（支持多个进程名，以英文逗号分隔），同时选择该条件覆盖的服务器范围，单击确定。



字段说明：

- 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（支持多个端口并以英文逗号分隔，不限端口请留空）。
- 勾选两个条件时，需要同时满足才能命中白名单。
- 若服务器范围选择全部服务器，将对用户 APPID 下所有服务器添加信任该白名单条件，请谨慎操作。

4. 设置完成后，可在白名单管理列表查看该条件，告警列表中满足该条件的事件会被标记为白名单事件。
5. 在白名单管理页面，可对白名单进行筛选删除等操作。
   - 筛选：已配置的白名单支持按关键字及标签查询（多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔）筛选。





   - 自定义设置列表字段：在白名单列表上方，单击 ，可设置列表展示字段，选择完成后，单击确定，即可设置成功。



- 编辑：在目标白名单的右侧操作栏，单击【编辑】，可对已创建的白名单进行编辑。



- 删除：在白名单列表中，支持对已配置的白名单进行删除。



高危命令

本文档将为您介绍如何查看并操作高危命令事件列表。

背景信息

基于多维度多种手段，主机安全可对系统中的命令实现实时监控，并且可通过配置规则对命令危险程度进行等级划分，若检测出高危命令，系统会向您提供实时告警通知。

操作步骤

告警列表

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵防御】>【高危命令】，进入高危命令的告警列表标签页。
2. 在高危命令的【告警列表】标签页，可查看高危命令告警列表，并进行相关操作。在告警列表界面可展示发生高危命令告警的主机名称/实例ID、IP地址、命中策略类型、命中策略、威胁等级等信息，列表展示字段可进行自定义。
   - 筛选：高危命令告警列表支持选择日期查看，支持按关键字及标签查询（多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔）事件，同时支持按威胁等级及状态筛选事件。



   - 自定义列表字段：在高危命令事件列表上方，单击 ，可设置列表展示字段，选择完成后，单击【确定】，即可设置成功。



- 事件列表导出：在高危命令告警列表上方，单击 ，可将高危命令告警列表导出。
- 详情：单击【详情】，可查看高危命令告警详情及进程树信息。



- 标记已处理：建议您参照告警详情中的"修复建议"，人工对该告警进行处理，处理后可将告警标记为已处理。
- 加入白名单：对当前告警的域名创建放行策略，当再次发生相同攻击时将不再进行告警，同时当前告警状态将变更为"已加白"。
- 创建拦截策略：对当前告警的域名创建拦截策略，当再次发生相同攻击时将为您进行自动拦截。
- 忽略：仅将本次告警进行忽略，若再有相同情况发生依然会进行告警。
- 删除记录：删除该告警记录，控制台将不再显示，无法恢复记录，请慎重操作。

策略配置

创建自定义策略

高危命令功能支持创建自定义策略，通过设置策略对威胁命令进行相应的处理行为。

1. 登录主机安全租户端控制台 ，在左侧导航栏选择【入侵防御】>【高危命令】，进入高危命令页面。
2. 选择【策略配置】>【创建策略】，进入创建策略页面。
3. 在创建策略页面，填写策略的基本信息，包括策略名称、策略描述和启用状态。
4. 填写策略详情，包括选择黑名单/白名单及其对应的执行动作，填写正则表达式，选择威胁等级，选择生效主机范围。
   - 黑名单规则，指发现主机存在威胁命令时将产生告警通知。

     说明

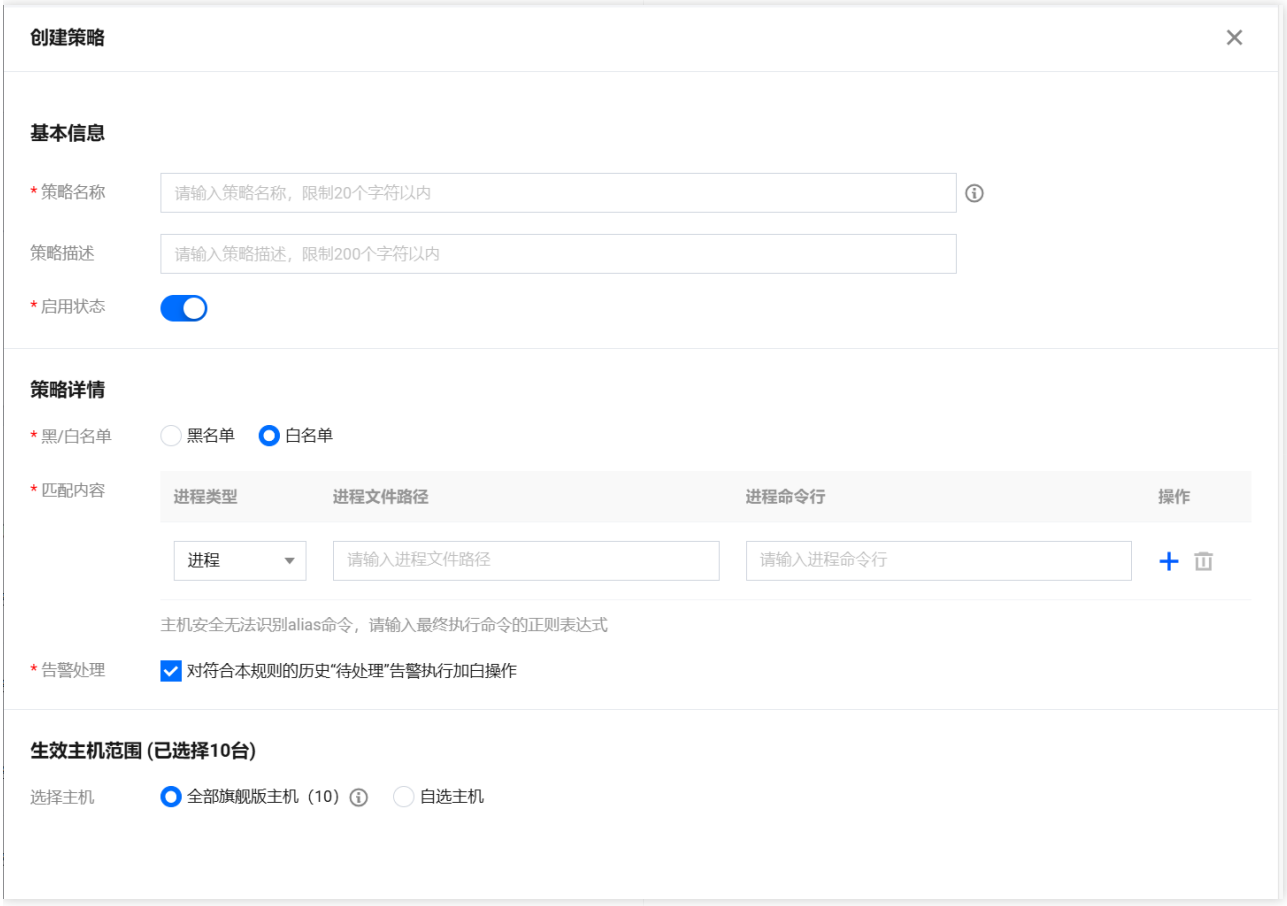
     - 拦截策略指当发现主机存在威胁命令时，将对威胁命令的执行进行自动拦截，并告警通知。
     - 拦截策略仅支持旗舰版机器。



- 白名单规则，指对威胁命令进行放行，不再产生告警或拦截行为。

  说明

  - 若生效主机范围选择全部专业版或旗舰版主机，新增专业版或旗舰版主机时，将自动加入策略生效范围。
  - 可勾选对符合本策略规则的历史“待处理”告警，执行本策略规则的操作。



5. 设置完成后，可在策略列表查看，列表中应用于黑名单的策略会被标记为相应的威胁等级。
6. 在策略列表中可对策略进行筛选、编辑和删除等操作。



- 筛选：已配置的策略支持按关键字及标签查询（多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔）筛选，支持按威胁等级（全部/高危/中危/低危/无），支持按执行动作（告警/拦截/放行），支持按生效状态（已生效/未生效）进行筛选。



- 自定义设置列表字段：在策略列表上方，单击 ，可设置列表展示字段，选择完成后，单击【确定】，即可设置成功。
- 启用状态：列表支持设置策略的启用状态，可在启用状态列，单击【启用开关】，决定该策略是否启用。
- 编辑：在策略列表的右侧操作栏，单击【编辑】，可对已创建的策略进行编辑。
- 删除：在策略列表中，支持对已配置的策略进行删除。

系统策略

高危命令功能新增系统自动拦截规则，开启后，支持自动拦截检测出的系统高危命令，部分内容仍需您手动配置策略。

- 系统高危命令：主机安全运营专家与算法专家经过沉淀的系统高危命令，此名单中的高危命令可进行自动拦截。
- 拦截原理说明：高危命令自动拦截采用查杀命中规则的进程的方式，例如，如果进程 A 尝试创建一个"/bin/bash -i"进程（假设"bash -i"已被列入黑名单），那么这个尝试创建的"/bin/bash"进程将会被终止（或创建失败），而进程 A 本身不会受到影响。

  > 说明：
  >
  > - 如您发现误拦截情况，可创建自定义策略进行加白处理。
  > - 系统自动拦截规则仅限旗舰版主机使用。

网络攻击

网络攻击基于安全攻防团队技术支持，为您自动化监测恶意流量。结合入侵过程中产生的恶意行为。实时对攻击和告警进行自动化关联分析，输出攻击流量数据、通知攻击事件。本文档将为您介绍如何查看和处理网络攻击告警。

限制说明

- 检测对象：仅支持专业版/旗舰版的 Linux 主机。
- 检测范围：仅检测部分出现 EXP、且在云上有攻击成功案例的热点漏洞攻击行为。
- 漏洞防御：仅支持旗舰版的 Linux 主机。

防御状态说明

- 支持漏洞防御（未开启）：主机安全支持防御该漏洞，但该主机未对该漏洞开启防御。
- 支持漏洞防御（已开启）：主机安全支持防御该漏洞，且该主机已对该漏洞开启防御。
- 暂不支持漏洞防御：主机安全不支持防御该漏洞。

> 注意：
>
> - 漏洞防御未开启可能原因：防御开关未开启、该主机非旗舰版或不在防御主机范围内。
> - 存在攻击事件表示当前有黑客利用该漏洞的攻击手法进行攻击，并不表示当前机器存在此漏洞。

告警统计

1. 登录主机安全租户端控制台，在左侧导航栏，选择【入侵防御】>【网络攻击】。
2. 在网络攻击页面，支持查看网络攻击中漏洞防御状态，待处理告警相关数据统计及 Top5 情况。



字段说明：

- 漏洞防御状态：体现漏洞防御开关的状态。
- 待处理网络告警：当前待处理的告警数量。
- 受攻击资产：当前待处理告警所涉及到的受攻击资产数。
- 受攻击端口：当前待处理告警所涉及到的受攻击端口数。
- 攻击来源 IP：当前待处理告警的攻击来源 IP 数。

查看告警

在网络攻击页面，支持查看网络攻击详情，包括主机名称/实例 ID、IP 地址、目标端口等信息。



字段说明：

- 主机名称/实例 ID：受攻击的主机的名称和实例 ID。
- IP 地址：指受攻击主机的公网/内网IP。
- 目标端口：受攻击端口。
- 攻击来源 IP/地址：指攻击者的来源 IP及所在地。
- 漏洞名称：指攻击者有利用某漏洞的攻击手法进行攻击，以及目前漏洞防御的开启状态。
- 攻击状态：指攻击者攻击后的结果，尝试攻击（被攻击但未被攻击成功）、攻击成功（实锤攻击）。
- 最近攻击时间：最近检测到攻击行为的时间。
- 攻击次数：累计检测到相同攻击的次数。
- 处理状态：待处理、已处理、已加白、已忽略。
- 详情：支持查看告警详情、危害描述、解决方案。

网络攻击详情 • 待处理

标记已处理 | 开启漏洞防御 | 加入白名单 | 忽略 | 删除记录

告警详情 | 进程树 | 事件调查

主机名/IP 详情
[redacted] • 客户端在线
内 [redacted] 外 [redacted]

最近攻击时间 2023-12-30 09:11:45
攻击次数 1
目标端口 8080

告警详情

攻击状态	尝试攻击
攻击源IP	[redacted]6
攻击源地址	[redacted]
漏洞名称	Apache log4j2 远程代码执行漏洞 (CVE-2021-44228)
漏洞CVE编号	CVE-2021-44228
漏洞全网攻击热度	• 支持漏洞防御(未开启)
服务进程	node /root/tcs/tcs-installer/frontend/frontend-platform/server.js
攻击数据包	[redacted]

危害描述

告警描述：告警说明该端上已经有发现恶意网络攻击流量，请注意相关防护，否则可能会存在被入侵风险。
该告警是在主机侧感知到来自外部的使用热门漏洞攻击的请求，若非自行扫描则通常代表该主机网络服务对外暴露，且正在被攻击/探测。

解决方案

建议方案：
1. 建议相关应用部署WAF防护/云防火墙防护/开启漏洞防御
2. 如果端口应用不需要对外，通过云防火墙或者安全组限制端口对公网暴露
3. 若该告警为自行扫描，则可通过添加来源IP到白名单来过滤告警。

处理告警

1. 在网络攻击告警列表中，单击操作列的【处理】。

> 说明：
>
> 选中一个或多个告警，可以单击左上角的【标记已处理】【忽略】【删除记录】，进行批量操作。



2. 支持对待处理的告警标记已处理、开启漏洞防御、加入白名单、忽略、删除记录操作。

   - 标记已处理：人工对该告警进行处理，处理后可将告警标记为“已处理”。
   - 加入白名单：将攻击来源IP加入白名单，后续主机安全将不再对该来源IP的网络攻击行为进行告警，请谨慎操作。



   - 忽略：仅将本次告警进行忽略，若再有相同情况发生仍然会进行告警。
   - 删除记录：删除该告警记录，控制台将不再显示，无法恢复记录，请慎重操作。

Java内存马

概述

主机安全支持实时监控、捕捉 JavaWeb 服务进程内存中存在的未知 Class，结合安全攻防经验及专家知识自动识别内存木马。若检测到 Java 内存马，系统会向您提供实时告警通知。

操作步骤

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵防御】 > 【Java 内存马】，进入 Java 内存马页面。
2. 选择【插件配置】，插件配置是监测 Java 内存马的前提，您可对旗舰版主机进行插件的开启和关闭，并观测插件的具体运行状态。

   > 说明：
   >
   > - 启用 Java 内存马插件后，主机安全会自动检测主机上 JavaWeb 服务进程，并注入检测探针到服务进程中，实时监控黑客通过漏洞、Shell 等注入的 Java 内存马。
   > - 已成功注入 Java 内存马插件的主机，将实时监控、捕捉 JavaWeb 服务进程内存中存在的未知 Class，结合安全攻防经验及专家知识自动识别内存木马。若检测到 Java 内存马，系统会向您提供实时告警通知。



字段说明：

- 启用/关闭插件：Java 内存马插件默认关闭，支持用户手动设置开关，可单主机设置，也可多选主机批量设置。
- 插件状态：全部正常、存在异常、未开启。
- 首次开启时间：指首次启用插件的时间。
- 更新时间：指近期启用或关闭插件的时间。
- 详情：可查看当前已注入的 Java 内存马插件运行状态，包括进程 PID、进程主类名、插件状态（注入中、注入成功、插件超时、插入退出、注入失败）、注入日志。

启用 Java 内存马插件后，您可选择【告警列表】查看检测到的 Java 内存马事件，并进行相关处理操作。



字段说明：

- 主机名称/实例ID：被检出存在 Java 内存马的主机名称和实例ID。
- IP地址：被检出存在 Java 内存马的主机IP地址。
- Java 内存马类型：包括 Filter 型、Listener 型、Servlet 型、Interceptors 型、Agent 型、其他。
- 说明：归纳说明 Java 内存马的概况。
- 首次发现时间：该 Java 内存马首次被检测到的时间。
- 最近检测时间：近期检测发现该 Java 内存马仍存在的时间。
- 状态：待处理、已处理、已加白、已忽略。
- 操作：
    - 单击【详情】可查看该内存马事件详情。



- 单击 Java 内存马详情中的【查看文件】，可查看落地文件的反编译 Java 文件，支持复制，支持下载反编译 Java 文件或原 Class 文件。



- 单击【处理】可对事件进行标记已处理、加入白名单、忽略、删除记录操作，可单事件处理，也可多选事件批量处理。


添加白名单
白名单内容
• 加白内容包含下述5个条件，设置其中任一条件后白名单即可生效，若设置多个条件匹配此规则，条件间将以"或/且"关系进行生效。
• 白名单保存成功后，5分钟内生效，后续可在白名单管理列表对相应规则进行编辑、删除操作。
* 加白条件
Class (类名)
Parent class name (父类名)
且
Inherited API (继承的接口)
Note (注释)
Class Loader (所属类加载器)
告警处理
对符合本规则的历史"待处理"告警执行加白操作
生效主机范围（已选择104台）
选择主机
全部旗舰版主机（104）
自选主机

核心文件监控

核心文件监控的监控规则分为系统规则和自定义规则。系统规则为主机安全运营专家与算法专家经过多模型沉淀的规则配置，适用于大部分的篡改用户配置监控需求，您也可以根据业务需要自定义规则，自定义规则支持编辑、复制和删除。

> 说明：
>
> - 核心文件监控属于主机安全旗舰版功能。
> - 核心文件监控目前支持 Linux 内核版本为3.10及以上的操作系统。

新建规则

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵防御】 >【核心文件监控】。
2. 在【监控规则配置】页面中，单击左上角处的【新增规则】，右侧弹出新增规则弹窗。
3. 在新增规则弹窗中，依次配置基础设置、规则内容设置和生效服务器范围参数。

   - 基础设置



     字段说明：

     - 规则名称：自定义名称。
     - 威胁等级：根据实际需求可选择高危、中危、低危或无。
     - 启用状态：可启用或不启用该新增规则。

   - 规则内容设置：单击【添加规则】，可添加多行，最大添加20行。



字段说明：

- 监控行为：修改文件/读取文件。
- 进程路径：文件篡改动作发起的进程文件路径，例如程序 /usr/bin/vi，对应规则可以是 */vi。
- 文件路径：例如 /etc/cron.d/attack 对应规则可以是 /etc/cron.d/*。
- 执行动作：告警指的是对文件系统变化产生自动告警事件，记录事件详情；放行指的是对文件系统变化产生事件进行放行操作，记录事件详情。

  > 说明：
  >
  > 当告警放行进程路径及被访问文件一致，且生效服务器有重叠，重叠部分服务器不产生告警（即优先以放行条件为准）。

  - 生效主机范围：可根据实际需求选择全部服务器或自选服务器。

4. 配置完成后，单击【保存】即可。

管理规则

编辑规则

1. 在【核心文件监控】>【监控规则配置】中展示了已新增的规则，操作列支持【复制】【编辑】【删除】。



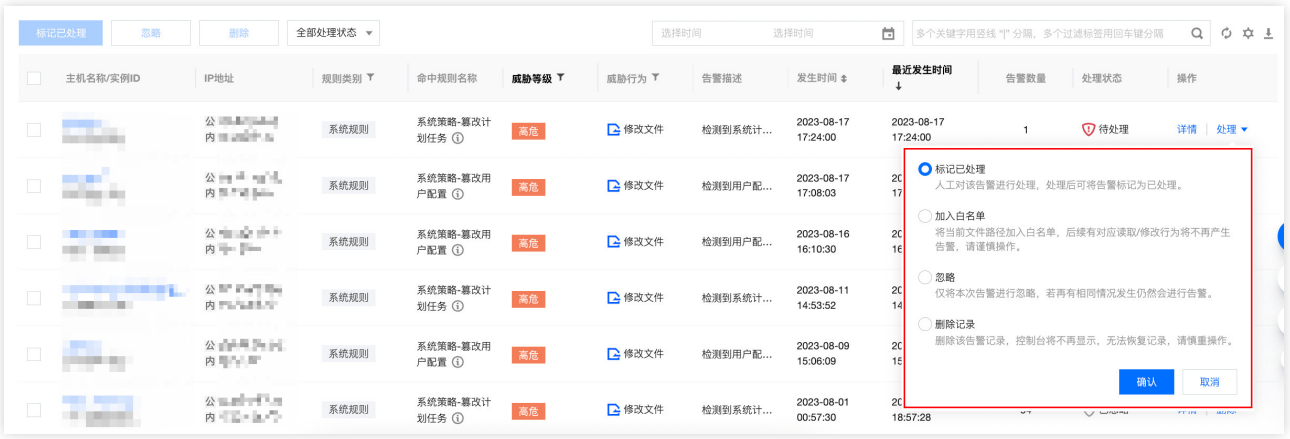
> 注意：
>
> 删除后，规则将无法恢复，请谨慎操作。

告警列表

告警列表支持查看核心文件异常告警记录，可对告警记录进行处理（标记已处理、加入白名单、忽略），也可对告警记录进行删除。

处理告警记录

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【入侵防御】 > 【核心文件监控】。
2. 在【告警列表】页面，选择所需告警记录，单击【处理】，选择标记已处理、加入白名单、忽略或删除记录。

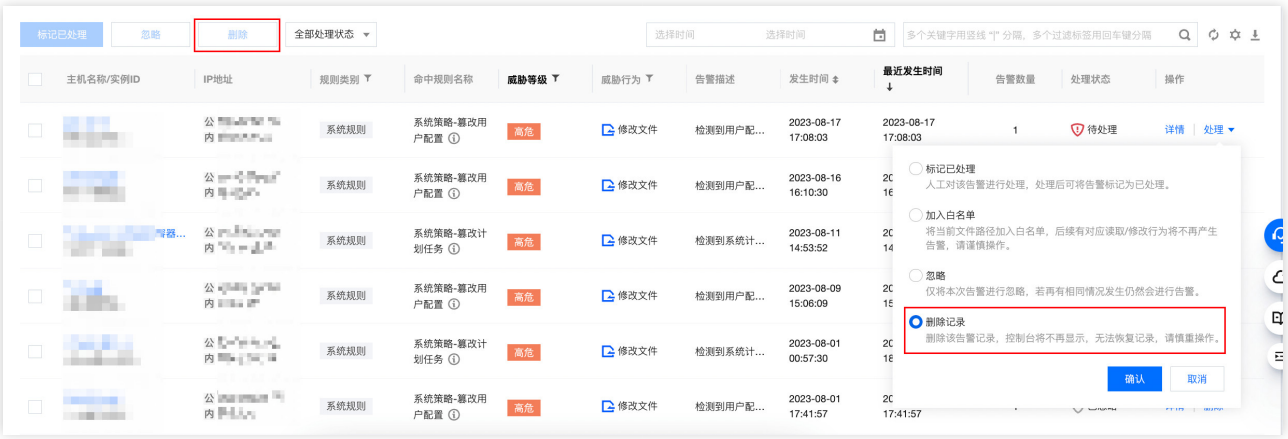


字段说明：

- 标记已处理：人工对该告警进行处理，处理后可将告警标记为已处理。
- 加入白名单：将当前文件路径加入白名单，后续有对应读取/修改行为将不再产生告警，请谨慎操作。
- 忽略：仅将本次告警进行忽略，若再有相同情况发生仍然会进行告警。
- 删除记录：删除该告警记录，控制台将不再显示，无法恢复记录，请慎重操作。

删除告警记录

1. 在【告警列表】页面，支持单个删除告警记录或批量删除告警记录。
   - 单个：选择所需告警记录，单击【删除】，弹出确认删除对话框。



   - 批量：选择一个或多个告警记录，单击左上角的【删除】，弹出确认删除对话框。



2. 在确认删除对话框中，单击【确定】，即可删除所选告警记录。

> 说明：
>
> 删除的告警记录，控制台将不再显示，无法恢复记录，请慎重操作。

漏洞管理

漏洞管理旨在帮助客户扫描系统中存在的安全漏洞并提供漏洞信息及修复建议等信息，部分漏洞可开启精准防御、可自动修复。本文档将为您介绍如何进行漏洞管理。

限制说明

- 漏洞管理范围说明如下：（‘✓’表示支持，‘-’表示暂不支持）。

漏洞管理功能	**漏洞类型**	**Linux 系统**	**Windows 系统**
漏洞扫描 专业版、旗舰版主机适用	Linux 软件漏洞	✓	-
	Windows 系统漏洞	-	✓
	Web-CMS 漏洞	✓	✓
	应用漏洞	✓	✓
漏洞防御 旗舰版主机适用	Linux 软件漏洞	-	-
	Windows 系统漏洞	-	-
	Web-CMS 漏洞	✓仅支持部分漏洞	-
	应用漏洞	✓仅支持部分漏洞	-
漏洞自动修复 旗舰版主机适用 （仅限CVM云服务器）	Linux 软件漏洞	✓ 仅支持部分漏洞	-
	Windows 系统漏洞	-	-
	Web-CMS 漏洞	✓ 仅支持部分漏洞	✓ 仅支持部分漏洞
	应用漏洞	-	-

> 说明：
>
> 因漏洞修复可能对用户业务造成影响，漏洞自动修复并非检出漏洞后立即进行自动化修复，须用户了解漏洞后单击修复并进行数据备份，才可进行自动化修复。

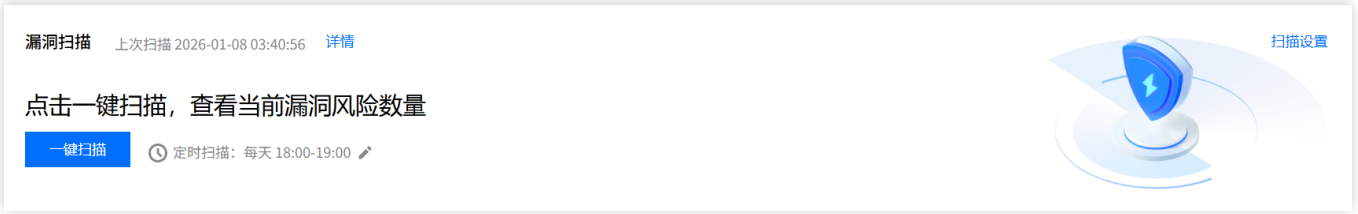
- 漏洞扫描支持的操作系统，详情如下：

操作系统	系统版本	系统漏洞	应用漏洞/Web-CMS漏洞
Centos	Centos 5	✓	✓

	Centos 6	✓	✓
	Centos 7	✓	✓
	Centos 8	✓	✓
Debian	Debian 8	-	✓
	Debian 9	-	✓
	Debian 10	-	✓
	Debian 11	-	✓
	Debian 12	-	✓
Windows	Windows Server 2008	✓	✓
	Windows Server 2012	✓	✓
	Windows Server 2016	✓	✓
	Windows Server 2019	✓	✓
	Windows Server 2022	✓	✓
Ubuntu	Ubuntu 16.04	✓	✓
	Ubuntu 18.04	✓	✓
	Ubuntu 20.04	✓	✓
	Ubuntu 21.04	✓	✓
	Ubuntu 22.04	✓	✓
	Ubuntu 24.04	✓	✓
Tlinux/Tencentos	Tlinux	-	✓
RockyLinux	RockyLinux	-	✓
Opencloudos	Opencloudos	-	✓

漏洞扫描

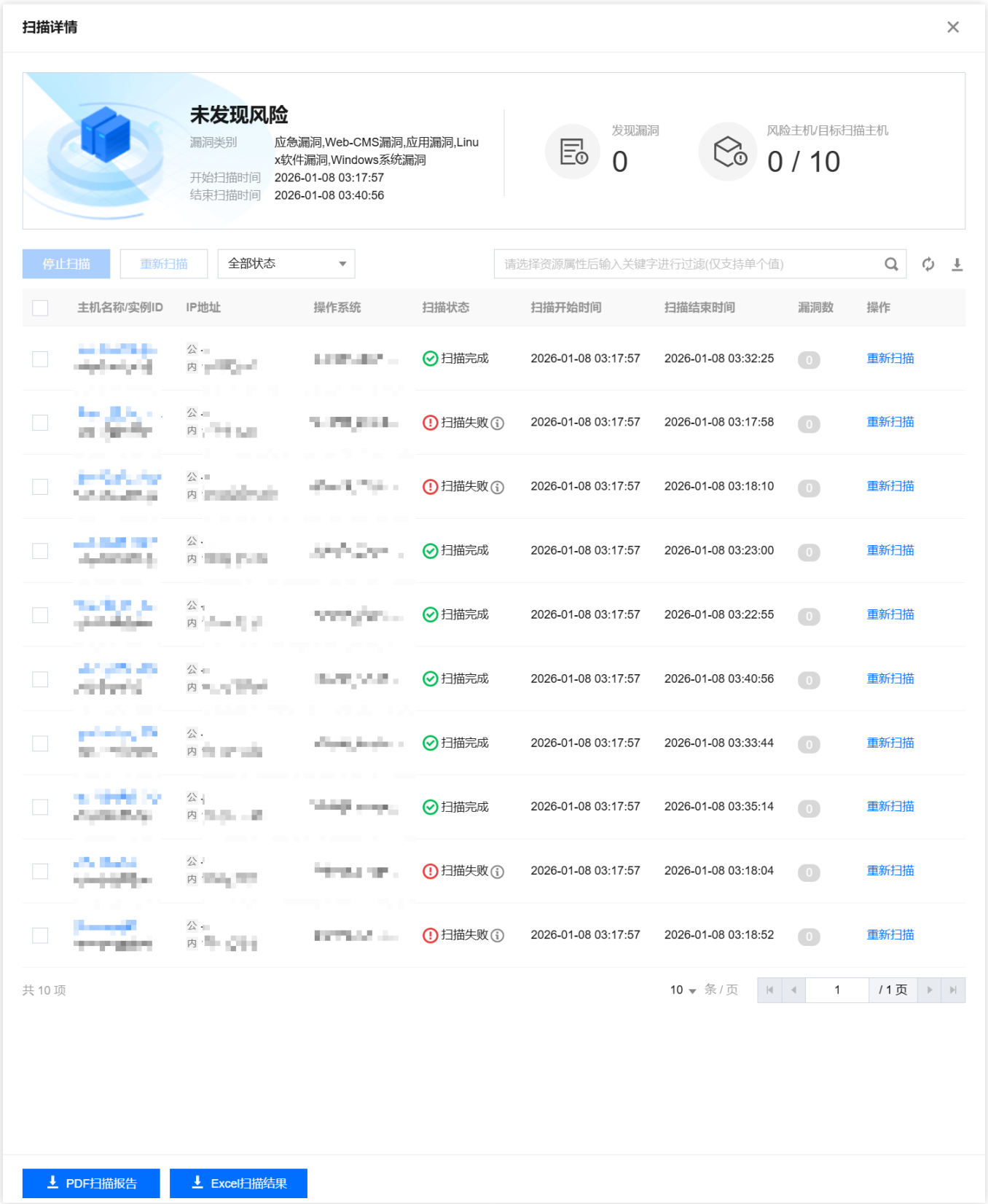
1. 登录[主机安全租户端控制台]，单击左侧导航中的【漏洞管理】。
2. 在漏洞扫描模块中，支持一键扫描、定时扫描设置。



- 单击【一键扫描】**，**将打开一键扫描设置弹窗，您可对本次扫描的漏洞类别、漏洞威胁等级、扫描超时时长、扫描服务器范围进行设置；单击【扫描设置】将打开漏洞设置弹窗并锚点至【定时扫描】，您可对定时扫描开关、周期、漏洞类别及漏洞威胁等级进行设置。

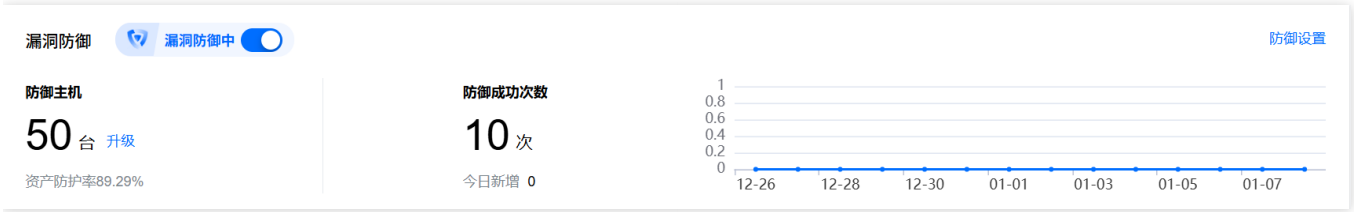


- 单击【详情】可查看上一次漏洞扫描的详情，并支持下载 PDF 扫描报告、Excel 扫描结果。



漏洞防御

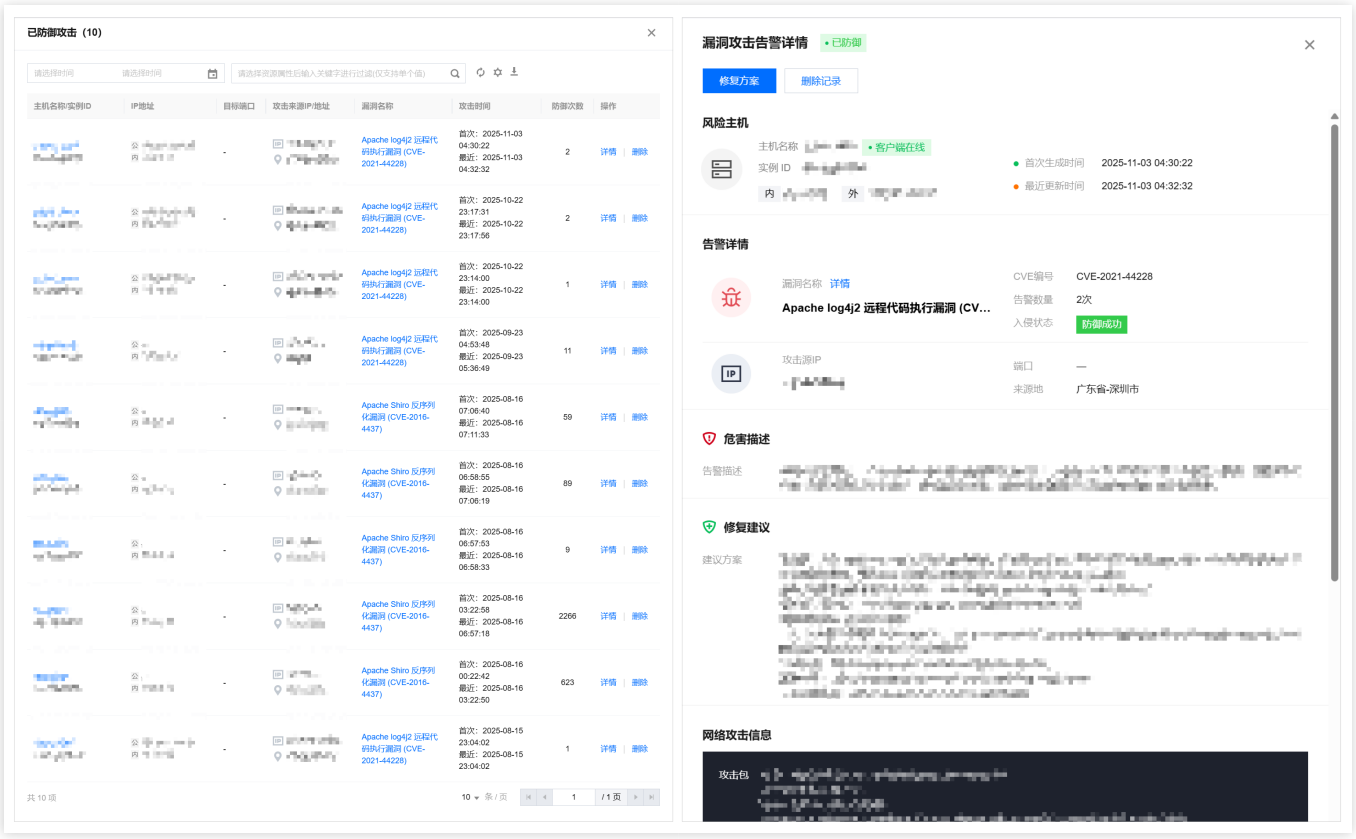
在【漏洞防御】模块中，支持漏洞防御开关启停、查看防御主机台数、防御成功次数及防御趋势情况。



- 单击【防御设置】将打开漏洞设置弹窗并锚点至【漏洞防御】，您可设置漏洞防御开关、查看可防御漏洞范围、勾选防御更多服务、选择防御主机范围、查看防御插件详情。



- 单击【防御成功次数】，您可查看当前已成功防御的攻击，且可查看攻击详情。



漏洞处置

1. 在漏洞管理页下方，您可查看当前检出漏洞的统计情况及详细漏洞列表。
2. 在**【漏洞概览】**模块中，展示了漏洞检出情况、网络攻击事件次数及今日新增情况，并展示了主机安全漏洞库总数。



字段说明：

- 全部漏洞：检出 Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞的数量总和。
- 影响主机：检出漏洞的主机数量。
- 网络攻击事件：统计近1个月内网络攻击事件的数量。
- 已支持漏洞：可查看主机安全支持检测的漏洞库，单次模糊搜索最多可展示100条结果。

3. 在【漏洞列表】模块中，分为【应急漏洞】、【全部漏洞】2类，二者主要区别如下。

维度	应急漏洞	全部漏洞

定位	针对新发现、影响范围广、危害程度高的紧急漏洞而设置的重点漏洞清单。	汇总展示所有已检出的服务器漏洞。
操作方式	用户可主动发起扫描。	展示已扫描结果。
更新机制	基于运营端漏洞库设置更新应急漏洞列表。	基于扫描结果动态更新。
覆盖范围	仅包含应急漏洞。	包含所有已检出的漏洞（含应急漏洞）。
使用场景	用于应急响应场景，快速识别和处置紧急漏洞。	用于全面了解当前服务器的漏洞情况，进行漏洞管理和修复。

4. 由于均是从检出视角展示漏洞，二者本质无差异，下面以【全部漏洞】举例，为您介绍漏洞处置。



字段说明：

- 漏洞名称/标签：漏洞名称指当前检出的漏洞，标签指该漏洞的标签（如：远程利用、服务重启、存在 EXP 等）。
- 漏洞类型：Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞。
- 威胁等级：严重、高危、中危、低危。
- CVSS：指通用漏洞评分系统的评分，分数范围从0到10，0代表最不严重，10代表最严重。
- CVE 编号：公共漏洞暴露库中，识别该漏洞的唯一编号。
- 最后扫描时间：最近一次扫描到该漏洞的时间。
- 影响主机：存在该漏洞的主机数量。
- 处理状态：待修复、修复中、扫描中、已修复、已忽略、修复失败。
- 是否支持自动修复：可自动修复、不支持自动修复。
- 操作
  - 修复方案：暂不支持自动修复的漏洞，可单击【修复方案】打开漏洞详情弹窗，根据修复方案手动修复漏洞。
  - 自动修复：部分 Linux 软件漏洞、Web-CMS 漏洞支持自动修复，可单击【自动修复】选择需要修复的服务器进行修复，请参见漏洞自动修复。
  - 更多：重新扫描（重新对该漏洞进行扫描）；忽略（对该漏洞进行忽略，后续不再对此漏洞目前影响的主机扫描该漏洞）。

安全基线

本文档将介绍如何使用基线管理功能，帮助您管理服务器中的基线安全。

背景信息

云平台主机安全支持对基线检测项进行定期检测和一键检测，支持对指定主机上的指定基线项进行检测，支持通过检测策略了解基线通过率及风险情况，提供基线和检测项的风险等级和修复建议，提供默认基线策略，有助于您更好的管理服务器中的基线安全。

操作指南

1. 登录主机安全租户端控制台，在左侧导航栏中，选择【基线管理】>【安全基线】，进入安全基线页面。
2. 在安全基线页面提供基线策略的设置、周期性检测和指定策略的一键检测功能，支持查看基线策略的通过率和风险状况，以及基线检测结果列表，并可查看基线和检测项详情信息及修复方案，可对指定服务器检测项进行忽略。



基线策略

基线策略是基于用户自定义设置的基线检测项的集合，基于策略维度了解基线的通过率及风险情况。

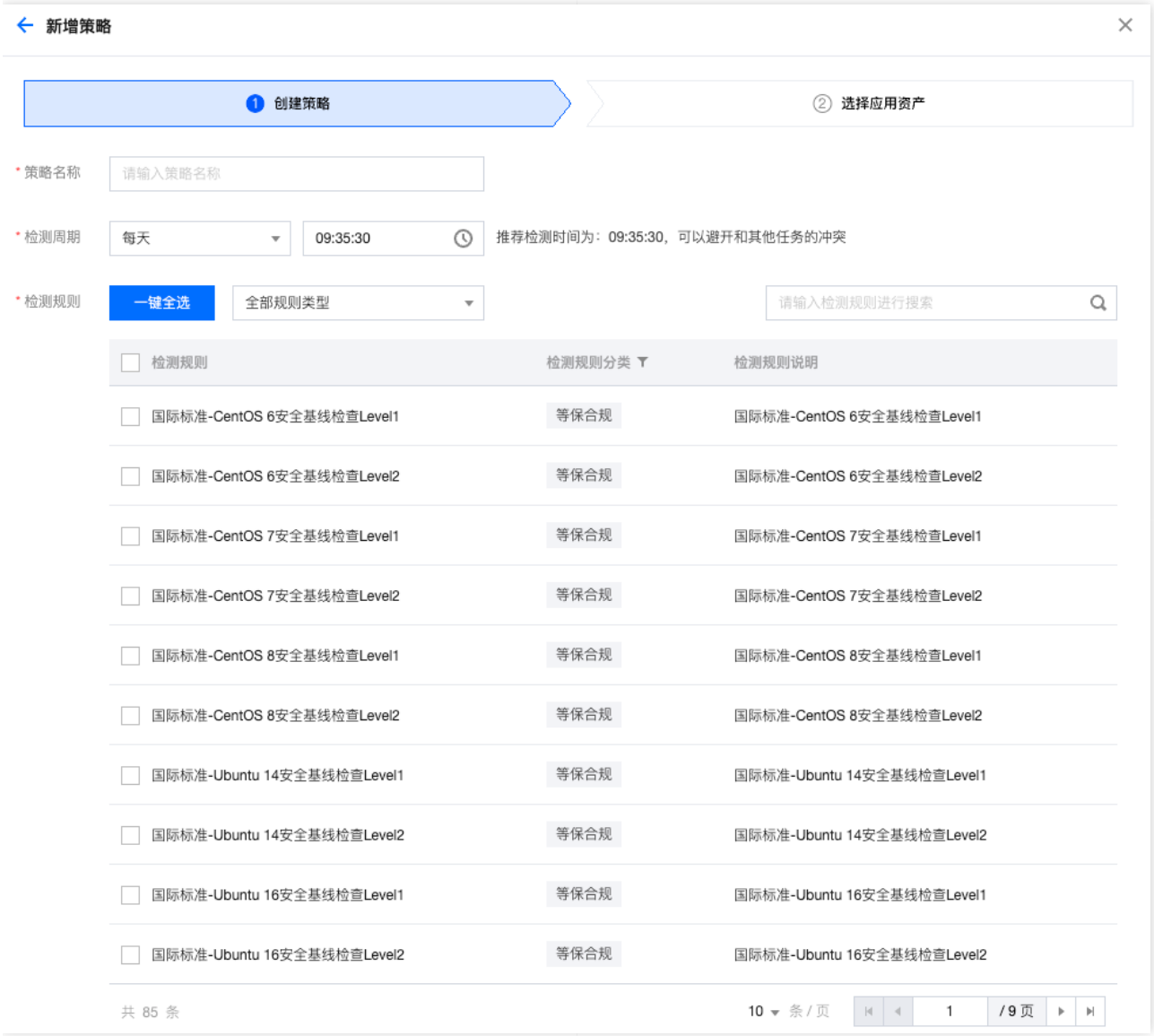
- 云平台默认基线策略：云平台主机安全根据网络安全主流的基线检测内容为您提供默认基线检测策略，包括：国际标准基线、弱密码、未授权访问、等保二级、等保三级、云安全标准策略。您可以增加默认基线策略中的检测项和需要检测的服务器，该策略默认每隔7天，第7天晚上0点检测全量专业版或旗舰版服务器。
- 新增基线策略

1. 在安全基线页面右上角，单击【基线检测设置】。
2. 在【检测策略设置】中，单击【新增策略】。



3. 在新增策略弹窗中，输入策略名称（不允许与现存策略名称重复）、选择检测周期、基线选项及应用资产，单击【保存】并更新。

> 说明：
>
> 主机安全最多支持创建20个基线策略，达到20个后则不允许再创建，但您可以删除现有基线后，再次创建。



基线检测

主机安全支持对基线检测项的定期检测和一键检测，支持对指定云服务器上的指定基线项进行检测。

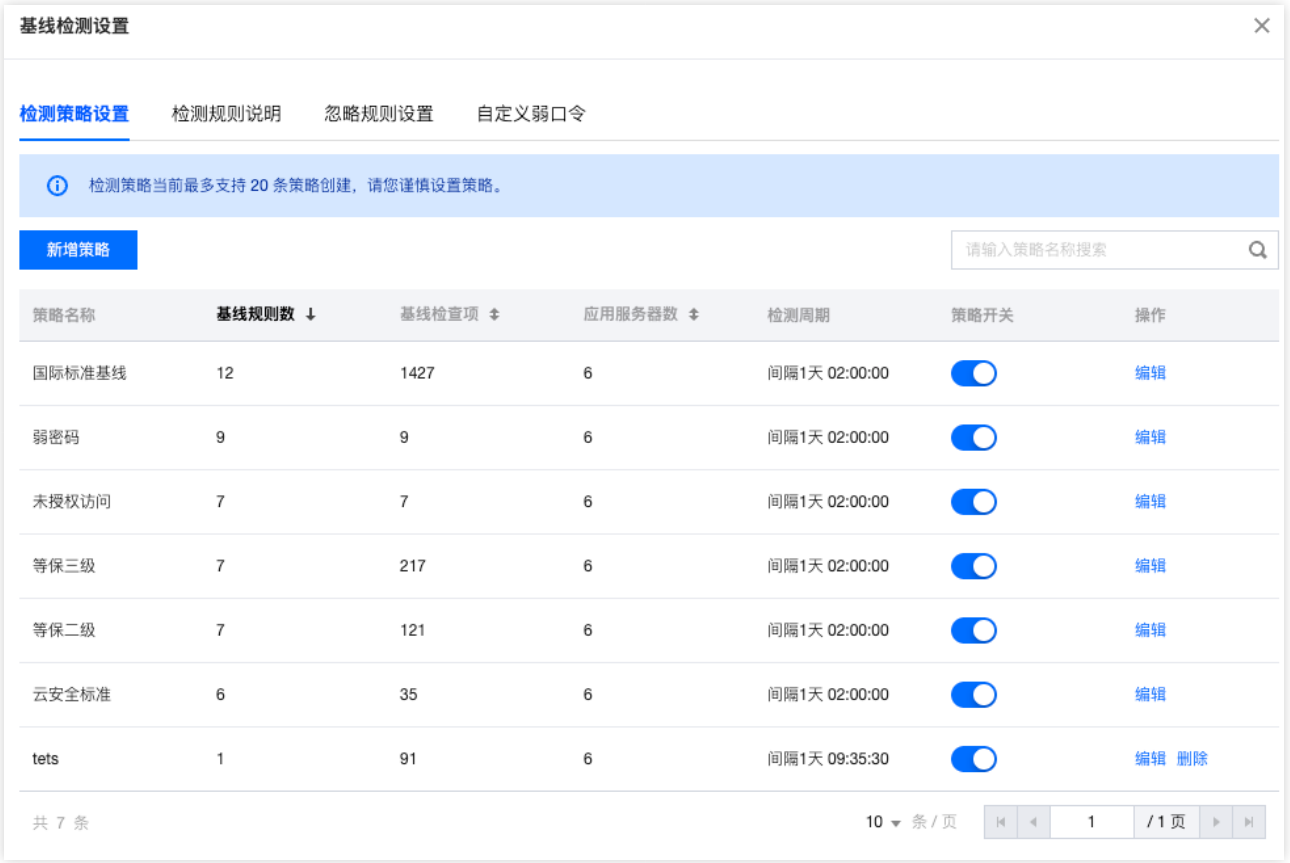
- 一键检测
  1.单击【一键检测】，选择需要检测的基线策略下发检测（检测一般持续2 - 5分钟），检测完成后，检测结果会显示在安全基线页下方。





- 周期检测

1. 在安全基线页右上角，单击【基线检测设置】。
2. 在检测策略设置中，可以进行周期检测设置。



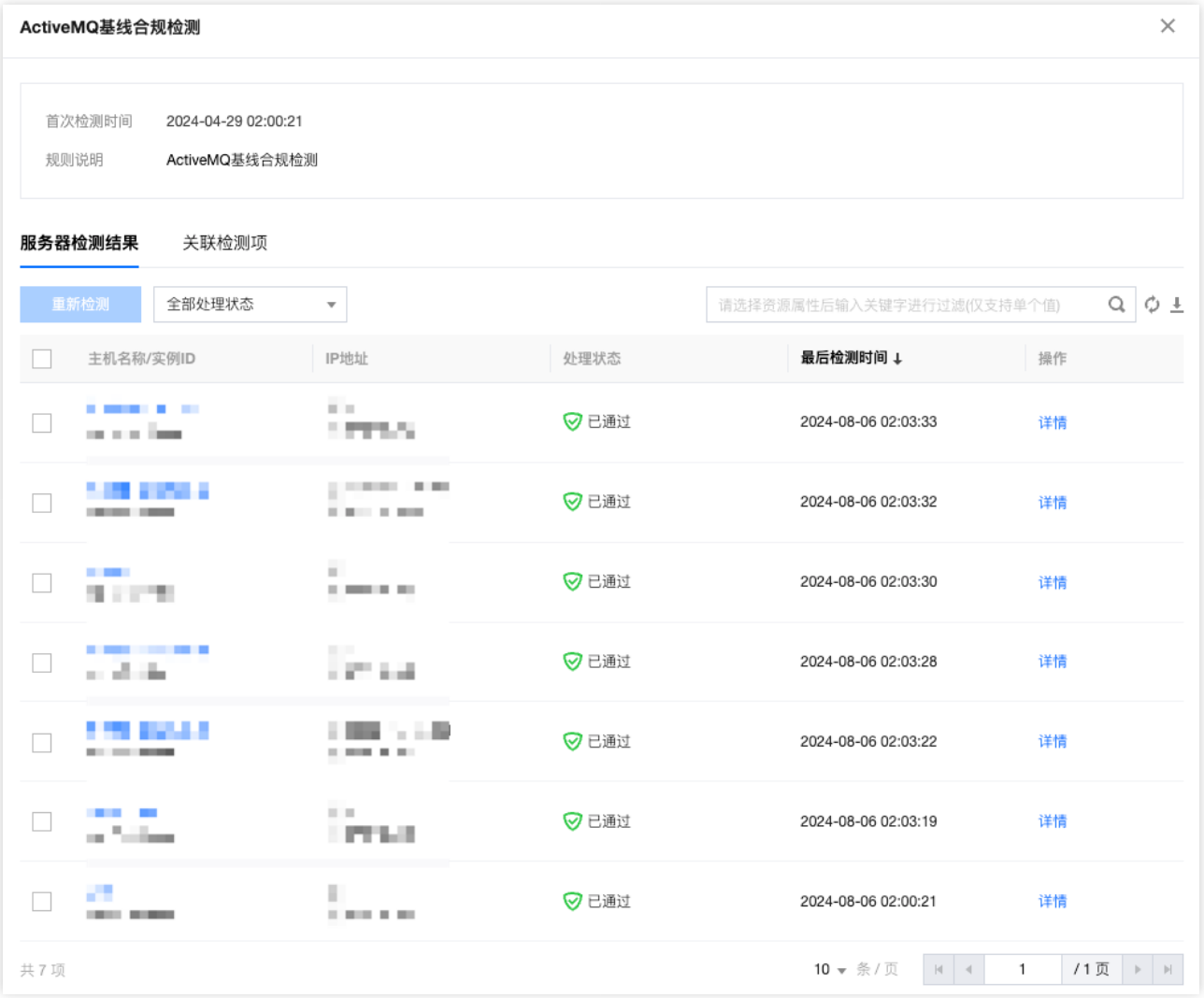
基线检测结果列表

在安全基线页面下方，可查看基线检测结果列表，支持查看基线检测详情，支持对单个基线进行模糊搜索和状态筛选，并支持对所有表格进行下载。



字段说明：

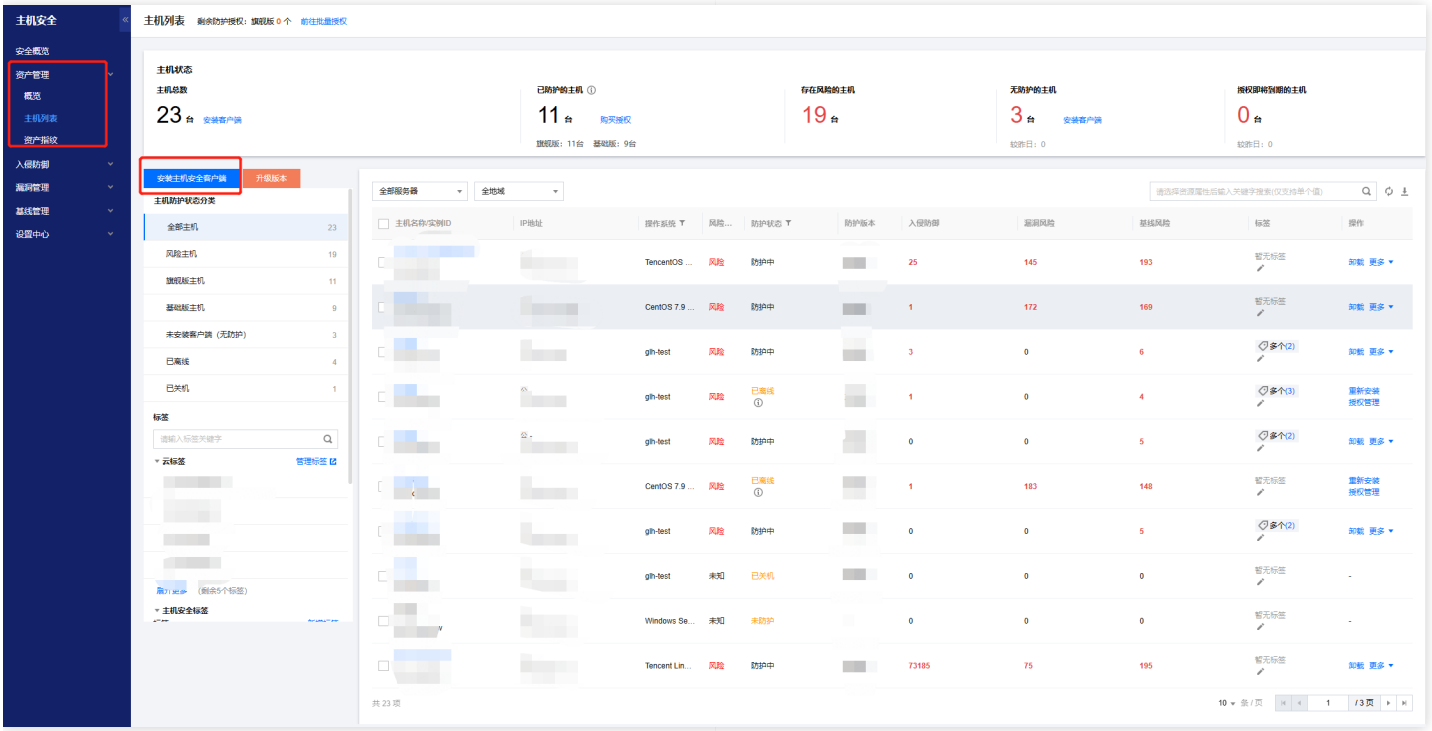
- 检测规则名称：基线检测规则名称，包含若干相同类别的检测项。
- 具体检测项：该检测规则下所有的检测项合计数量。
- 检测服务器数：该检测规则检测过的服务器数量。
- 最后检测时间：最近一次进行该检测规则检测的时间。
- 处理状态：未通过、已通过。
- 操作：
    - 重新检测：可重新对该检测规则进行检测。
    - 查看详情：可查看服务器检测结果和关联检测项。
    - 忽略：忽略选中的检测规则。


ActiveMQ基线合规检测
首次检测时间 2024-04-29 02:00:21
规则说明 ActiveMQ基线合规检测
服务器检测结果
关联检测项
重新检测
全部处理状态
请选择资源属性后输入关键字进行过滤(仅支持单个值)
主机名称/实例ID
IP地址
处理状态
最后检测时间
操作
已通过 2024-08-06 02:03:33 详情
已通过 2024-08-06 02:03:32 详情
已通过 2024-08-06 02:03:30 详情
已通过 2024-08-06 02:03:28 详情
已通过 2024-08-06 02:03:22 详情
已通过 2024-08-06 02:03:19 详情
已通过 2024-08-06 02:00:21 详情
共 7 项
10 条 / 页
1
/ 1 页

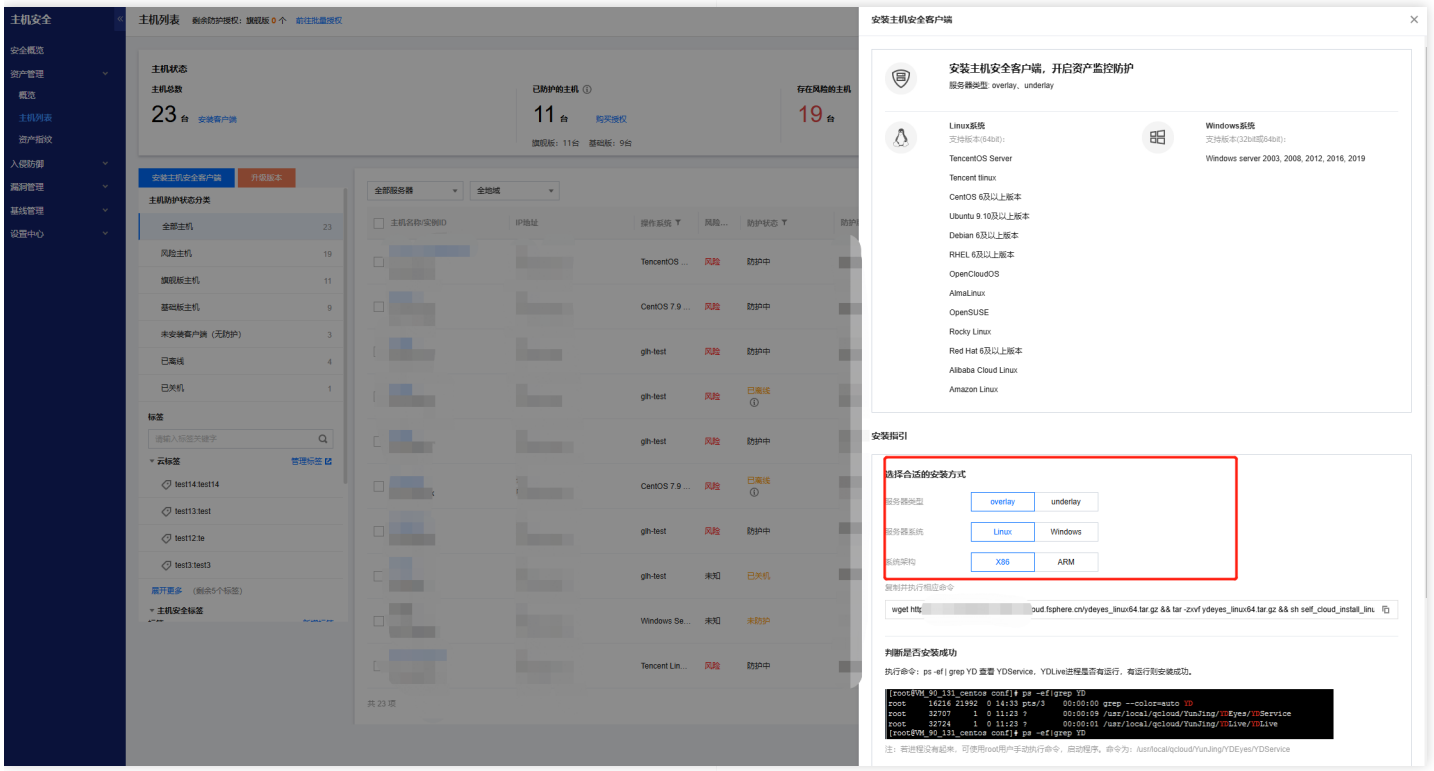
常用操作

未防护主机安装agent

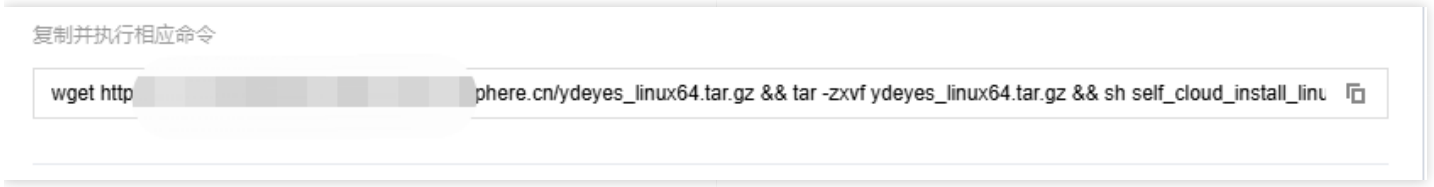
1。登录主机安全租户端，资产管理->主机列表->安装主机安全客户端。



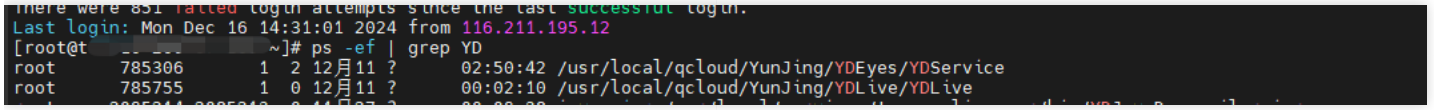
2.根据所安装机器的架构与类型选择合适的安装链接。



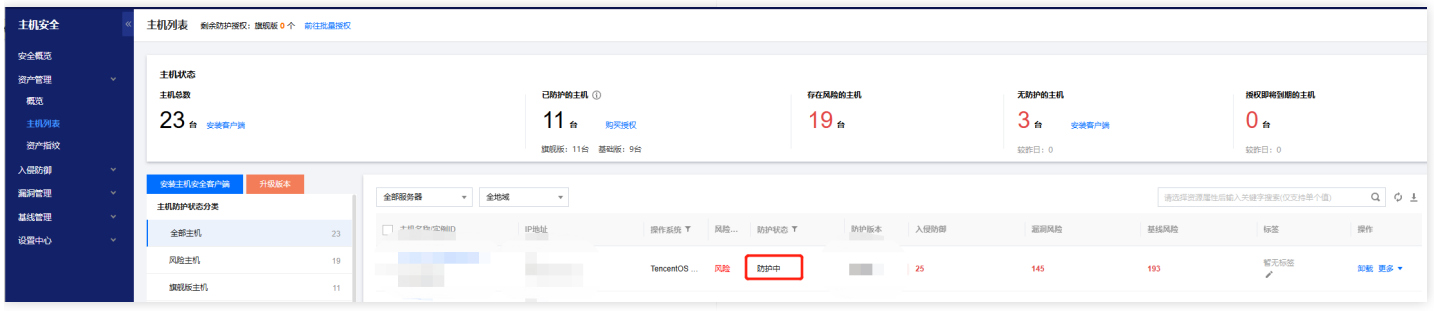
3.复制主机安全agent安装的链接登录到机器上用root权限执行。



4.执行完成后执行ps-ef | grep YD查看主机安全agent是否正常启动。

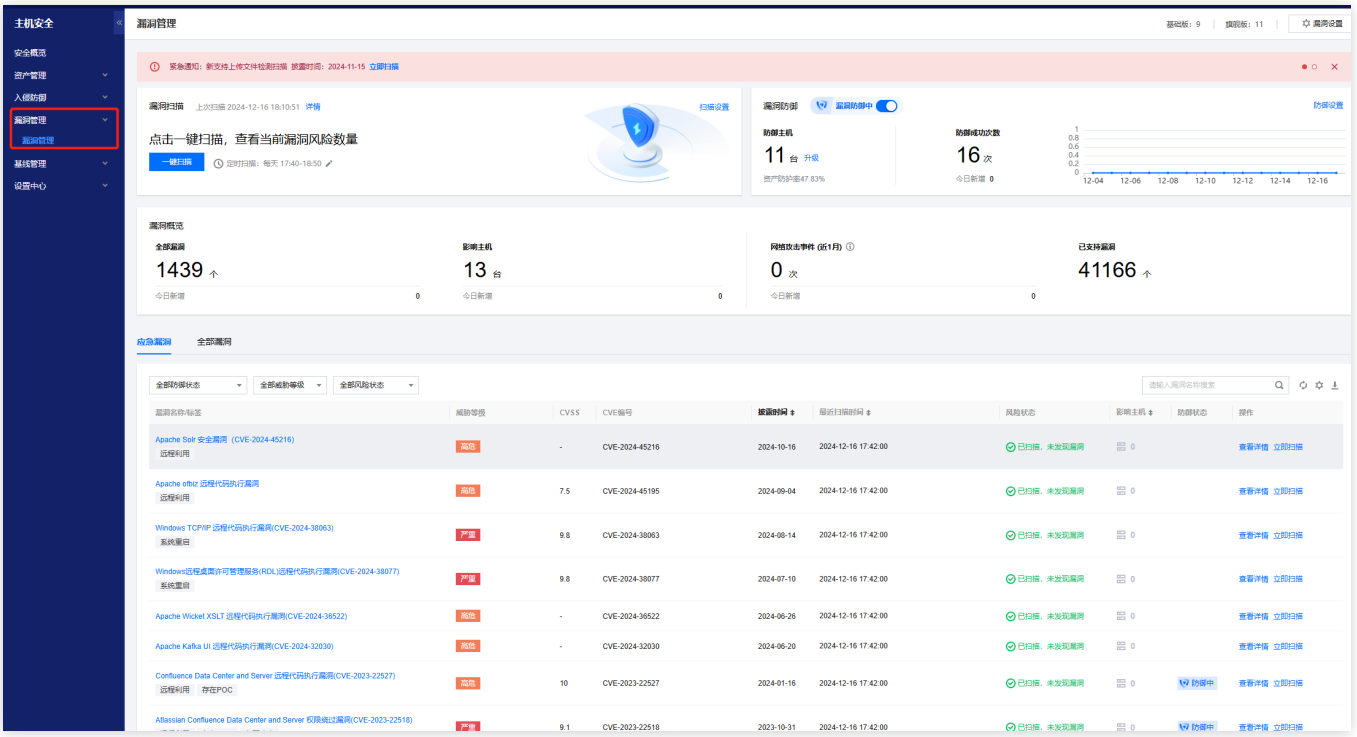


5.查看到机器成功上线之后可以在主机安全租户端看到机器状态显示防护中。

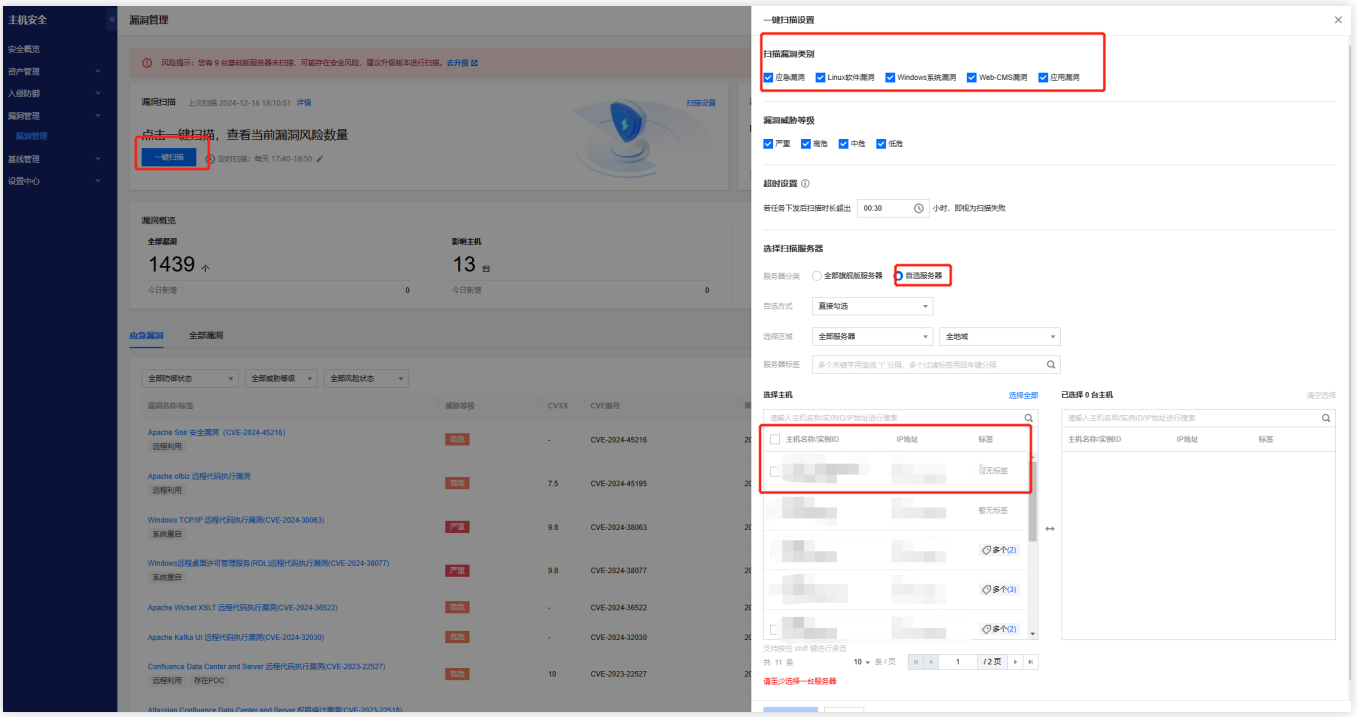


单台主机漏洞扫描

1. 登录主机安全租户端->漏洞管理->漏洞管理。



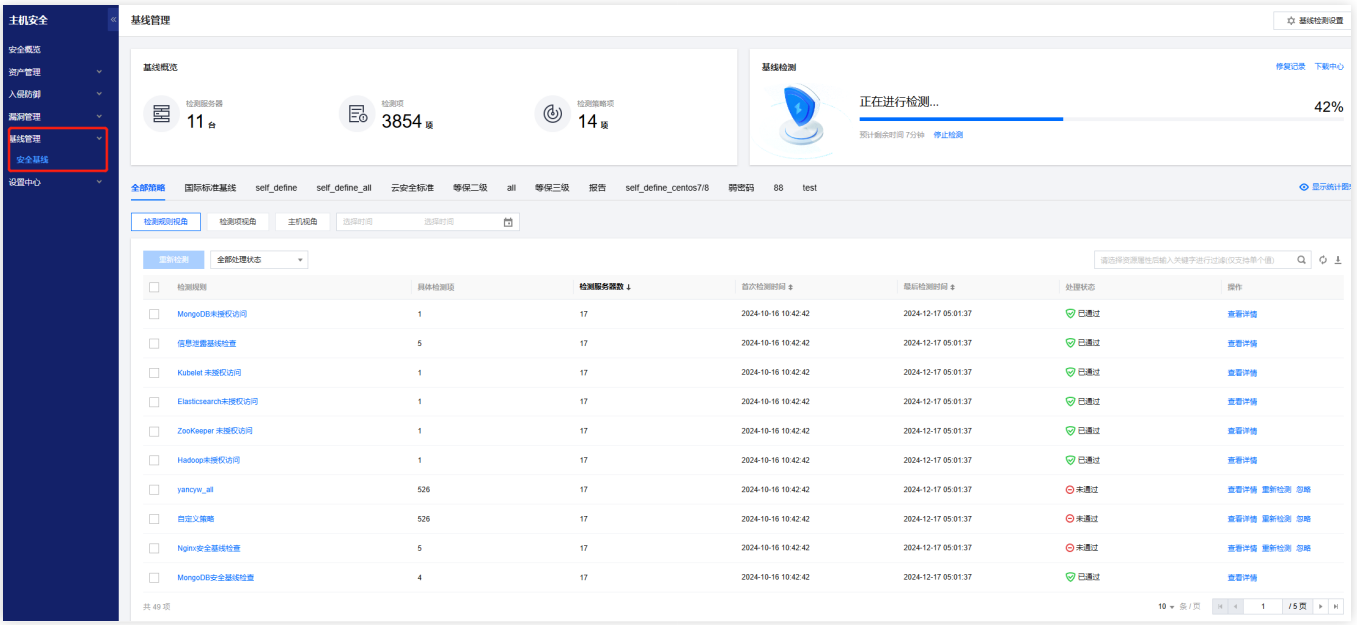
2. 点击一键扫描->勾选需要扫描的漏洞类型->自选服务器



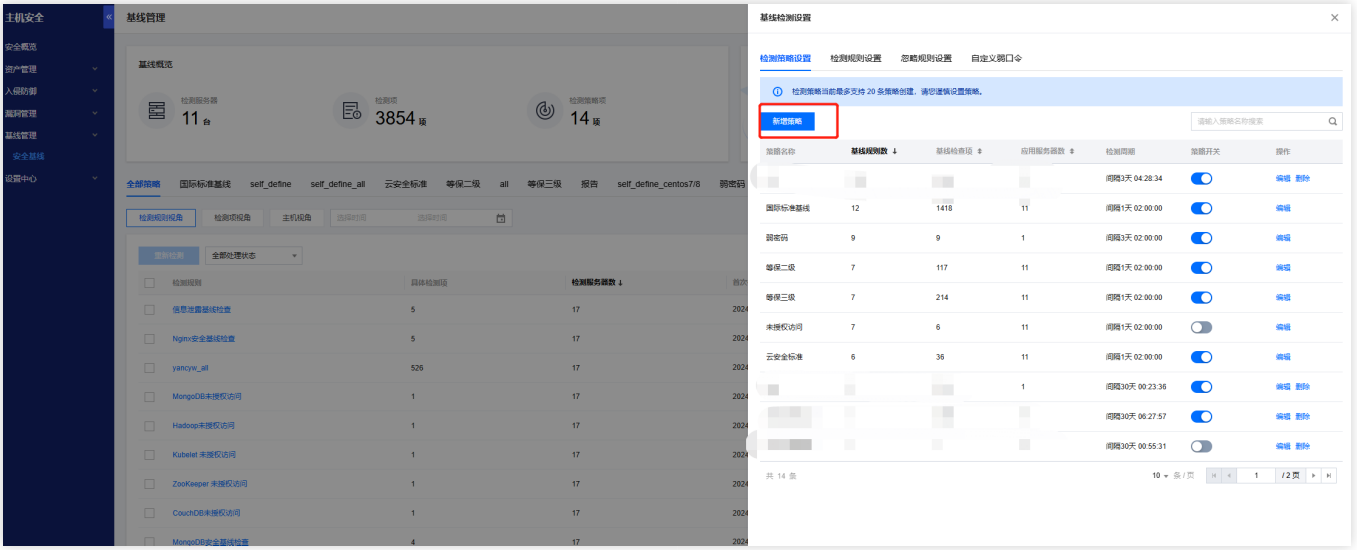
3. 全部配置完成后点击下方一键扫描即可完成单台机器漏洞扫描。

单台主机基线扫描

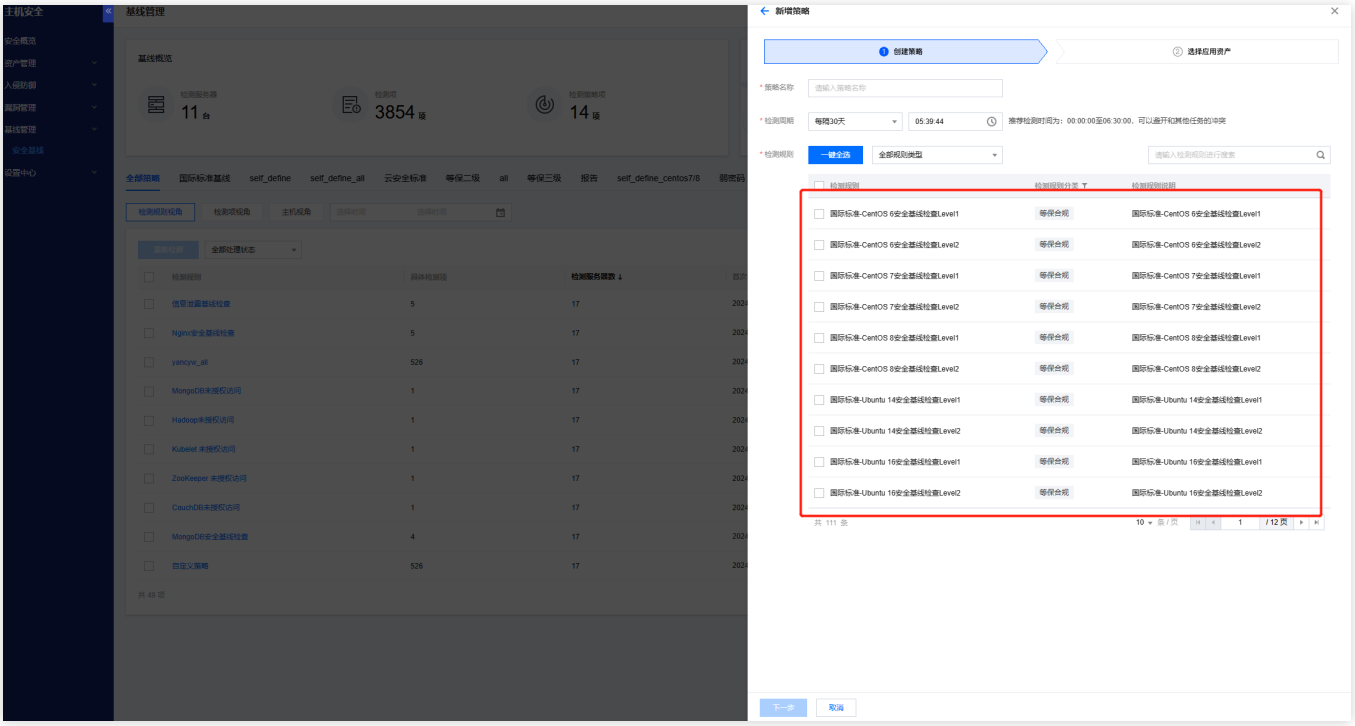
1. 登录主机安全租户端->基线管理->安全基线。



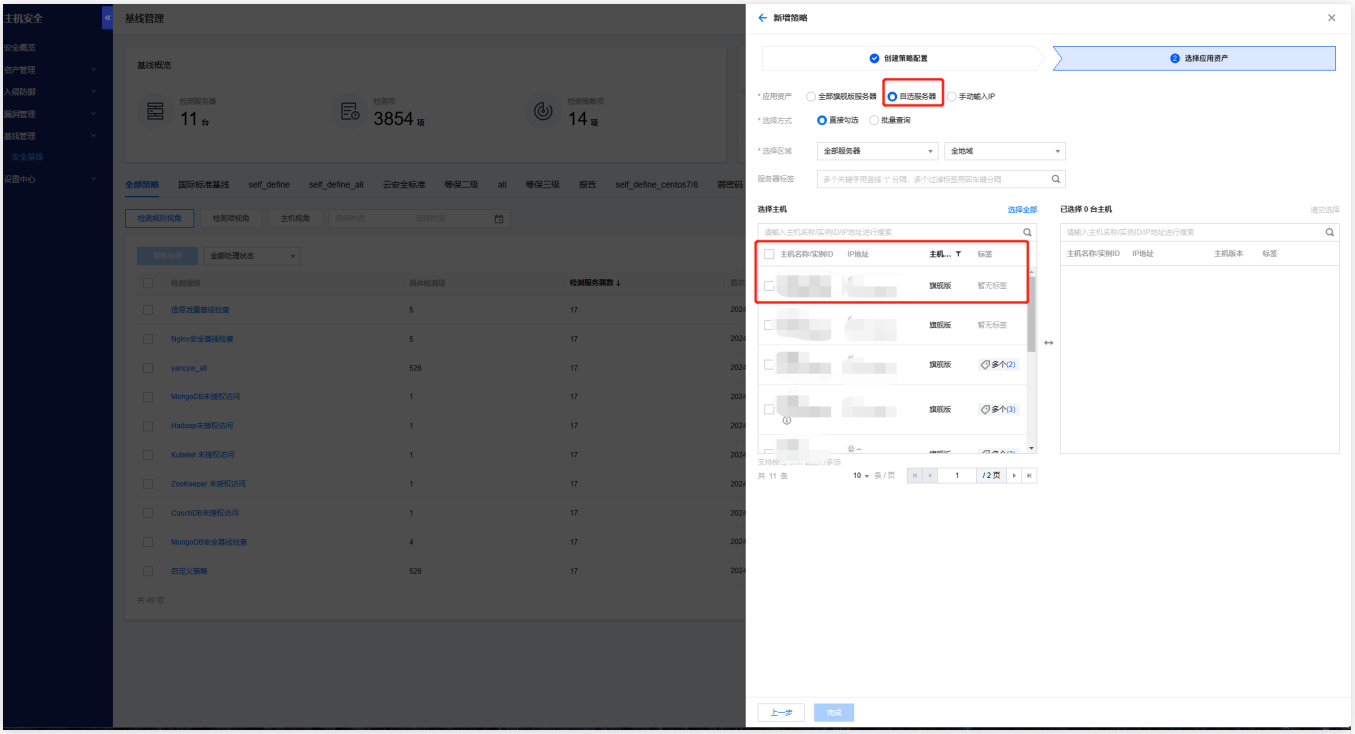
2. 点击右上角基线检测设置->选择新增策略。



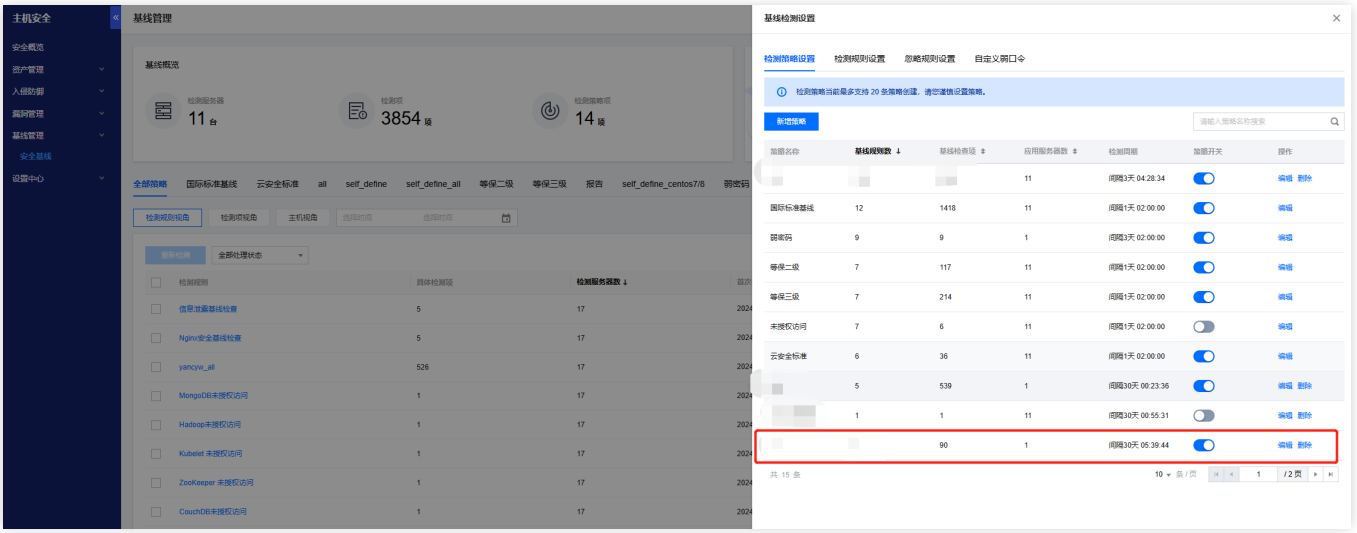
3. 在新增策略页面选择需要勾选的基线检测项。



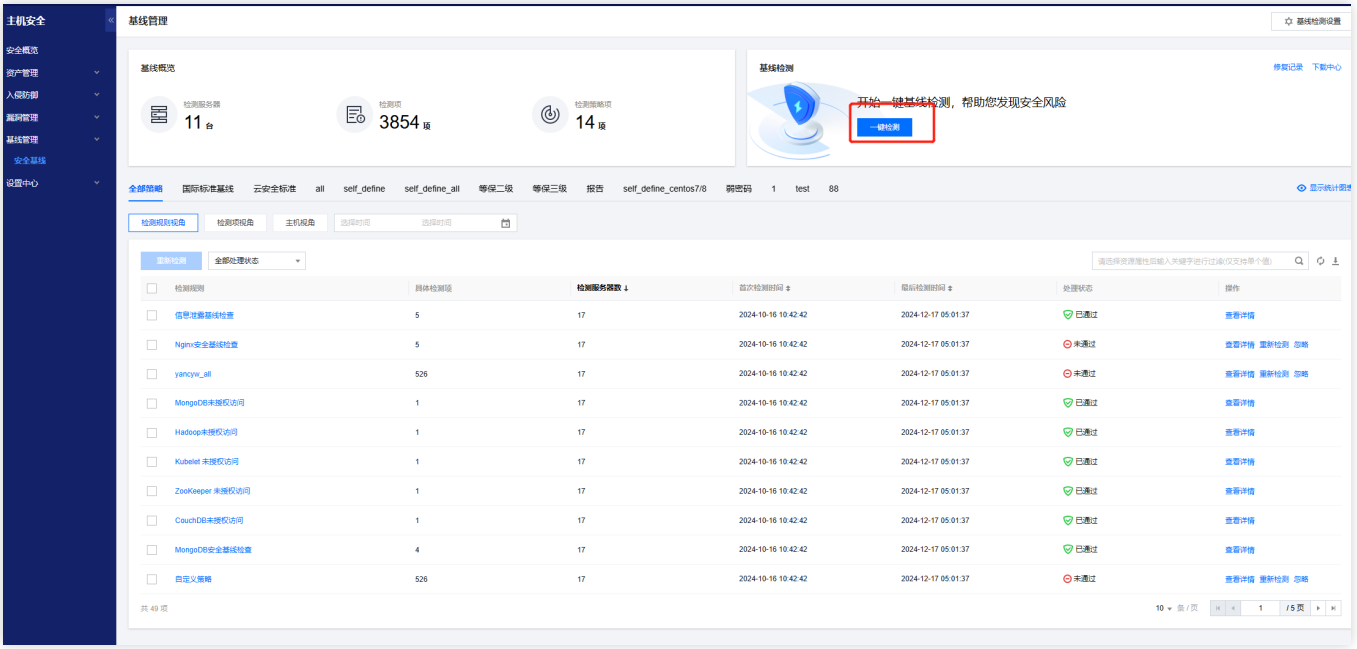
4. 勾选完成后点击下一步，选择需要策略应用的主机。



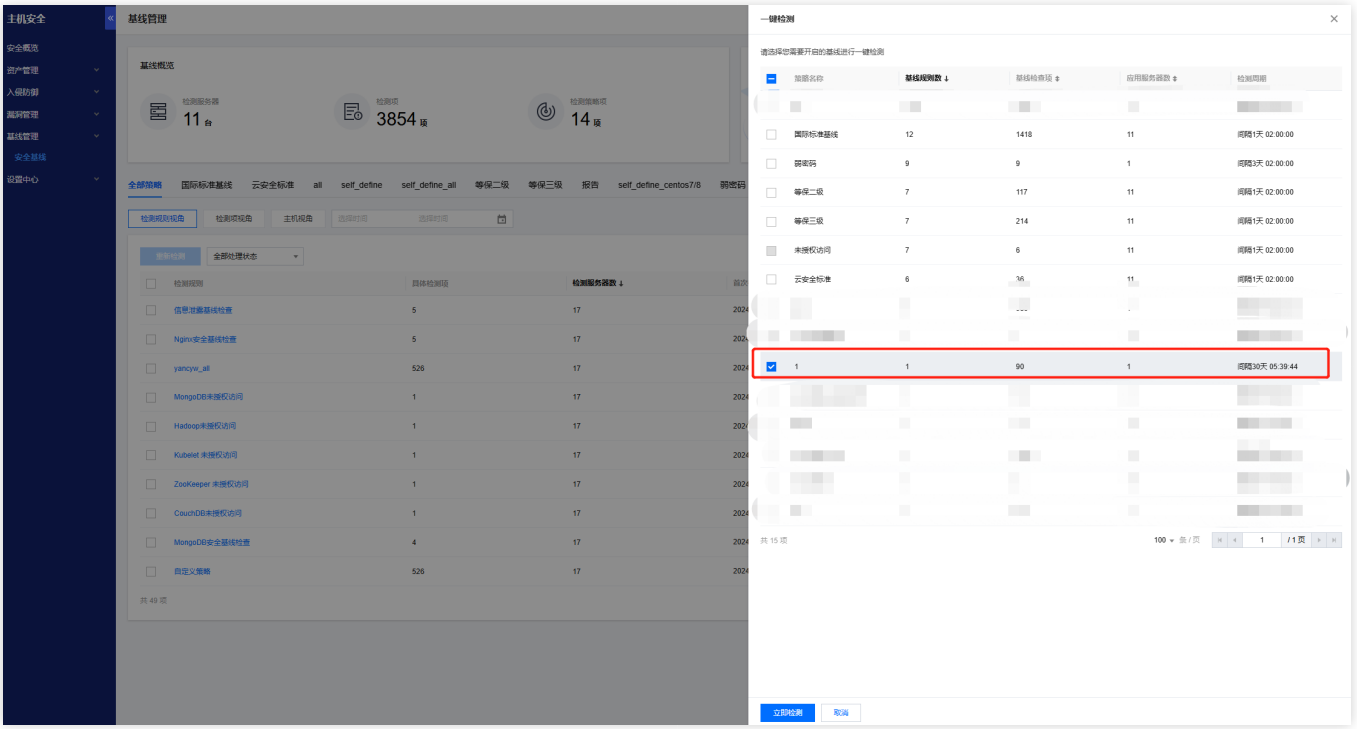
5. 点击下一步策略创建成功，会自动返回到基线检测设置页面，可以看到刚刚新创建的策略已经展示。



6. 返回到安全基线页面，点击一键检测。



7. 选择我们刚刚创建的基线检测策略。



点击立即检测回立刻开始执行基线扫描。

故障处理
Linux入侵类问题排查思路

本文档将指导您如何排查 Linux 入侵类问题并提供被入侵后的安全优化建议。

> 说明：
>
> 若已明确入侵事件属于挖矿或木马，请按 挖矿木马自助清理手册 进行处置。

深入分析，查找入侵原因

一、检查隐藏账户及弱口令

1. 检查服务器系统及应用账户是否存在弱口令：
   - 检查说明：检查管理员账户、数据库账户、MySQL 账户、tomcat 账户、网站后台管理员账户等密码设置是否较为简单，简单的密码很容易被黑客破解。
   - 解决方法：以管理员权限登录系统或应用程序后台，修改为复杂的密码。
   - 风险性：高。
2. 使用 last 命令查看下服务器近期登录的账户记录，确认是否有可疑 IP 登录过机器：
   - 检查说明：攻击者或者恶意软件往往会往系统中注入隐藏的系统账户实施提权或其他破坏性的攻击。
   - 解决方法：检查发现有可疑用户时，可使用命令 usermod -L 用户名 禁用用户或者使用命令 userdel -r 用户名 删除用户。
   - 风险性：高。
3. 通过 less /var/log/secure|grep 'Accepted' 命令，查看是否有可疑 IP 成功登录机器：
   - 检查说明：攻击者或者恶意软件往往会往系统中注入隐藏的系统账户实施提权或其他破坏性的攻击。
   - 解决方法：使用命令 usermod -L 用户名 禁用用户或者使用命令 userdel -r 用户名 删除用户。
   - 风险性：高。
4. 检查系统是否采用默认管理端口：

   - 检查系统所用的管理端口（SSH、FTP、MySQL、Redis® 等）是否为默认端口，这些默认端口往往被容易自动化的工具进行暴破成功。

   - 解决方法：
     a.在服务器内编辑 /etc/ssh/sshd_config 文件中的 Port 22，将22修改为非默认端口，修改之后需要重启 ssh 服务。

     > 注意：
     >
     > 当对端口进行修改时，需同时在云服务器控制台上修改对应主机的安全组配置，在其入站规则中，放行对应端口。

b.运行/etc/init.d/sshd restart（CentOS）或 /etc/init.d/ssh restart（Debian / Ubuntu）命令重启使配置生效。
c.修改 FTP、MySQL、Redis® 等的程序配置文件的默认监听端口21、3306、6379为其他端口。
d.限制远程登录的 IP，编辑/etc/hosts.deny 、/etc/hosts.allow两个文件来限制 IP。

- 风险性：高。

5. 检查/etc/passwd文件，看是否有非授权账户登录：
   - 检查说明：攻击者或者恶意软件往往会往系统中注入隐藏的系统账户实施提权或其他破坏性的攻击。
   - 解决方法：使用命令 usermod -L 用户名禁用用户或者使用命令 userdel -r 用户名删除用户。
   - 风险性：中。

二、检查恶意进程及非法端口

1. 运行 netstat -antp ，查看服务器是否有未被授权的端口被监听，查看下对应的 pid。
   - 检查服务器是否存在恶意进程，恶意进程往往会开启监听端口，与外部控制机器进行连接。
   - 解决方法：若发现有非授权进程，运行 ls -l /proc/$PID/exe 或 file /proc/$PID/exe （$PID 为对应的 pid 号），查看下 pid 所对应的进程文件路径。
     如果为恶意进程，删除对应的文件即可。
   - 风险性：高。
2. 使用 ps -ef 和 top 命令查看是否有异常进程
   - 检查说明：运行以上命令，当发现有名称不断变化的非授权进程占用大量系统 CPU 或内存资源时，则可能为恶意程序。
   - 解决方法：确认该进程为恶意进程后，可以使用 kill -9 进程名 命令结束进程，或使用防火墙限制进程外联。
   - 风险性：高。

三、检查恶意程序和可疑启动项

1. 使用 chkconfig --list 和 cat /etc/rc.local 命令，查看开机启动项中是否有异常的启动服务。
   - 检查说明：恶意程序往往会添加在系统的启动项，在用户关机重启后再次运行。
   - 解决方法：如发现有恶意进程，可使用 chkconfig 服务名 off 命令关闭，同时检查 /etc/rc.local 中是否有异常项目，如有请注释掉。
   - 风险性：高。
2. 进入 cron 文件目录，查看是否存在非法定时任务脚本。
   - 检查说明：查看 /etc/crontab ， /etc/cron.d ， /etc/cron.daily ， cron.hourly/ ， cron.monthly ， cron.weekly/ 是否存在可疑脚本或程序。
   - 解决方法：如发现有不认识的计划任务，可定位脚本确认是否正常业务脚本，如果非正常业务脚本，可直接注释掉任务内容或删除脚本。
   - 风险性：高。

四、检查第三方软件漏洞

1. 如果您服务器内有运行 Web、数据库等应用服务，请您限制应用程序账户对文件系统的写权限，同时尽量使用非 root 账户运行。
   - 检查说明：使用非 root 账户运行，可以保障在应用程序被攻陷后，攻击者无法立即远程控制服务器，减少攻击损失。
   - 解决方法：进入 web 服务根目录或数据库配置目录。
     运行 chown -R apache:apache /var/www/xxxx 、 chmod -R 750 file1.txt 命令配置网站访问权限。
   - 风险性：中。
   - 具体参考下方网站目录文件权限示例。
2. 升级修复应用程序漏洞
   - 检查说明：机器被入侵，部分原因是系统使用的应用程序软件版本较老，存在较多的漏洞而没有修复，导致可以被入侵利用。
   - 解决方法：比较典型的漏洞例如 ImageMagick、openssl、glibc 等，用户可以根据已发布的安全通告指导或通过 apt-get/yum 等方式进行直接升级修复。
   - 风险性：高。

网站目录文件权限的参考示例如下：场景：
假设 HTTP 服务器运行的用户和用户组是 www，网站用户为 centos，网站根目录是 /home/centos/web 。
方法/步骤：

1. 我们首先设定网站目录和文件的所有者和所有组为 centos，www，如下命令：

```
chown -R centos:www /home/centos/web
```

2. 设置网站目录权限为750，750是 centos 用户对目录拥有读写执行的权限，设置后，centos 用户可以在任何目录下创建文件，用户组有有读执行权限，这样才能进入目录，其它用户没有任何权限。

```
find -type d -exec chmod 750 {} \;
```

3. 设置网站文件权限为640，640指只有 centos 用户对网站文件有更改的权限，HTTP 服务器只有读取文件的权限，无法更改文件，其它用户无任何权限。

```
find -not -type d -exec chmod 640 {} \;
```

4. 针对个别目录设置可写权限。例如，网站的一些缓存目录就需要给 HTTP 服务有写入权限、discuz x2 的 /data/ 目录就必须要写入权限。

```
find data -type d -exec chmod 770 {} \;
```

被入侵后的安全优化建议

- 推荐使用 SSH 密钥进行登录，减少暴力破解的风险。
- 在服务器内编辑 /etc/ssh/sshd_config 文件中的 Port 22，将 22 修改为其他非默认端口，修改之后重启 SSH 服务。可使用如下命令重启：

/etc/init.d/sshd restart（CentOS）或 /etc/init.d/ssh restart（Debian/Ubuntu）

> 注意：
>
> 当修改端口时，需同时在云服务器控制台上修改对应主机安全组配置，在其入站规则中放行对应端口。

- 如果必须使用 SSH 密码进行管理，选择一个好密码。
- 无论应用程序管理后台（网站、中间件、tomcat 等）、远程 SSH、远程桌面、数据库，都建议设置复杂且不一样的密码。
- 下面是一些好密码的实例（可以使用空格）：
  1qtwo-threeMiles3c45jia`` caser, lanqiu streets
- 下面是一些弱口令的示例，可能是您在公开的工作中常用的词或者是您生活中常用的词：
  公司名+日期（coca-cola2016xxxx）
  常用口语（Iamagoodboy）
- 使用以下命令检查主机有哪些端口开放，关闭非业务端口。

netstat -antp

- 通过安全组防火墙限制仅允许制定 IP 访问管理或通过编辑 /etc/hosts.deny 、 /etc/hosts.allow 两个文件来限制 IP。
- 应用程序尽量不使用 root 权限。
- 例如 Apache、Redis®、MySQL、Nginx 等程序，尽量不要以 root 权限的方式运行。
- 修复系统提权漏洞与运行在 root 权限下的程序漏洞，以免恶意软件通过漏洞提权获得 root 权限传播后门。
- 及时更新系统或所用应用程序的版本，如 Struts2、Nginx，ImageMagick、Java 等。
- 关闭应用程序的远程管理功能，如 Redis®、NTP 等，如果无远程管理需要，可关闭对外监听端口或配置。
- 定期备份云服务器业务数据。
- 对重要的业务数据进行异地备份或云备份，避免主机被入侵后无法恢复。
- 除了您的 home，root 目录外，您还应当备份 /etc 和可用于取证的 /var/log 目录。
- 安装主机安全 Agent，在发生攻击后，可以了解自身风险情况。

  > 说明：
  >
  > 如果以上步骤均不能排查出来问题，建议您联系运维人员进行处理。

Windows入侵类问题排查思路

本文档将指导您如何排查 Windows 入侵类问题。

深入分析，查找入侵原因

一. 检查帐户和弱口令

1. 查看服务器已有系统或应用帐户是否存在弱口令。
   - 检查说明：主要检查系统管理员帐户、网站后台帐户、数据库帐户以及其他应用程序（FTP、Tomcat、phpMyAdmin 等）帐户是否存在弱口令。

     > 说明：
     >
     > 帐户密码建议设置为大写、小写、特殊字符、数字组成的12 - 16位的复杂密码 ，也可使用密码生成器自动生成复杂密码。

   - 检查方法：根据实际情况自行确认。
   - 风险性：高。
2. 查看下服务器内是否有非系统和用户本身创建的账户。
   - 检查说明：一般黑客创建的异常账户账户名会在本地用户组显示出来。
   - 检查方法：打开 cmd 窗口，输入 lusrmgr.msc 命令，查看是否有新增的账户，如有管理员群组的（Administrators）里的新增账户，请立即禁用或删除掉。
   - 风险性：高。
3. 检查是否存在隐藏账户名。
   - 检查说明：黑客为了逃避检查，往往会在您服务器内创建隐藏账户，隐藏账户在本地用户内是查看不到的。
   - 检查方法（您也可以通过下载 LP_Check 安全工具检查是否有隐藏账户）：
     a.在桌面打开运行（可使用快捷键 Win + R），输入 regedit，即可打开注册表编辑器。
     b.选择 HKEY_LOCAL_MACHINE/SAM/SAM，默认无法查看该选项内容，右键菜单选择权限，打开权限管理窗口。
     c.选择当前用户（一般为 Administrator），将权限勾选为完全控制，然后确定，关闭注册表编辑器。
     d.再次打开注册表编辑器，即可选择 HKEY_LOCAL_MACHINE/SAM/SAM/Domains/Account/Users。
     e.在 Names 项下可以看到实例所有用户名，如出现本地账户中没有的账户，即为隐藏账户，在确认为非系统用户的前提下，可删除此用户。
   - 风险性：高。

二. 检查恶意进程和端口

1. 检查是否存在恶意进程在系统后台运行。
   - 检查说明：攻击者在入侵系统后，往往会运行恶意进程与外部进行通信，通过分析外联的进程，即可以找出入侵的控制进程。
   - 检查方法：

     a.登录服务器，选择开始 > 运行。

     b.输入 cmd ，然后输入 netstat –nao 查看下服务器是否有未被授权的端口被监听。

     c.打开任务管理器，检查对应的 PID 进程号所对应的进程是否为正常进程，例如通过 PID 号查看下运行文件的路径，删除对应路径文件，您也可以通过微软官方提供的 Process Explorer 工具进行排查。
   - 风险性：高。

三. 检查恶意程序及启动项

1. 检查服务器内部是否有异常的启动项。
   - 检查说明：攻击者在入侵系统后，往往会把恶意程序放到启动项中开机执行。
   - 检查方法：

     a.登录服务器，选择开始 > 所有程序>启动。

     b.默认情况下此目录在是一个空目录，确认是否有非业务程序在该目录下。

     c.选择开始 > 运行，输入 msconfig ，查看是否存在命名异常的启动项目，若存在则取消勾选命名异常的启动项目，并到命令中显示的路径删除文件。

     d.选择开始 > 运行，输入 regedit ，打开注册表，查看开机启动项是否正常，特别注意如下三个注册表项：

     HKEY_CURRENT_USER\software\micorsoft\windows\currentversion\run

     HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

     HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce

     检查注册表右侧是否有启动异常的项目，如有请删除，并建议安装杀毒软件进行病毒查杀，清除残留病毒或木马。
   - 风险性：高。

2. 查看正在连接的会话。
   - 检查说明：检查服务器与网络上的其它服务器之间的会话或计划任务。
   - 检查方法：

     a.登录服务器，选择开始 > 运行。

     b.输入 cmd ，然后输入 netstat -ano ，检查服务器与网络上的其它服务器之间的会话，并确认是否为正常连接。输入 schtasks，检查服务器中的计划任务，并确认是否为正常的计划任务。
   - 风险性：中。

四. 检查第三方软件漏洞

1. 如果您服务器内有运行对外应用软件（WWW、FTP 等），请您对软件进行配置，限制应用程序的权限，禁止目录浏览或文件写权限。
2. 开通Web 应用防火墙 防护，查看 Web 应用防护攻击日志。

常见问题

如何恢复被入侵后的网站或系统？

系统确认被入侵后，往往系统文件会被更改和替换，此时系统已经变得不可信，最好的方法就是重新安装系统，同时给新系统安装所有补丁。

如何防止网站或系统被再次入侵？

1. 改变所有系统账户的密码为 复杂密码（至少与入侵前不一致）。
2. 修改默认远程桌面端口，操作如下：
    i. 选择开始 > 运行，然后输入 regedit 。
    ii. 打开注册表，进入如下路径：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp
    iii. KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Tenninal Server\WinStations\RDP-Tcp
    iv. 修改下右侧的 PortNumber 值。
3. 配置安全组防火墙只允许 指定 IP 才能访问远程桌面端口。
4. 定期备份重要业务数据和文件。
5. 定期更新操作系统及应用程序组件版本（如 FTP、Struts2 等），防止被漏洞利用。
6. 安装主机安全 Agent 和防病毒软件进行定期体检和扫描。

Linux 客户端离线排查

本文档将指导您进行 Linux 客户端离线排查，包括客户端进程未启动排查及网络故障排查。

客户端进程未启动排查

1. 请查询主机安全进程是否存在。输入： ps -ef|grep YD 。
   正常状态下，主机安全存在两个进程，如下图所示：

```
[root@VM_145_42_centos ~]# ps -ef|grep YD
root      9059     1  0 Oct30 ?        00:00:41 /usr/local/qcloud/YunJing/YDEyes/YDService
root     14340     1  0 Oct23 ?        00:00:58 /usr/local/qcloud/YunJing/YDLive/YDLive
```

- 如果进程不存在，可能存在以下情况：
- 服务器未安装主机安全或者客户端已被卸载，请根据 快速入门 安装指引，进行客户端安装。
- 客户端可能出现异常冲突或者崩溃，导致进程没有启动。

2. 若服务器已安装主机安全或者客户端，可采用以下方法排查客户端进程未启动原因：

- 可查看客户端日志，存放路径： /usr/local/qcloud/YunJing/log 。
- 可执行命令： sh /usr/local/qcloud/YunJing/startYD.sh 启动主机安全服务。

网络故障排查

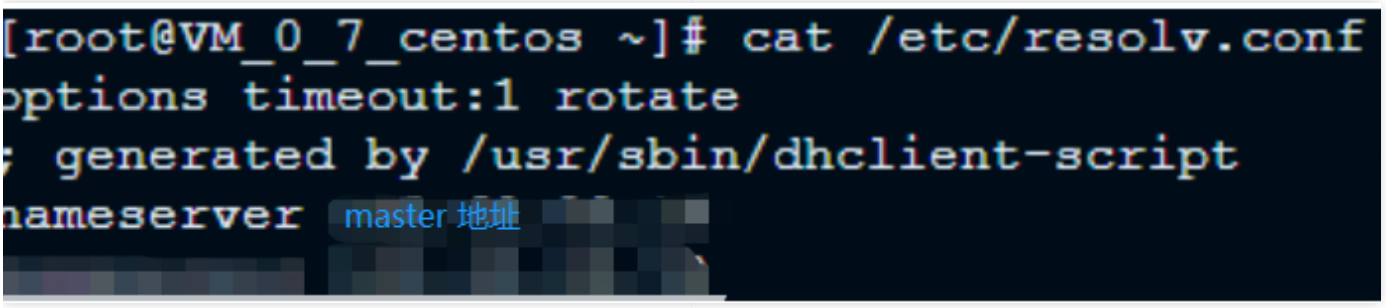
如果进程存在，但主机安全不在线，大部分原因是网络不通，请按照以下操作进行排查：

1. 如果无法访问主机安全域名，可以尝试修改 DNS。可以通过执行如下命令行，排查主机安全域名是否可以访问：
   - VPC 网络和裸金属云服务器环境： telnet s.yd.finance.cloud.tencent.com 5574 。
     正常情况下：返回如下图所示结果。



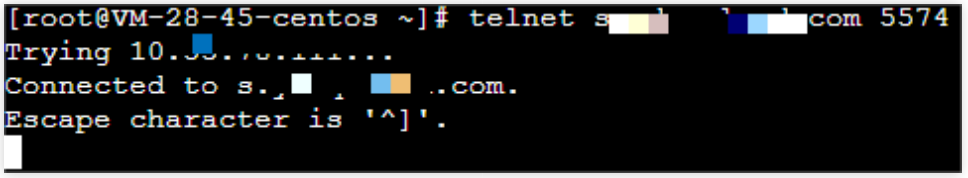
     如果无法访问：
     a. 可以尝试修改 dns nameserver 字段： vim /etc/resolv.conf``nameserver master地址

b. 修改完成后，重新执行 telnet s.yd.finance.cloud.tencent.com 5574 检测能否连通。



c. 如果可以连通，等待几分钟后（时间长短根据网络情况而定），控制台将能看到对应服务器重新上线。

- 基础网络环境（非 VPC 上的服务器）： telnet s.yd.finance.cloud.tencent.com 5574 。
  正常情况下：返回如下图所示结果。



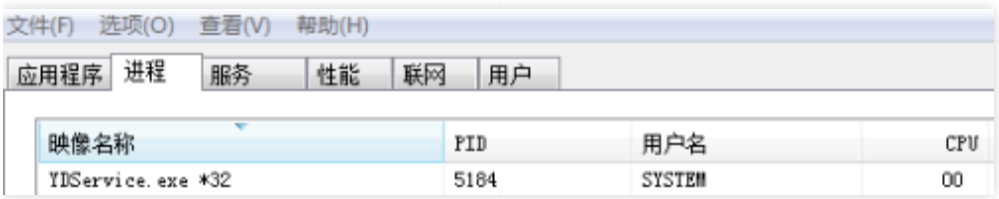
  如果无法访问：
  a. 可以尝试修改 dns nameserver 字段： vim /etc/resolv.conf ，先把原有的 nameserver 字段注释，再新增 nameserver 字段，具体的 nameserver ip 相关内容。
  b. 修改完成后，重新执行 telnet s.yd.finance.cloud.tencent.com 5574 检测能否连通。
  c. 如果可以连通，等待几分钟后（时间长短根据网络情况而定），控制台将能看到对应服务器重新上线。

2. 防火墙策略限制，需要在 Linux 客户端开放 TCP 端口：5574、8080、80、9080。
3. 如果主机安全进程存在，且不是由于网络原因导致的客户端离线，请打包客户端日志（日志路径： /usr/local/qcloud/YunJing/log ）并联系技术支持工程师进行反馈。

Windows 客户端离线排查

客户端进程未启动排查

请查询主机安全进程是否存在。
打开 Windows 任务管理器，查找名为 YDService.exe 的进程是否存在。



1. 如果进程不存在，可能存在以下情况：
   - 服务器未安装主机安全或者客户端已被卸载，请根据 快速入门 安装指引，进行客户端安装。
   - 客户端可能出现异常冲突或者崩溃，导致进程没有启动。
2. 排查方法：
   - 可查看客户端日志，存放路径： C:\Program Files\QCloud\YunJing\log 。
   - 可执行命令： sc start ydservice 手动运行客户端。

网络故障排查

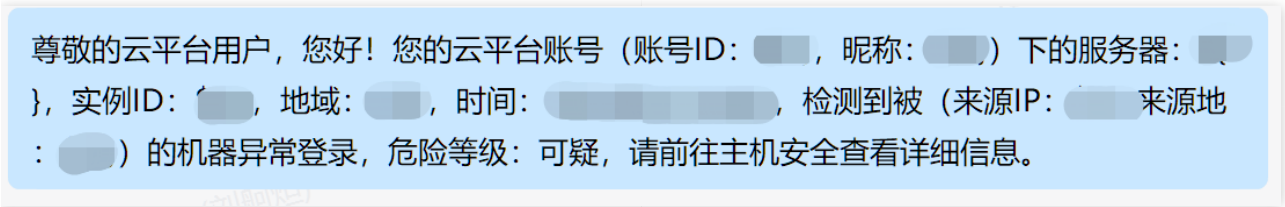
如果进程存在，但主机安全客户端不在线，大部分原因是网络不通，请按照以下操作进行排查：

1. 检查 DNS 是否被修改，可以通过执行如下命令行进行排查，只要其中一个返回正常结果，则表示 DNS 无问题：
   - 基础网络下载地址（非 VPC 服务器）： telnet s.yd.finance.cloud.tencent.com 5574 。
   - VPC 和裸金属云服务器下载： telnet s.yd.finance.cloud.tencent.com 5574。
2. 防火墙阻拦导致故障，需要开放5574、8080、80、9080端口。
3. 如果主机安全进程存在，且不是由于网络原因导致的客户端离线，请打包客户端日志（日志路径： C:\Program Files\QCloud\YunJing\log ）联系技术支持工程师进行反馈。

异常登录的消息提醒

现象描述

用户接收到服务器被异常登录的消息提醒，如下以短信消息为例：



可能原因

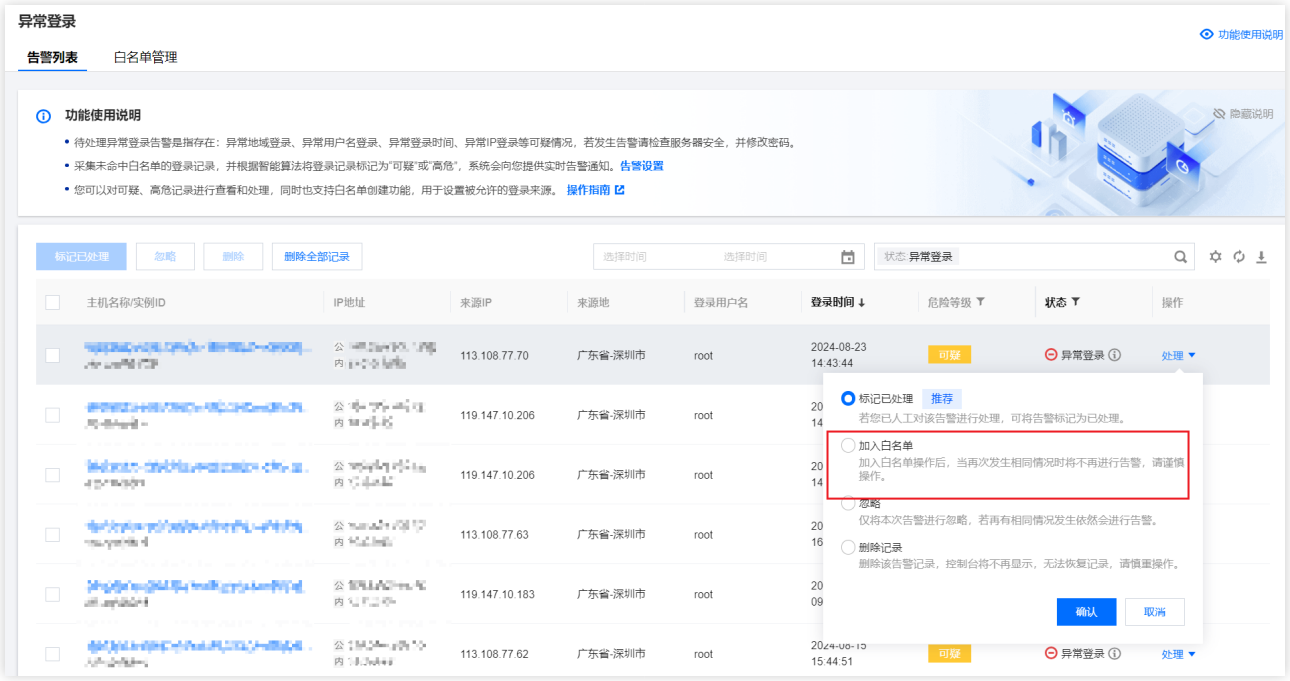
当您账号下的服务器有登录行为时，主机安全若发现本次登录没有命中登录白名单，会根据智能算法将该登录记录标记为“可疑”或“高危”，并触发实时告警提醒。

> 说明：
>
> - 默认仅告警危险等级为“高危”的异常登录事件，可通过【设置中心】> 【告警设置】勾选设置。
> - 异常登录危险等级是依托算法对服务器过往登录情况综合判定。

处理步骤

在收到的异常登录告警提醒后，请您按照下列步骤进行确认：

1. 请确认本次登录行为是否为合法登录。
    - 是，请将该登录记录加入白名单，后续该登录行为再次发生，不再产生告警。



- 否，请执行步骤2。

2. 确定为非法登录，初步判断您服务器告警的异常登录事件，是由于不常使用的用户被破解，建议您立即修改登录密码以及服务器上保存过的相关登录凭证。建议参考 Linux 入侵类问题排查思路 和 Windows 入侵类问题排查思路对服务器进行常规排查。

加固方法

后续您可以通过如下加固方法，以提高服务器安全性：

- 服务器设置大写、小写、特殊字符、数字组成的12-16位的复杂密码。
- 修改云服务器 Linux 系统默认远程登录端口，如下所示：
  修改文件：/etc/ssh/sshd_config

Port 22 #在第三行或第四行，如果前面有井号，请删除，修改为65534以下即可

可在远程连接中用 vi 命令，或 sftp 下载到本地修改，修改后使用以下命令重启 ssh 服务。

/etc/init.d/sshd restart #centos系统，重启ssh服务命令
/etc/init.d/ssh restart #debian/ubuntu系统，重启 ssh 服务命令

平台有安全组功能，建议您仅放行需要的业务协议和端口，不建议放行所有协议所有端口 。
配置云服务器系统防火墙，建议开启云防火墙 。
确保云服务器已安装的防护软件 主机安全客户端进程 处于正常运行状态，并开启实时告警，有异常登录时，及时反馈到您。
及时修复云服务器系统组件与 Web 组件存在的安全漏洞。

> 说明：
>
> 做好如上云服务器系统安全防护，虽可有效降低安全风险，但也无法保证绝对安全，建议定期做好云服务器系统的安全巡检

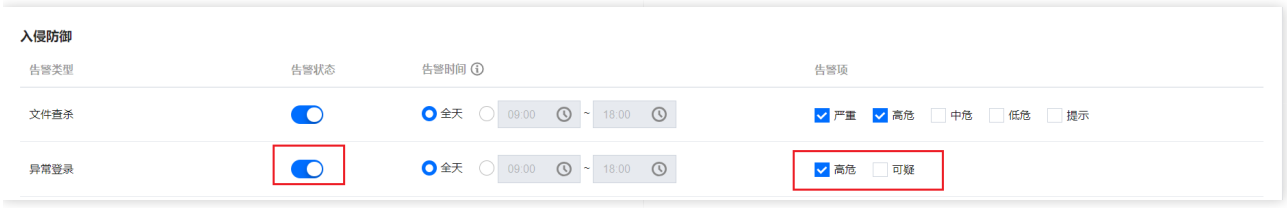
> 及数据备份，以防突发情况导致数据丢失、或业务不可用。
> 在安全加固的同时，也强烈建议您制作系统镜像、创建数据快照、自动定期快照。

常见问题

是否可以关闭异常登录检测？
不可以，关闭异常登录检测。
如果您不想接收异常登录的告警通知，您可以尽量配全登录白名单，或者关闭异常登录告警。
配全登录白名单：在【异常登录】页，选择【白名单管理】 >【添加白名单】，将常用登录来源 IP 添加为白名单。



关闭异常登录告警：在【设置中心】页面，将告警状态设为关闭，或取消勾选告警项"高危"或"可疑"即可。



实践教程
漏洞自动修复

本文将为您介绍自动修复漏洞的实践教程。

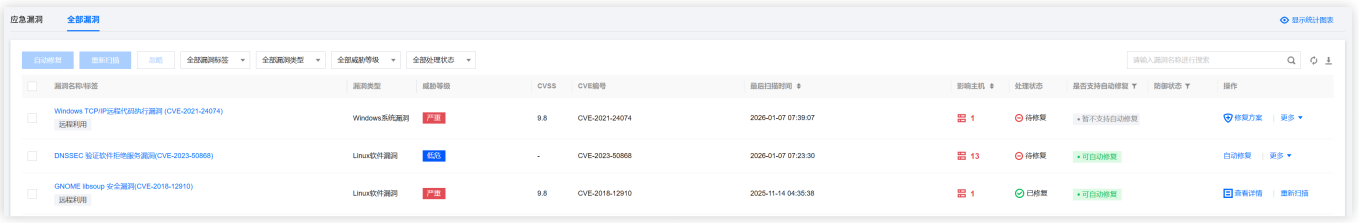
> 注意：
>
> - 因漏洞修复可能对用户业务造成影响，漏洞自动修复并非检出漏洞后立即进行自动化修复，须用户了解漏洞后单击修复并进行数据备份，才可进行自动化修复。
> - 自动修复漏洞可能会在您的主机上执行命令，可能影响到正在运行的应用或系统核心组件，可能影响您业务的连续性。对于核心业务主机，建议您充分考虑后再决策修复哪些漏洞及漏洞修复的先后顺序。

限制说明

- 支持自动修复的主机：仅支持CVM云服务器（主机安全客户端在线，且已绑定主机安全旗舰版授权）。
- 支持自动修复的漏洞：Linux 软件漏洞（部分）、Web-CMS 漏洞（部分）。

操作指南

1. 登录[主机安全租户端控制台]，单击左侧导航中的【漏洞管理】，底部可见漏洞检出列表。
2. 在漏洞列表中，分为应急漏洞、全部漏洞两类，由于均是从检出视角展示漏洞，二者本质无差异，下面以【全部漏洞】为例来介绍漏洞自动修复各个步骤。



- 可自动修复的漏洞在操作列中有【自动修复】操作，用户可手动触发自动修复。
- 暂不可自动修复的漏洞或受影响主机存在不符合前述限制要求的，在操作列中有【修复方案】操作，用户可参照修复方案进行手动修复。

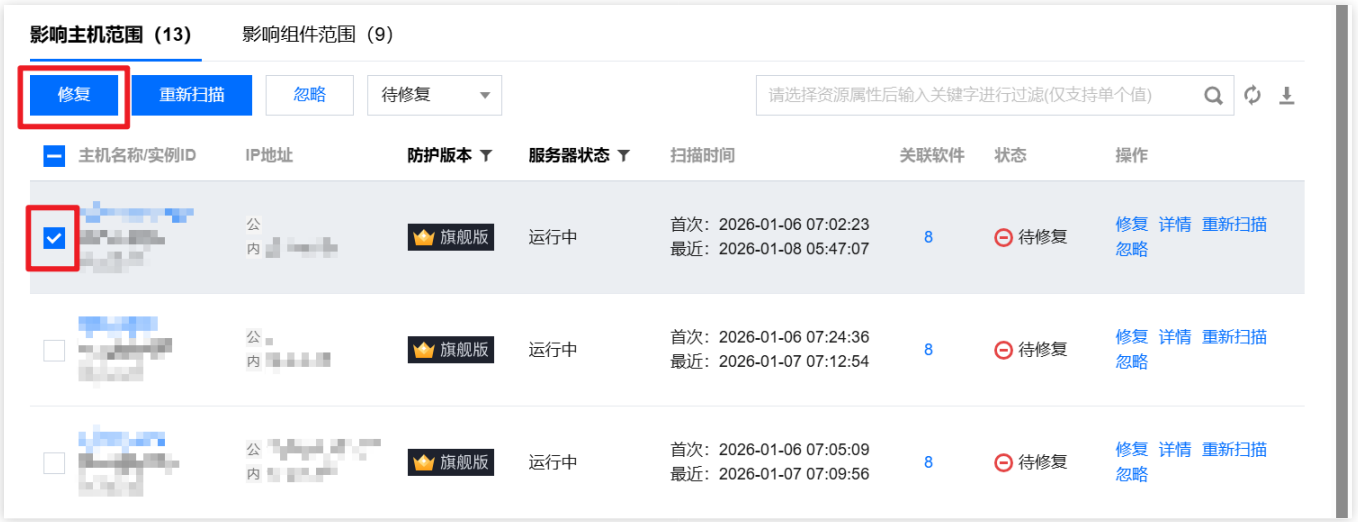
步骤1：查看漏洞详情

单击蓝字【漏洞名称】，打开漏洞详情弹窗，查看漏洞描述、修复方案、影响面等信息。



步骤2：选择需要修复的主机

1. 在受影响的服务器列表中选择您要修复的主机，单击【修复】**，**打开修复漏洞弹窗。



2. 在修复漏洞弹窗中，确定修复主机范围和修复组件范围后，单击【下一步】进行快照创建。



步骤3：选择是否创建快照

1. 请根据实际需求创建快照：

- 自动创建快照并修复：支持设置快照名称、快照保存时长（3天、7天、15天，建议保留7天时间，以便在有需求的情况下及时回滚）。
- 不创建快照直接修复：若今日所选修复主机均已创建过快照，此选项将变为可选状态。



2. 单击【开始修复】进入自动修复流程。

步骤4：自动修复

用户可在当前弹窗抽屉中查看最新修复进度。



步骤5：查看主机状态变更

返回【漏洞详情】，关注主机状态变更。若漏洞修复失败，状态则为修复失败；若漏洞修复成功，状态则变更为已修复。



- 漏洞修复后，若对您的业务产生了较大影响，您可单击【回滚】，将前往【云服务器 > 快照列表】，可选择您修复前创建的快照进行回滚。回滚成功后，请重启服务器，对漏洞进行重新扫描。
- 漏洞修复后，可进行【重新扫描】，再次验证漏洞是否已修复。
- 漏洞修复后，也可单击**【修复详情】**，查看修复的具体过程。

常见问题
功能相关

为什么 Jar 包类的漏洞多次扫描时，每次检测结果可能不一致？

Jar 包类漏洞，例如 Struts2 漏洞的检测依赖 Jar 包运行态是否加载，未运行服务时是不能检测到漏洞的，运行服务时 Webserver 对于Jar 包的加载分为动态加载和静态加载。在动态加载模式下，Struts2 漏洞只有在 Jar 包运行时才能被检测出来，所以每个时段检测结果存在差异。建议您针对高危 Jar 包漏洞进行多次检测，提升检测结果的准确度。

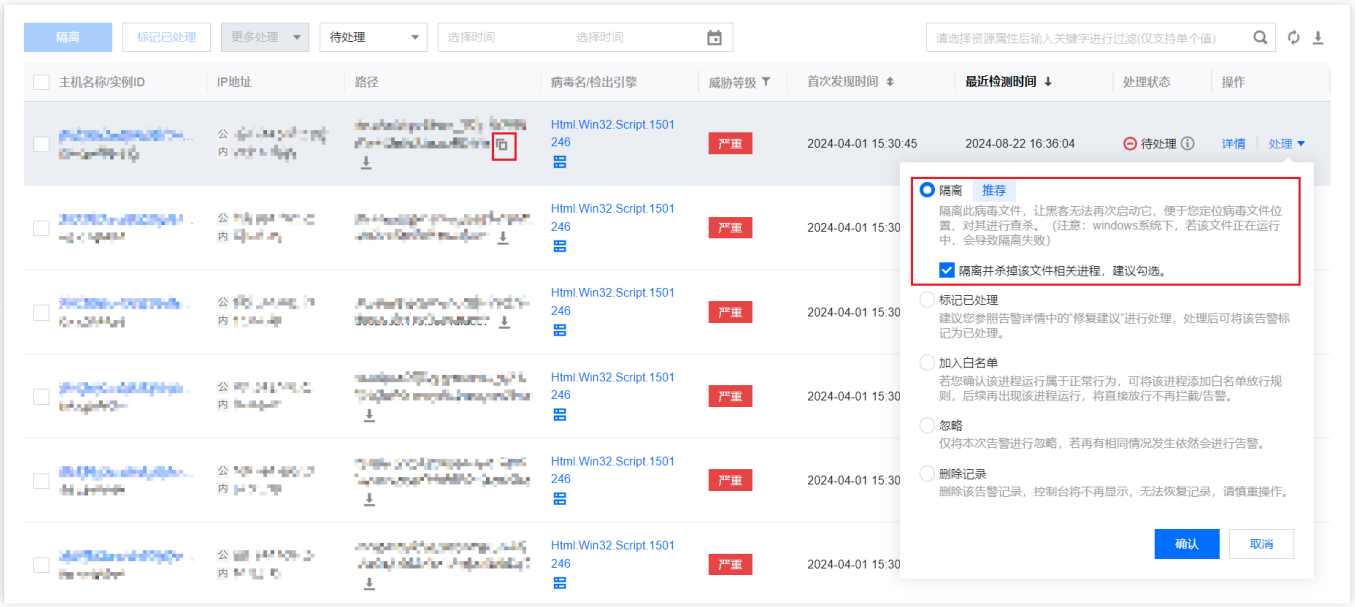
主机安全扫描频率是多少？

可自定义周期扫描，也可手动扫描。

如何对木马文件进行处理？

在【文件查杀】页面，可对木马文件进行如下处理：

- 删除：单击复制木马文件路径，定位木马并手动删除该文件。
- 加入白名单：您可执行加入白名单操作，后续主机安全将不再对该机器的该文件进行检测。
- 隔离：当前尚不支持拦截木马，仅支持事中或事后检测并告警，但可对该文件执行隔离操作，防止该文件再次被启动。



概览页安全评分机制是怎样的？

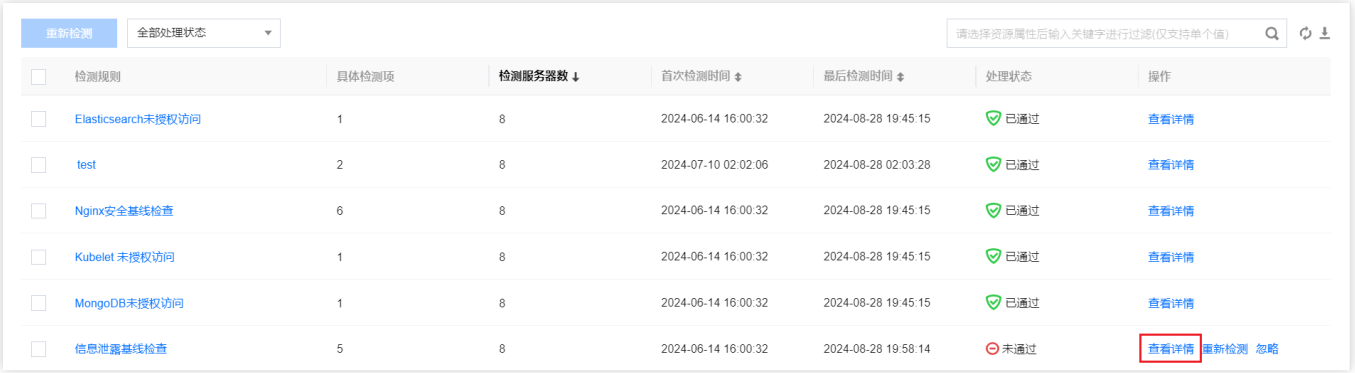
概览页安全评分机制，请参见 安全概览 文档。

安全基线在产品设置过后，多久可以生效？

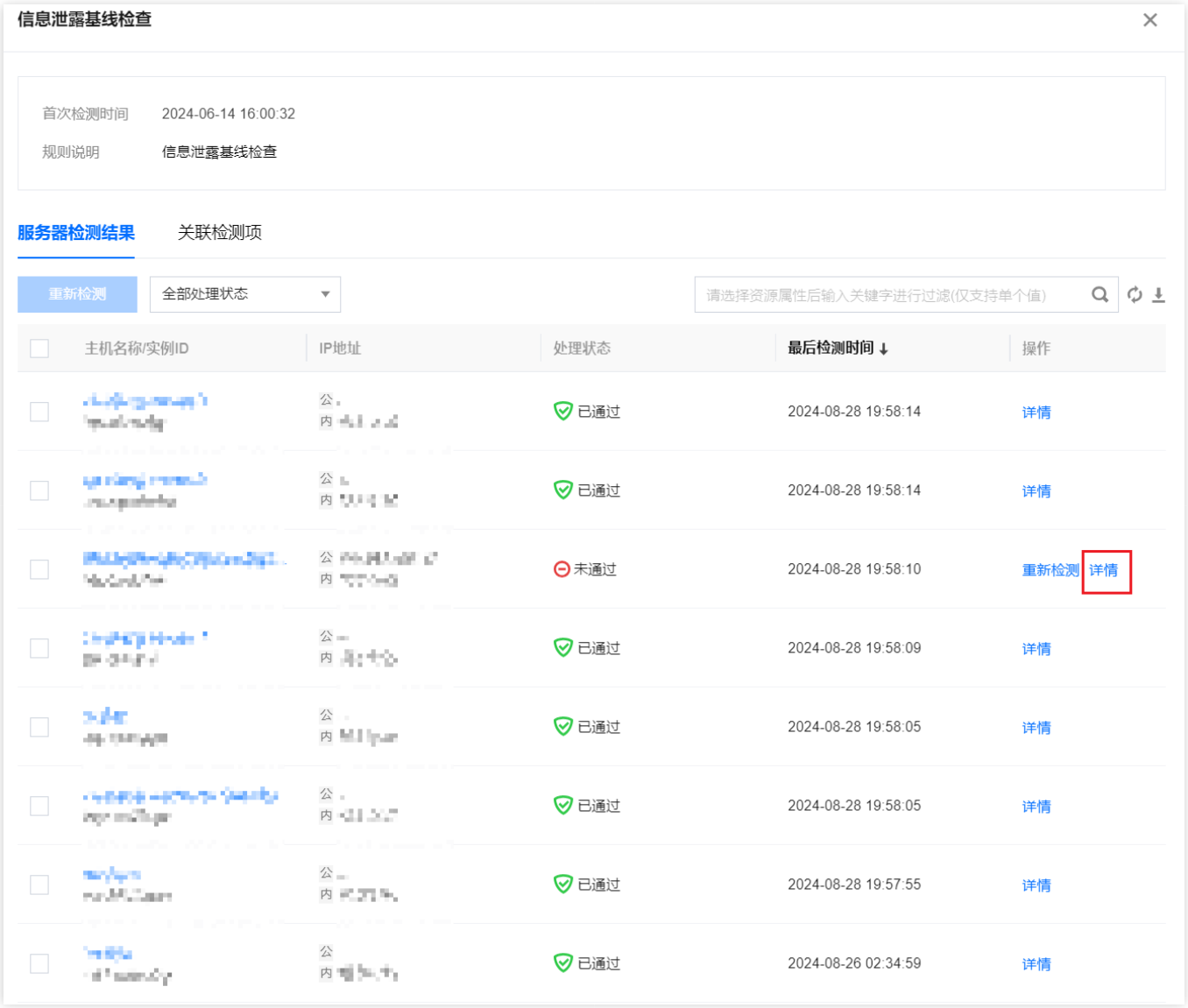
安全基线在产品设置后，即时生效。

主机安全基线检测"未通过"怎么处理？

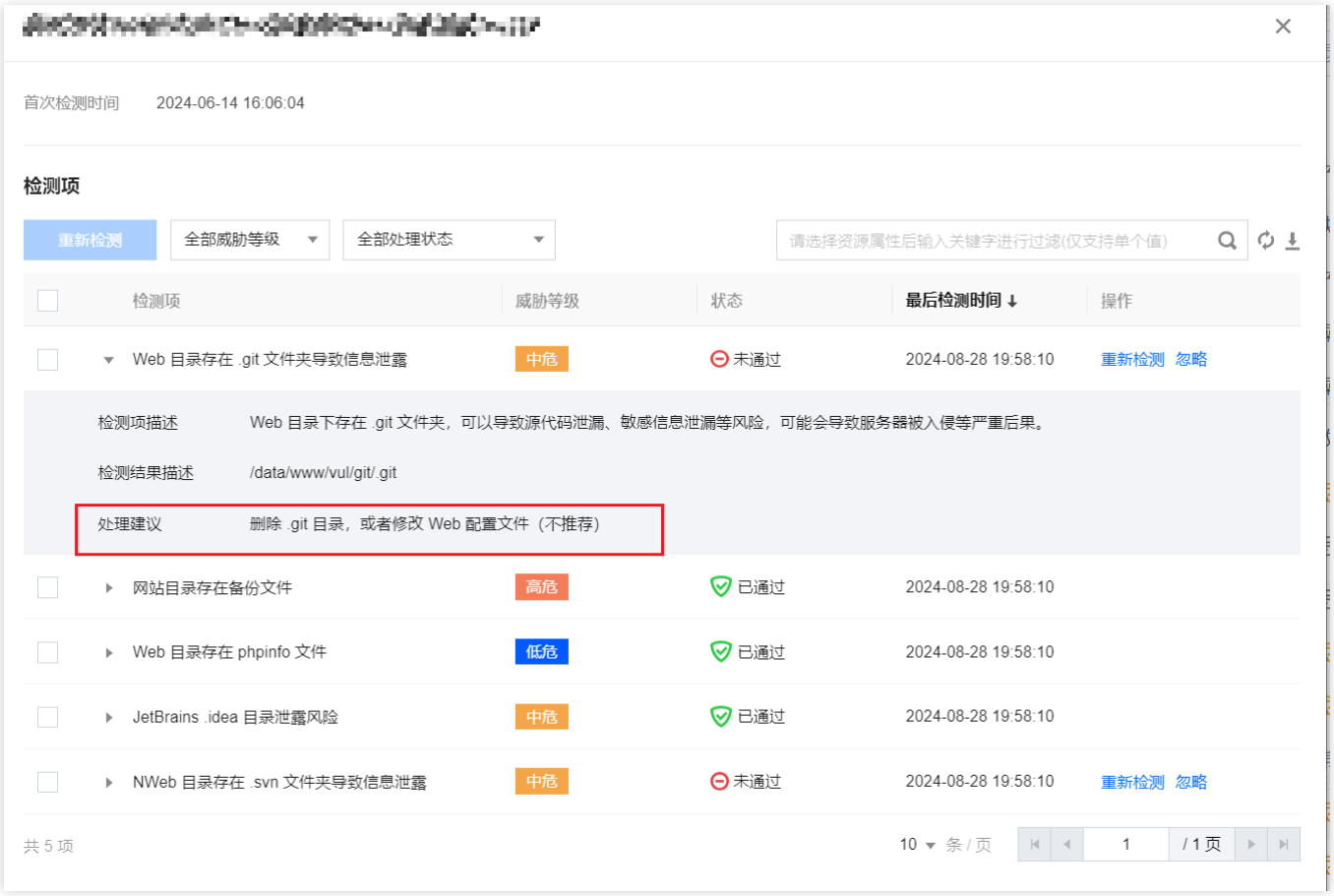
1. 进入【安全基线】页面，选择未通过的检测项，单击操作列下的【查看详情】，进入该检测项的详情页面。



2. 在基线检测结果页面中，选择未通过检测的服务器，单击【详情】，进入检测详情页面。



3. 在检测详情中可查看未通过的检测项，以及处理建议。



主机安全发现漏洞木马等攻击是否会进行通知？

会，若主机安全发现木马、应急漏洞或者其他攻击的行为，会通过站内信、短信、邮件或企业微信方式的方式进行告警通知，具体方式您可以在【消息中心】>【消息订阅】中进行设置。

入侵相关

入侵常见问题

云服务器被入侵有哪些危害？

- 业务被中断：数据库、文件被篡改或删除，导致服务无法访问，系统瘫痪。
- 数据被窃取：黑客窃取企业数据后公开售卖，客户隐私数据被泄漏，导致企业品牌受损、用户流失。
- 被加密勒索：黑客入侵云服务器后通过植入不可逆的加密勒索软件对数据进行加密，对企业进行金钱勒索。
- 服务不稳定：黑客在云服务器中运行挖矿程序、DDoS 木马程序，消耗大量系统资源，导致云服务器不能提供正常服务。

如何降低云服务器被入侵概率？

- 及时修复高危漏洞及基线相关问题。
- 设置强密码，避免暴破攻击。
- 定期巡检账号、权限、端口并及时处理主机安全租户端控制台上的告警信息。

云服务器被入侵后要如何防护？

防范措施建议如下：

- 云服务器密码设置为大写、小写、特殊字符、数字组成的12 - 16位的复杂密码 ，也可使用密码生成器自动生成复杂密码。
- 删除云服务器上设置的不需要的用户，且对于不需要登录的用户，请将其权限设置为禁止登录。
- 修改远程登录服务的默认端口号并禁止超级管理员用户登录。
- 针对 Linux 系统较为安全的方法是只使用密钥登录，禁止密码登录。
- 不建议向公网开放核心应用服务端口访问，例如 mysql、redis 等，您可修改为本地访问或禁止外网访问。
- 如果您的本地外网 IP 固定，建议使用安全组或者系统防火墙设置，禁止除了本地外网 IP 之外的所有 IP 的登录请求。

> 注意：
>
> 做好日常云服务器系统的安全防护，可以有效加强云服务器系统安全， 但无法保证绝对安全。 建议定期做好云服务器系统的安全巡检及数据备份，以防突发情况导致数据丢失或业务不可用。

如何做好云服务器防范措施？

建议升级主机安全专业版或旗舰版，并处理中危及以上的安全事件。

木马类问题

主机安全发现漏洞木马等攻击是否会进行通知？

会，若主机安全发现木马、应急漏洞或者其他攻击的行为，会通过站内信、短信、邮件或企业微信的方式进行告警通知，具体方式您可以在【消息中心】>【消息订阅】中进行设置。

如何处理木马及病毒文件？

- 若发现病毒及木马文件需及时进行隔离或删除相应恶意文件。
- 部分顽固木马、病毒可能存在重复写入的情况，需排查机器上是否存在弱口令、漏洞等异常情况并进行修复，同时删除恶意文件。
- 部分感染型病毒木马极难进行清理，建议定期对机器做快照备份。

异常登录类问题

云服务器显示登录异常怎么解决？

基于管理员的常用登录地进行异常登录判断，请仔细检查登录记录。若非管理员本人登录，密码可能已经泄露，用户需要对云服务器进行详细的安全检查。

如何处理异常登录告警？

1. 首先确认该异常登录是否为业务相关人员进行的登录，若非业务相关人员登录，在控制台确认是否存在木马、漏洞及源占用异常等情况，若有异常情况，请及时处理。
2. 确认该登录账户是否存在密码强度较弱的情况，及时进行修改。
3. 排查机器中的登录账号是否存在异常账号或权限过高的账户，及时禁用账户或调整权限。

正常登录行为被误报为异常登录，要如何消除误报？

您可以登录主机安全租户端控制台，在左侧导航中选择【入侵防御】>【异常登录】，在异常登录页面，找到被定义为异常登录的记录，在右侧操作栏中，单击【加白名单】，通过自定义添加登录白名单，即可消除误报。

是否可以关闭异常登录检测？

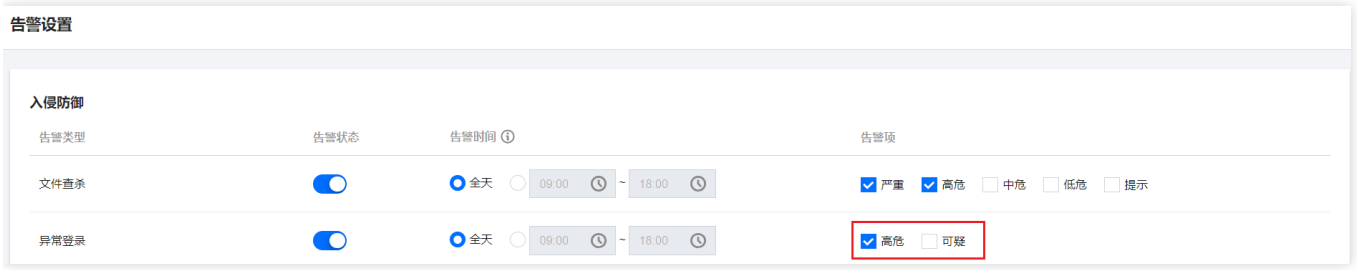
不可以关闭异常登录检测。如果您不想接收异常登录的告警通知，您可以将登录来源添加到白名单，或者取消勾选告警通知，操作步骤如下：

- 方式1：在【异常登录】页面，选择【白名单管理】>【添加白名单】，将登录来源添加为白名单。



- 方式2：在【设置中心】>【告警设置】页面，取消勾选异常登录的"高危"和"可疑"告警项即可。

> 注意：
>
> 如取消勾选，您将不能实时接收到异地登录的告警通知，请谨慎操作。



">密码泄露类问题

云服务器被暴力破解如何处理？

若云服务器被暴力破解成功，需尽快排查机器上的异常并进行处理：

- 排查机器中的账户是否存在弱口令，修改口令强度较弱的密码或采用密钥的方式进行登录，同时可通过设置安全组等方式降低被暴力破解的风险。
- 主机安全已上线密码破解阻断功能，可进行有效拦截。

提示密码被暴力破解成功之后该如何解决?

密码破解成功后，云服务器可能已被黑客入侵并留下了后门程序。

- 检查云服务器安全状况，是否还有其它未知账户和木马文件，如果存在请立即删除和修复，并修改云服务器登录密码。
- 根据实际情况决定是否需要对云服务器进行重置，并设置复杂密码，尽量字母、数字、特殊字符3种组合，长度在15位及以上。

防护状态离线类问题

云服务器的防护状态显示离线要如何解决?

主机安全客户端未连接服务端，导致后台显示离线，建议重新下载主机安全客户端进行安装，离线的可能原因如下：

- 云服务器启用了防火墙规则。
- 云服务器安装了第三方恶意软件，导致安全防护程序被破坏。

> 说明：
>
> 故障排查方式请参见 Linux 客户端离线排查 或 Windows 客户端离线排查。

软件相关说明
功能行为描述

Webshell 检测

Webshell 是黑客入侵过程中常用工具，主机安全客户端会对服务器上新创建的 Web 程序文件进行可疑风险判断，对于少量疑似 Webshell 文件，需要上报到云端，通过云端的机器学习检测引擎模块做进一步检测，检测完成后会实时删除该样本文件。主机安全默认提供每天全盘扫描服务，检测过程不会提取任何涉及用户隐私的数据。

登录异常提醒

登录异常提醒功能可以帮助用户识别异常的管理员登录行为，需要采集登录日志中的来源 IP、时间、登录用户名、登录状态数据到云端进行风险计算，登录日志数据需在云端保存一个月。

密码破解提醒

密码破解提醒功能可以告诉用户当前遭受的密码破解事件和破解结果，需要采集登录日志中的来源 IP、时间、登录用户名、登录状态数据到云端进行风险计算，登录日志数据需在云端保存一个月。

恶意木马和病毒检测

恶意木马和病毒程序通常会窃取用户数据或者对外攻击，消耗大量系统资源导致业务不能正常提供服务。客户端会采集可疑恶意程序的哈希指纹到云端，通过云查杀模块对哈希指纹进行检测，若云端哈希库无该文件记录，需要上报可执行文件到云端，通过云端杀毒引擎进行检测，检测完后会实时删除该样本文件。主机安全默认提供每天全盘扫描服务，检测过程中不会提取任何涉及用户隐私的数据。

漏洞提醒

目前主机安全支持检测影响面较大的 Linux 和 Windows 双平台的漏洞，以及符合安全要求的基线检测。
漏洞管理功能会显示当前主机上的漏洞风险情况，同时提供修复方案供用户参考。该模块执行时会从云端下载漏洞策

略库在本地执行检测，对于存在漏洞风险的主机，会上报应用软件的名称、版本号、路径、发现时间。主机安全默认提供每天漏洞扫描服务，这个过程不会提取任何涉及用户隐私的数据。

升级维护

升级维护功能主要提醒用户对客户端进行升级，以获得最新的安全防护服务，客户端软件需要采集主机安全版本号、操作系统配置信息、安全规则版本号到云端进行判断和提醒，该过程不会提取任何涉及用户隐私的数据。

客户端进程说明

名称	Windows 系统	Linux 系统
程序安装目录	C:\program files\qcloud\yunjing\ydeyes C:\program files\qcloud\yunjing\ydlive	/usr/local/qcloud/YunJing/
进程名称	YDService 云镜主服务进程 YDLive 守护进程 YDPython 漏洞&基线扫描插件 YDQuaraV2 木马隔离插件 qtflame 资产采集插件	YDService 云镜主服务进程 YDLive 守护进程 YDPython 漏洞&基线扫描插件 YDUtils 进程扫描插件 YDQuaraV2 木马隔离插件 qtflame 资产采集插件 tcss-agent 容器基线扫描插件 css-scan 容器镜像扫描插件
注册服务名称	YDService YDLive YDEdr	-

客户端程序所占用端口是系统随机返回的，无固定端口范围，若占用端口与用户业务端口冲突，重启客户端程序即可。

- 客户端重启命令（Linux系统）

1. 暂停客户端程序服务

/usr/local/qcloud/YunJing/stopYDCore.sh

2. 重新启动客户端

/usr/local/qcloud/YunJing/startYD.sh

- 客户端重启命令（Windows系统）
  输入以下命令，或打开任务管理器的服务，找到 YDService 服务，右键重启。

1. 暂停客户端程序服务

net stop YDService

2. 重新启动客户端

net start YDService

安全基线检测列表

本文档将为您介绍主机安全的安全基线检测列表。

> 注意：
>
> 安全基线在产品设置后，将即时生效。

Name	Level	Vul_type
CouchDB 未授权访问	高	配置不当
Docker Daemon 2375 管理端口开启	高	远程代码执行
Elasticsearch 未授权访问	高	配置不当
JavaRMI 远程代码执行	高	远程代码执行
Jenkins 未开启认证可导致命令执行	高	远程代码执行
Kubelet 未授权访问	高	安全基线
Linux 系统弱口令检测	高	远程代码执行
MongoDB 未授权访问	高	配置不当
MySQL 弱口令检测	高	弱口令
NFS 错误配置导致可挂载敏感目录	高	配置不当
Redis® 基线合规检测	高	远程代码执行
RPCBind 配置不当检测	高	安全基线
Rsync 弱口令检测	高	弱口令
Rsync 无密码访问	高	配置不当
Tomcat 弱口令检测	高	弱口令
Windows 用户弱口令检测	高	弱口令
Xampp 默认 FTP 密码	高	信息泄露
网站目录存在备份文件	高	信息泄露
FTP 匿名登录检测	中	信息泄露
IIS 配置错误导致存在解析漏洞	中	配置不当

Name	Level	Vul_type
Memcached UDP 端口可被利用为 DDOS 放大攻击	中	信息泄露
PHP-FPM 错误配置	中	安全基线
PostgreSQL 合规检测	中	远程代码执行
Web 目录存在 .git 文件夹导致信息泄露	中	信息泄露
Web 目录存在 .svn 文件夹导致信息泄露	中	信息泄露
Windows 隐藏账户检测	中	安全基线
Windows 影子账户检测	中	远程代码执行
ZooKeeper 未授权访问	中	配置不当
Hadoop未授权访问	低	远程代码执行
sudo 无密码用户检测	低	安全基线
Tomcat 样例目录检测	低	安全基线
Web 目录存在 phpinfo 文件	低	信息泄露
Windows 来宾账户状态检测	低	安全基线

API文档
主机安全（cwp）
版本（2018-02-28）
API 概览

API版本

V3

专家服务相关接口

接口名称	接口功能
DescribeEmergencyResponseList	应急响应列表
DescribeMonthInspectionReport	安全管家月巡检报告下载

入侵检测-反弹shell相关接口

接口名称	接口功能
DeleteMemShellRules	删除反弹Shell规则
DeleteReverseShellEvents	删除反弹Shell事件
DeleteReverseShellRules	删除反弹Shell规则
DeleteReverseShellRulesAggregation	删除反弹Shell规则
DescribeMemShellRules	获取反弹Shell规则列表
DescribeReverseShellEvents	获取反弹Shell列表
DescribeReverseShellRules	获取反弹Shell规则列表
DescribeReverseShellRulesAggregation	获取反弹Shell规则列表
DescribeReverseShellSystemPolicyConfig	查询反弹shell系统策略配置

接口名称	接口功能
DescribeShellPolicyList	查询反弹shell策略列表
ExportReverseShellEvents	导出反弹Shell事件
ModifyReverseShellRulesAggregation	编辑反弹Shell规则（支持多服务器选择）
ModifyReverseShellSystemPolicyConfig	修改反弹shell系统策略配置
ModifyShellPolicyStatus	编辑反弹shell策略开关

入侵检测-密码破解相关接口

接口名称	接口功能
DeleteBruteAttacks	删除暴力破解记录
DescribeBanMode	获取爆破阻断模式
DescribeBanRegions	获取阻断地域
DescribeBanStatus	获取阻断按钮状态
DescribeBanWhiteList	获取阻断白名单列表
DescribeBruteAttackList	获取密码破解列表
DescribeBruteAttackRules	获取爆破破解规则
ExportBruteAttacks	导出密码破解记录
ModifyBanMode	修改爆破阻断模式
ModifyBanStatus	设置阻断开关状态
ModifyBruteAttackRules	修改暴力破解规则
StopNoticeBanTips	不再提醒爆破阻断提示弹窗

入侵检测-异常登录相关接口

接口名称	接口功能
DeleteLoginWhiteList	删除异地登录白名单规则

接口名称	接口功能
DeleteNonlocalLoginPlaces	删除异地登录记录
DescribeHostLoginList	获取登录审计列表
DescribeLoginWhiteCombinedList	获取异地登录白名单合并后列表
DescribeLoginWhiteList	获取异地登录白名单列表
DescribeUsualLoginPlaces	查询常用登录地
ExportNonlocalLoginPlaces	导出异地登录记录

入侵检测-恶意请求相关接口

接口名称	接口功能
DeleteMaliciousRequests	删除恶意请求记录
DescribeMaliciousRequestWhiteList	查询恶意请求白名单列表
DescribeRiskDnsList	获取恶意请求列表
ExportMaliciousRequests	导出下载恶意请求文件

入侵检测-文件查杀相关接口

接口名称	接口功能
CreateNetAttackWhiteList	创建网络攻击白名单
CreateScanMalwareSetting	文件查杀检测
DeleteMalwareScanTask	入侵管理-终止扫描任务
DeleteMalwares	删除木马记录
DeleteNetAttackWhiteList	删除网络攻击白名单
DescribeJavaMemShellList	查询java内存马事件列表
DescribeMalWareList	获取木马列表
DescribeMalwareFile	获取木马文件下载地址

接口名称	接口功能
DescribeMalwareInfo	查看恶意文件详情
DescribeMalwareRiskWarning	风险预警提示
DescribeMalwareTimingScanSetting	查询定时扫描配置
DescribeNetAttackWhiteList	获取网络攻击白名单列表
DescribeScanMalwareSchedule	查询木马扫描进度
DescribeServersAndRiskAndFirstInfo	获文件查杀概览信息
ExportMalwares	导出木马记录
ModifyMalwareTimingScanSettings	定时扫描设置
ModifyNetAttackWhiteList	编辑网络攻击白名单
RecoverMalwares	恢复木马文件
SeparateMalwares	隔离木马
TrustMalwares	信任木马文件
UntrustMalwares	取消信任木马

入侵检测-本地提权相关接口

接口名称	接口功能
DeletePrivilegeEvents	删除本地提权事件
DeletePrivilegeRules	删除本地提权规则
DescribePrivilegeEvents	获取本地提权事件列表
DescribePrivilegeRules	获取本地提权规则列表
ExportPrivilegeEvents	导出本地提权事件

入侵检测-高危命令相关接口

接口名称	接口功能

接口名称	接口功能
CheckBashRuleParams	校验高危命新增用户规则参数
DeleteBashEvents	删除高危命令事件
DeleteBashRules	删除高危命令规则
DescribeBashEvents	获取高危命令列表
DescribeBashEventsNew	获取高危命令列表(新)
DescribeBashRules	获取高危命令规则列表
EditBashRules	新增或修改高危命令规则（支持多服务器选择）
ExportBashEvents	导出高危命令事件
SetBashEventsStatus	设置高危命令事件状态
SwitchBashRules	切换高危命令规则状态

其他接口

接口名称	接口功能
CreateLoginPermissionPush	下发登录许可
DeleteLogClsDeliverInfo	修改日志cls投递配置
DeleteScanTask	停止扫描任务
DescribeAssetEnvList	查询资产管理环境变量列表
DescribeClientException	获取客户端异常事件
DescribeClsAccountStatus	查询cls账户状态
DescribeClsLogsets	查询cls日志集列表
DescribeClsTopics	查询cls日志集列表
DescribeCustomerDetail	查询客户信息 客户级别,是否企业客户
DescribeGeneralStat	获取主机相关统计
DescribeLogClsDeliverInfo	获取cls投递信息

接口名称	接口功能
DescribeLogStorageConfig	获取日志存储配置
DescribeLogStorageRecord	获取日志存储量记录
DescribeLoginPermission	检查用户是否有指定主机登录权限
DescribeMachineInfoByHashKey	获取机器信息
DescribeMachineLoginType	获取主机登录方式
DescribeMachineLoginTypeStatus	获取主机登录方式状态
DescribeOrderList	查询资源订单列表
DescribeOverviewStatistics	获取概览统计数据
DescribeProVersionInfo	获取专业版概览信息
DescribeProVersionStatus	获取专业版状态
DescribeRecommendedProtectCpu	查询推荐购买防护核数
DescribeScanState	查询扫描状态
DescribeScanTaskDetails	查询扫描任务详情
DescribeSecurityDynamics	获取安全事件动态消息
DescribeSecurityEventStat	获取安全事件统计
DescribeSecurityEventsCnt	获取安全事件数统计数据
DescribeSecurityTrends	获取安全事件统计数据
DescribeTaskDuration	获取任务下发时长
DescribeTrialReport	查询主机安全授权试用报告(仅限控制台申领的)
DescribeUsersConfig	用于查询用户自定义配置
DescribeVersionStatistics	获取专业版和基础版机器数
DescribeVulTrend	获取漏洞态势信息
ExportScanTaskDetails	导出扫描任务详情
ExportSecurityTrends	导出风险趋势
ExportTasks	异步导出任务

接口名称	接口功能
ModifyEventAttackStatus	修改网络攻击事件状态
ModifyLogClsDeliverInfo	修改日志cls投递配置
ModifyLogClsDeliverSwitch	修改某个日志类型的cls投递开关
ModifyLogStorageConfig	修改日志存储配置
ModifyMachineLoginType	修改主机登录方式
ModifyOrder	新购/变配 订单
ModifyUsersConfig	用于创建/修改用户自定义配置
ModifyVulDefenceSwitch	安全中心漏洞防御、网络攻击开关修改

基线管理相关接口

接口名称	接口功能
ChangeRuleEventsIgnoreStatus	修改事件忽略状态
CreateBaselineStrategy	创建基线策略
DeleteBaselineStrategy	删除基线策略
DescribeBaselineAnalysisData	基线策略概览统计数据查询
DescribeBaselineBasicInfo	查询基线基础信息
DescribeBaselineDetail	查询基线详情
DescribeBaselineEffectHostList	基线影响主机列表
DescribeBaselineHostTop	服务器风险top接口
DescribeBaselineList	查询基线列表
DescribeBaselineRule	查询基线检测项信息
DescribeBaselineScanSchedule	基线检测进度查询
DescribeBaselineStrategyDetail	查询基线策略详情
DescribeBaselineStrategyList	用户基线策略列表查询

接口名称	接口功能
DescribeBaselineTop	基线检测项TOP
DescribeIgnoreBaselineRule	查询忽略检测项信息
DescribeIgnoreRuleEffectHostList	查询忽略检测项影响主机列表
DescribeStrategyExist	根据策略名查询策略是否存在
ExportBaselineEffectHostList	基线影响主机列表导出
ExportBaselineList	导出基线列表
ExportIgnoreBaselineRule	已忽略基线检测项导出
ExportIgnoreRuleEffectHostList	忽略检测项影响主机列表导出
UpdateBaselineStrategy	更新基线策略信息

安全运营相关接口

接口名称	接口功能
CreateSearchLog	添加历史搜索记录
CreateSearchTemplate	添加检索模板
DeleteSearchTemplate	删除检索模板
DescribeESAggregations	获取ES字段聚合结果
DescribeHistoryService	查询日志检索服务信息
DescribeIndexList	获取索引列表
DescribeLogStorageStatistic	获取日志检索容量使用统计
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

新版基线管理相关接口

接口名称	接口功能
DeleteBaselinePolicy	删除基线策略配置
DeleteBaselineRule	删除基线规则
DeleteBaselineRuleIgnore	删除基线忽略规则
DeleteBaselineWeakPassword	删除基线弱口令
DescribeBaselineDetectList	获取基线检测详情记录
DescribeBaselineDetectOverview	获取基线检测概览
DescribeBaselineDownloadList	获取基线下载列表
DescribeBaselineFixList	获取基线修复列表
DescribeBaselineHostDetectList	获取基线检测主机列表
DescribeBaselineHostIgnoreList	获取忽略规则主机列表
DescribeBaselineHostRiskTop	获取基线服务器风险TOP5
DescribeBaselineItemDetectList	获取基线检测项的列表
DescribeBaselineItemIgnoreList	获取忽略规则项列表
DescribeBaselineItemInfo	获取基线检测项信息
DescribeBaselineItemList	获取基线项检测结果列表
DescribeBaselineItemRiskTop	获取基线检测项TOP5
DescribeBaselinePolicyList	获取基线策略列表
DescribeBaselineRuleCategoryList	获取基线分类列表
DescribeBaselineRuleDetectList	获取基线规则检测列表
DescribeBaselineRuleIgnoreList	获取基线忽略规则列表
DescribeBaselineRuleList	获取基线规则列表
DescribeBaselineWeakPasswordList	获取基线弱口令列表
DescribeHotVulTop	获取全网热点漏洞
DescribeIgnoreHostAndItemConfig	获取一键忽略受影响的检测项和主机信息
DescribeVulStoreList	获取漏洞库列表

接口名称	接口功能
ExportBaselineFixList	导出修复列表
ExportBaselineHostDetectList	导出基线主机检测
ExportBaselineItemDetectList	导出基线检测项
ExportBaselineItemList	导出检测项结果列表
ExportBaselineRuleDetectList	导出基线检测规则
ExportBaselineWeakPasswordList	导出弱口令配置列表
FixBaselineDetect	修复基线检测
ModifyBaselinePolicy	修改或新增基线策略设置
ModifyBaselinePolicyState	修改或新增基线策略状态
ModifyBaselineRule	修改或新增基线检测规则
ModifyBaselineRuleIgnore	修改或新增基线忽略规则
ModifyBaselineWeakPassword	修改或新增弱口令
StartBaselineDetect	检测基线
StopBaselineDetect	停止基线检测
SyncBaselineDetectSummary	同步基线检测进度概要

漏洞管理相关接口

接口名称	接口功能
CancelIgnoreVul	取消漏洞忽略
CreateEmergencyVulScan	应急漏洞扫描
DescribeEmergencyVulList	应急漏洞列表
DescribeInjectRiskyServiceSwitch	查询java内存马和rasp的是否注入风险服务配置
DescribeScanSchedule	查询检测进度
DescribeScanVulSetting	定期检测配置查询

接口名称	接口功能
DescribeUndoVulCounts	获取指定漏洞分类统计数
DescribeVulCountByDates	获取近日指定类型的漏洞数量和主机数量
DescribeVulDefenceOverviewCount	获取漏洞防御策略和事件统计
DescribeVulDefenceSettingList	查询漏洞防御设置列表
DescribeVulEffectHostList	漏洞影响主机列表
DescribeVulHostCountScanTime	获取待处理漏洞数+影响主机数
DescribeVulHostTop	获取服务器风险top列表
DescribeVulInfoCvss	漏洞详情
DescribeVulLevelCount	查询漏洞数量等级分布统计
DescribeVulList	漏洞列表
DescribeVulTop	获取漏洞top统计
ExportVulDetectionExcel	导出本次漏洞检测Excel
ExportVulDetectionReport	导出漏洞检测报告
ExportVulEffectHostList	导出漏洞影响主机列表
ExportVulList	漏洞管理-导出漏洞列表
IgnoreImpactedHosts	忽略漏洞
ModifyInjectRiskyServiceSwitch	是否注入风险服务开关，包括内存马、rasp都是这个接口，容器rasp的开关在容器服务里
ScanVul	一键检测
ScanVulAgain	漏洞管理-重新检测接口
ScanVulSetting	定期扫描漏洞设置

设置中心相关接口

接口名称	接口功能
CreateAgentInstallTask	创建安装主机安全agent任务

接口名称	接口功能
CreateLicenseOrder	创建授权订单
DeleteLicenseRecord	删除授权记录
DescribeAgentInstallResult	获取机器安装结果
DescribeAgentInstallTaskResult	获取ageng安装任务完成情况
DescribeChangingAssetInfo	获取修改中的主机列表
DescribeLicenseBindList	查看授权绑定列表
DescribeLicenseBindSchedule	查询授权绑定进度
DescribeLicenseGeneral	授权概览信息
DescribeLicenseList	获取授权订单列表
DescribeSaveOrUpdateWarnings	更新用户告警设置
DescribeWarningList	获取当前用户告警列表
DescribeWarningServiceIPList	获取告警服务IP名单
DestroyOrder	销毁订单
ExportLicenseDetail	导出授权详情
ModifyAssetsProtectionStatus	修改主机防护状态
ModifyAutoOpenProVersionConfig	设置自动开通配置
ModifyLicenseBinds	授权批量绑定
ModifyLicenseOrder	编辑《主机安全-按量计费》授权订单
ModifyLicenseUnBinds	授权批量解绑
ModifyOrderAttribute	编辑订单属性
ModifyWarningSetting	修改告警设置

资产管理相关接口

接口名称	接口功能

接口名称	接口功能
CreateIncidentBacktracking	对旗舰版机器单次触发事件调查及告警回溯
DeleteCloudVendorAccountAK	删除AK配置
DeleteMachine	卸载云镜客户端
DeleteMachineTag	删除服务器关联的标签
DeleteTags	删除标签
DescribeAccountStatistics	获取帐号统计列表数据
DescribeAssetAppList	查询应用列表
DescribeAssetAppProcessList	获取软件关联进程列表
DescribeAssetCoreModuleInfo	获取内核模块详情
DescribeAssetCoreModuleList	查询资产管理内核模块列表
DescribeAssetDatabaseInfo	获取资产管理数据库详情
DescribeAssetDatabaseList	查询资产管理数据库列表
DescribeAssetHostTotalCount	获取主机所有资源数量
DescribeAssetInfo	获取资产数量概况
DescribeAssetInitServiceList	查询资产管理启动服务列表
DescribeAssetJarInfo	获取Jar包详情
DescribeAssetJarList	查询Jar包列表
DescribeAssetMachineDetail	获取资产管理主机资源详细信息
DescribeAssetMachineList	获取资源监控列表
DescribeAssetPlanTaskList	查询资产管理计划任务列表
DescribeAssetPortInfoList	获取资产管理端口列表
DescribeAssetProcessInfoList	获取资产管理进程列表
DescribeAssetRecentMachineInfo	获取主机概况趋势
DescribeAssetSystemPackageList	获取资产管理系统安装包列表
DescribeAssetUserInfo	获取主机账号详情

接口名称	接口功能
DescribeAssetUserList	获取账号列表
DescribeAssetWebAppList	获取资产管理Web应用列表
DescribeAssetWebAppPluginList	获取资产管理Web应用插件列表
DescribeAssetWebFrameList	获取资产管理Web框架列表
DescribeAssetWebLocationInfo	获取Web站点详情
DescribeAssetWebLocationList	获取Web站点列表
DescribeAssetWebServiceInfoList	查询资产管理Web服务列表
DescribeAssetWebServiceProcessList	获取Web服务关联进程列表
DescribeCloudVendorAccountAKList	获取用户添加的云厂商AK列表
DescribeComponentStatistics	获取组件统计列表
DescribeComponents	本接口 (DescribeComponents) 用于获取组件列表数据。
DescribeExportMachines	导出区域主机列表
DescribeHistoryAccounts	获取帐号变更历史列表
DescribeImportMachineInfo	查询批量导入机器信息
DescribeMachineInfo	获取机器详情
DescribeMachineOsList	查询机器操作系统列表
DescribeMachineRegionList	查询主机地域列表
DescribeMachineRegions	获取机器地域列表
DescribeMachines	获取区域主机列表
DescribeOpenPortStatistics	获取端口统计列表
DescribeProcessStatistics	获取进程统计列表
DescribeTagMachines	获取指定标签关联的服务器信息
DescribeTags	获取所有主机标签
EditTags	新增或编辑标签
ExportAssetCoreModuleList	导出资产管理内核模块列表

接口名称	接口功能
ExportAssetWebServiceInfoList	导出资产管理Web服务列表
ModifyMachineRemark	修改主机备注信息
ScanAsset	资产指纹启动扫描
SyncAssetScan	同步资产扫描信息
UpdateMachineTags	关联机器标签列表

高级防御相关接口

接口名称	接口功能
CreateMaWorkloadLabel	创建微告警负载标签
CreateProtectServer	添加网站防护服务器
DeleteAttackLogs	删除网络攻击日志
DeleteMaConnEvent	删除微告警访问事件
DeleteMaCustomPolicy	删除微告警自定义白名单
DeleteMaLabel	删除微告警标签
DeleteMaSelfLearnPolicy	删除微告警自学习子策略
DeleteMaWhitelist	删除微告警全局白名单
DeleteProtectDir	删除防护网站
DeleteWebPageEventLog	删除事件记录
DescribeAttackEventInfo	网络攻击事件详情
DescribeAttackEvents	按分页形式展示网络攻击检测事件列表
DescribeAttackLogInfo	网络攻击日志详情
DescribeAttackLogs	网络攻击日志列表
DescribeAttackStatistics	网络攻击数据统计
DescribeAttackTop	网络攻击top5数据列表

接口名称	接口功能
DescribeAttackTrends	网络攻击趋势数据
DescribeAttackVulTypeList	获取网络攻击威胁类型列表
DescribeMaConnEventList	获取微告警访问事件
DescribeMaCustomPolicyList	获取微告警自定义白名单
DescribeMaGlobalConf	获取微告警全局配置
DescribeMaHostList	获取微告警主机列表
DescribeMaLabel	获取微告警标签信息
DescribeMaLabelList	获取微告警标签列表
DescribeMaLabelSourceList	获取微告警标签来源列表
DescribeMaPodList	获取微告警POD列表
DescribeMaSelfLearnConfig	获取微告警自学习策略
DescribeMaSelfLearnPolicyList	获取微告警自学习子策略列表
DescribeMaSummary	获取微告警整体概要
DescribeMaWhitelist	获取微告警全局白名单设置
DescribeMaWorkloadLabel	获取微告警负载标签
DescribeMaWorkloadList	获取微告警负载列表
DescribeMachineList	网页防篡改获取区域主机列表
DescribeNetAttackSetting	查询网络攻击设置
DescribeProtectDirList	防护目录列表
DescribeProtectDirRelatedServer	查询防护目录关联服务器
DescribeServerRelatedDirInfo	查询服务器关联目录详情
DescribeWebPageEventList	查询篡改事件列表
DescribeWebPageGeneralize	查询网页防篡改概览信息
DescribeWebPageProtectStat	查询网页防篡改防护统计
DescribeWebPageServiceInfo	查询网站防篡改服务信息

接口名称	接口功能
DisableSelfLearn	关闭微告警自学习
ExportAttackEvents	导出网络攻击事件
ExportAttackLogs	导出网络攻击日志
ExportMaConnEventList	导出微告警访问事件
ExportMaCustomPolicyList	导出微告警自定义白名单
ExportMaHostList	导出微告警主机列表
ExportMaPodList	导出微告警POD列表
ExportMaSelfLearnPolicyList	导出微告警自学习子策略
ExportMaWhitelist	导出微告警全局白名单
ExportProtectDirList	导出防护目录列表
ExportWebPageEventList	导出篡改事件列表
ModifyMaConnEventType	更改微告警访问事件类型，可实现取消加白
ModifyMaCustomPolicy	创建或者更改微告警自定义白名单
ModifyMaCustomPolicyStatus	更微告警自定义白名单状态
ModifyMaGlobalConf	修改微告警全局配置
ModifyMaLabel	新增或更改标签信息
ModifyMaSelfLearnConfig	配置自学习策略
ModifyMaWhitelist	更改微告警全局白名单设置
ModifyMaWhitelistStatus	更改微告警全局白名单状态
ModifyMaWorkloadLabel	更改微告警负载标签
ModifyMaWorkloadMonitor	更改微告警负载监控
ModifyMemShellRules	编辑或者创建java内存马白名单
ModifyNetAttackSetting	修改网络攻击设置
ModifyWebPageProtectDir	创建网站防护目录
ModifyWebPageProtectSetting	修改网站防护设置

接口名称	接口功能
ModifyWebPageProtectSwitch	网站防护设置开关

调用方式
接口签名v1

TCloudFinanceZone 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TCloudFinanceZone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

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	shjr
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' : 'shjr',
    '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=shjr&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.finance.cloud.tencent.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.finance.cloud.tencent.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=shjr&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.finance.cloud.tencent.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=shjr&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TCloudFinanceZone 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
- Node

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.finance.cloud.tencent.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=shjr&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 CloudAPIDemo {
    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.finance.cloud.tencent.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.finance.cloud.tencent.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)).app
end("&");
        }
        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.Intege
r.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", "shjr"); // 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.finance.cloud.tencent.com"
    data = {
        'Action' : 'DescribeInstances',
        'InstanceIds.0' : 'ins-09dx96dg',
        'Limit' : 20,
        'Nonce' : 11886,
        'Offset' : 0,
        'Region' : 'shjr',
        '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

TCloudFinanceZone 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TCloudFinanceZone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.finance.cloud.tencent.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.finance.cloud.tencent.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=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
```

最终完整的调用信息如下：

```
https://cvm.finance.cloud.tencent.com/?Limit=10&Offset=0

Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2018-10-09/cvm/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
Content-Type: application/x-www-form-urlencoded
Host: cvm.finance.cloud.tencent.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: shjr
```

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
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 CloudAPITC3Demo {
    private final static String CHARSET = "UTF-8";
    private final static String ENDPOINT = "cvm.finance.cloud.tencent.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-urlencode
d";
    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.finance.cloud.tencent.com";
        String region = "shjr";
        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" + canonicalQueryStri
ng + "\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" + hashedCan
onicalRequest;
        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)).toLow
erCase();
        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.finance.cloud.tencent.com"
endpoint = "https://" + host
region = "shjr"
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

1. 服务地址

地域（Region）是指物理的数据中心的地理区域。TCloudFinanceZone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

TCloudFinanceZone 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

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 cor
rect."
        },
        "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

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。
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。

错误码	错误描述
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

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。

参数名称	类型	必选	描述
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。
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。TCloudFinanceZone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。

专家服务相关接口
应急响应列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

专家服务-应急响应列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeEmergencyResponseList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序字段 StartTime，EndTime 示例值： StartTime
Filters	否	否	Array of Filters	过滤条件。 • Keyword- String - 是否必填：否 - 关键词过滤， • Status - String - 是否必填：否 - 状态 示例值：查看
Limit	否	否	Uint64	需要返回的数量，最大值为100 示例值： 10
Offset	否	否	Uint64	排序步长 示例值： 0

参数名称	必选	允许NULL	类型	描述
Order	否	否	String	排序方法 示例值： desc

3. 输出参数

参数名称	类型	描述
List	Array of EmergencyResponseInfo	应急响应列表 示例值：查看
TotalCount	Uint64	总条数 示例值： 100
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

安全管家月巡检报告下载

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

专家服务-安全管家月巡检报告下载

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeMonthInspectionReport
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Limit	是	否	Uint64	分页大小 示例值： 10
Offset	是	否	Uint64	分页步长 示例值： 10

3. 输出参数

参数名称	类型	描述
List	Array of MonthInspectionReport	巡检报告列表 示例值：查看
TotalCount	Uint64	总条数 示例值： 10

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	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
ResourceInsufficient	资源不足。
LimitExceeded	超过配额限制。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

入侵检测-反弹shell相关接口
删除反弹Shell规则

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除内存马白名单规则

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DeleteMemShellRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
GroupIDs	是	否	Array of String	批次ID数组. (最大100条) 示例值： ["1","2"]

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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

删除反弹Shell事件

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据Ids删除反弹Shell事件

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	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：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组. (最大100条) 示例值： [232196162]

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
LimitExceeded.AreaQuota	超出批量添加数量。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

删除反弹Shell规则

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除反弹Shell规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteReverseShellRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组. (最大100条) 示例值： [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

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
LimitExceeded.AreaQuota	超出批量添加数量。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter.DateRange	时间区间格式错误。
InvalidParameter.RegexRuleError	正则参数格式错误。
InvalidParameter.ReverShellKeyFieldAllEmpty	进程名/目标IP/目标端口，不能同时为空。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

删除反弹Shell规则

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除反弹Shell规则-聚合版本

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DeleteReverseShellRulesAggregation
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
GroupIDs	是	否	Array of String	批次ID数组. (最大100条) 示例值： ["85c909fe-c87c-11e9-a100-5cb90191ae78"]

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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取反弹Shell规则列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取java内存马白名单列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMemShellRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序字段，目前有：CreateTime、ModifyTime，默认按照ModifyTime排序 示例值： ModifyTime
Filters	否	否	Array of Filter	过滤条件。 • Keywords - String - 是否必填：否 - 加白内容使用base64编码 示例值：查看
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Order	否	否	String	排序升序还是倒序，DESC有ASC、 示例值： ASC

3. 输出参数

参数名称	类型	描述
List	Array of MemShellRule	列表内容 示例值：查看
TotalCount	Uint64	总条数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取反弹Shell列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取反弹Shell列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-06 15:48:41。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	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：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序字段：CreateTime-发生时间 示例值： CreateTime
Filters	否	否	Array of Filter	过滤条件。 • MachineName - String - 是否必填：否 - 主机别名 • Ip - String - 是否必填：否 - 主机ip • InstanceID - String - 是否必填：否 - 主机实例ID • CreateBeginTime - String - 是否必填：否 - 发现时间范围的开始时间 • CreateEndTime - String - 是否必填：否 - 发现时间范围的结束时间 • Status - string - 是否必填：否 - 状态 0 待处理、2 已加白、 3 已处理、4 已忽略、 5 已删除 • DetectBy - String - 是否必填：否 - 检测方式 0行为分析、1命令特征检测 • InnerNetAlarmShow - String - 是否必填：否 - 是否展示内网数据 1是 0否 • ProcName - String - 是否必填：否 - 进程名 • Uuid - String - 是否必填：否 - 主机安全唯一Uuid

参数名称	必选	允许NULL	类型	描述
				• Quuid - String - 是否必填：否 - 主机Quuid 示例值：查看
Limit	否	否	Uint64	返回数量，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Order	否	否	String	排序方式：根据请求次数排序：asc-升序/desc-降序 示例值： desc

3. 输出参数

参数名称	类型	描述
List	Array of ReverseShell	列表内容 示例值：查看
TotalCount	Uint64	总条数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。

错误码	描述
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取反弹Shell规则列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取反弹Shell规则列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeReverseShellRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • Keywords - String - 是否必填：否 - 关键字(进程名称) 示例值：查看
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
List	Array of ReverseShellRule	列表内容 示例值：查看
TotalCount	Uint64	总条数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
LimitExceeded.AreaQuota	超出批量添加数量。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter.DateRange	时间区间格式错误。
InvalidParameter.RegexRuleError	正则参数格式错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取反弹Shell规则列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取反弹Shell规则列表-聚合版本

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeReverseShellRulesAggregation
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序字段，目前有：CreateTime、ModifyTime，默认按照ModifyTime排序 示例值： ModifyTime
Filters	否	否	Array of Filter	过滤条件。 • Keywords - String - 是否必填：否 - 关键字(进程名称) • WhiteType - String - 是否必填：否 - 规则类型 1正则 0普通 示例值：查看
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

参数名称	必选	允许NULL	类型	描述
Order	否	否	String	排序升序还是倒序，DESC有ASC、 示例值： ASC

3. 输出参数

参数名称	类型	描述
List	Array of ReverseShellRuleAggregation	列表内容 示例值：查看
TotalCount	Uint64	总条数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

查询反弹shell系统策略配置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询反弹shell系统策略配置

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeReverseShellSystemPolicyConfig
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
InnerIPShow	Bool	内网ip展示 示例值： true
InnerNetAlarmShow	Bool	内网告警展示 示例值： true
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

查询反弹shell策略列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询反弹shell策略列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeShellPolicyList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列:[UpdateTime,CreateTime] 示例值： CreateTime
Filters	否	否	Array of Filters	过滤参数 Id,IdIn 示例值：查看
Limit	否	否	Uint64	限制条数,默认10 示例值： 10
Offset	否	否	Uint64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
List	Array of ShellPolicyList	列表数据 示例值：查看
TotalCount	Uint64	总条数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

导出反弹Shell事件

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出反弹Shell事件

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportReverseShellEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 • MachineName - String - 是否必填：否 - 主机别名 • Ip - String - 是否必填：否 - 主机ip • InstanceID - String - 是否必填：否 - 主机实例ID • CreateBeginTime - String - 是否必填：否 - 发现时间范围的开始时间 • CreateEndTime - String - 是否必填：否 - 发现时间范围的结束时间 • Status - string - 是否必填：否 - 状态 0 待处理、2 已加白、 3 已处理、4 已忽略、 5 已删除 • DetectBy - String - 是否必填：否 - 检测方式 0行为分析、1命令特征检测 • InnerNetAlarmShow - String - 是否必填：否 - 是否展示内网数据 1是 0否 • ProcName - String - 是否必填：否 - 进程名 • Uuid - String - 是否必填：否 - 主机安全唯一Uuid • Quuid - String - 是否必填：否 - 主机Quuid

参数名称	必选	允许NULL	类型	描述
				示例值：查看

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	该参数已废弃 示例值： http://www.ay.com/ay
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
FailedOperation.Export	导出文件失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

编辑反弹Shell规则（支持多服务器选择）

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

编辑反弹Shell规则（支持多服务器选择）-聚合版本-支持正则

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyReverseShellRulesAggregation
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
DestIp	否	否	String	目标IP 示例值： 172.17.0.2
DestPort	否	否	String	目标端口 示例值： 80
EventId	否	否	Uint64	事件列表和详情点击加白时关联的事件id (新增规则时请留空) 示例值： 12
GroupID	否	否	String	批次id 示例值： 85c909fe-c87c-11e9-a100-5cb90191ae78
HandleHistory	否	否	Uint64	处理历史事件， 0:不处理 1:处理 示例值： 1

参数名称	必选	允许NULL	类型	描述
HostIp	否	否	String	主机IP 示例值： 172.17.0.2
Id	否	否	Uint64	规则ID(新增时请留空) 示例值： 1
IsGlobal	否	否	Uint64	是否全局规则(默认否) 示例值： 1
ProcessName	否	否	String	进程名 示例值： nginx
RuleRegexp	否	否	String	正则表达式,base64编码 示例值： c2ggcmVkaXMuc2g=
Uuids	否	否	Array of String	客户端ID数组 示例值： ["a9fe0359-04d9-417f-ab6d-4941891d6c4b"]
WhiteType	否	否	Uint64	加白方式， 0:常规加白 1:正则加白 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。

错误码	描述
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

修改反弹shell系统策略配置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

修改反弹shell系统策略配置

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyReverseShellSystemPolicyConfig
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
InnerIPShow	是	否	Bool	内网ip展示 示例值： true
InnerNetAlarmShow	是	否	Bool	内网告警展示 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

编辑反弹shell策略开关

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

编辑反弹shell策略开关

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyShellPolicyStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
IsEnabled	否	否	Uint64	0 开启, 1关闭 示例值： 0
PolicyId	否	否	Uint64	策略ID 示例值： 2001

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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

入侵检测-密码破解相关接口
删除暴力破解记录

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (DeleteBruteAttacks) 用于删除暴力破解记录。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DeleteBruteAttacks
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	暴力破解事件Id数组。(最大 100条) 示例值： [1,2]

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取爆破阻断模式

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取爆破阻断模式

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeBanMode
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
Mode	String	阻断模式，STANDARD_MODE：标准阻断， DEEP_MODE：深度阻断 示例值： STANDARD_MODE
StandardModeConfig	StandardModeConfig	标准阻断模式的配置 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取阻断地域

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取阻断地域

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeBanRegions
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Mode	是	否	String	阻断模式，STANDARD_MODE：标准阻断，DEEP_MODE：深度阻断 示例值： STANDARD_MODE

3. 输出参数

参数名称	类型	描述
RegionSet	Array of RegionSet	地域信息列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取阻断按钮状态

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取阻断按钮状态

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeBanStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
OpenSmartMode	Bool	是否开启智能过白模式 示例值： true
ShowTips	Bool	是否弹窗提示信息 false: 关闭，true: 开启 示例值： false
Status	Uint64	阻断开关状态: 0 -- 关闭 1 -- 高级阻断 2 -- 基础阻断(只阻断情报库黑ip) 示例值： 1

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	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取阻断白名单列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取阻断白名单列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBanWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • Keywords - String - 是否必填：否 - 查询关键字 示例值：查看
Limit	否	否	Uint64	返回数量，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
TotalCount	Uint64	总记录数 示例值： 4
WhiteList	Array of BanWhiteListDetail	白名单列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取密码破解列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取密码破解列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-06 18:35:50。

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：DescribeBruteAttackList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序字段：CreateTime-首次攻击时间 示例值： CreateTime
Filters	否	否	Array of Filter	过滤条件。 • MachineName - String - 是否必填：否 - 主机别名筛选 • InstanceID - String - 是否必填：否 - 实例ID • Quuid - String - 是否必填：否 - 云服务器uuid • Status - String - 是否必填：否 - 状态筛选：失败：FAILED 成功：SUCCESS • UserName - String - 是否必填：否 - UserName筛选 • SrcIp - String - 是否必填：否 - 来源ip筛选 • CreateBeginTime - String - 是否必填：否 - 首次攻击时间筛选，开始时间 • CreateEndTime - String - 是否必填：否 - 首次攻击时间筛选，结束时间 • ModifyBeginTime - String - 是否必填：否 - 最近攻击时间筛选，开始时间 • ModifyEndTime - String - 是否必填：否 - 最近攻击时间筛选，结束时间

参数名称	必选	允许NULL	类型	描述
				• Banned - String - 是否必填：否 - 阻断状态筛选，多个用","分割：0-未阻断（全局ZK开关关闭），82-未阻断(非专业版)，83-未阻断(已加白名单)，1-阻断成功(已完成)，2-未阻断-程序异常，3-未阻断-内网攻击暂不支持阻断，4-未阻断-安平暂不支持阻断，10-阻断成功(生效中) • DataFrom - Int - 命中规则：0-登录规则，1-情报规则 • EventType - String - 是否必填：否 - 破解状态筛选：200-破解失败(密码错误),300-破解成功,400-破解失败(账号不存在) 示例值：查看
Limit	否	否	Uint64	需要返回的数量，最大值为100 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 1
Order	否	否	String	排序方式：根据请求次数排序：asc-升序/desc-降序 示例值： asc

3. 输出参数

参数名称	类型	描述
BruteAttackList	Array of BruteAttackInfo	密码破解列表 示例值：查看
TotalCount	Uint64	总数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。

错误码	描述
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.DateRange	时间区间格式错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取爆破破解规则

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取爆破破解规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeBruteAttackRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
Rules	Array of BruteAttackRuleList	爆破阻断规则列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

导出密码破解记录

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (ExportBruteAttacks) 用于导出密码破解记录成CSV文件。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：ExportBruteAttacks
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 • MachineName - String - 是否必填：否 - 主机别名筛选 • InstanceID - String - 是否必填：否 - 实例ID • Quuid - String - 是否必填：否 - 云服务器uuid • Status - String - 是否必填：否 - 状态筛选：失败：FAILED 成功：SUCCESS • UserName - String - 是否必填：否 - UserName筛选 • SrcIp - String - 是否必填：否 - 来源ip筛选 • CreateBeginTime - String - 是否必填：否 - 首次攻击时间筛选，开始时间 • CreateEndTime - String - 是否必填：否 - 首次攻击时间筛选，结束时间 • ModifyBeginTime - String - 是否必填：否 - 最近攻击时间筛选，开始时间 • ModifyEndTime - String - 是否必填：否 - 最近攻击时间筛选，结束时间 • Banned - String - 是否必填：否 - 阻断状态筛选，多个用","分割：0-未阻断（全局ZK开关关闭），82-未阻断(非专业版)，

参数名称	必选	允许NULL	类型	描述
				83-未阻断(已加白名单)，1-阻断成功(已完成)，2-未阻断-程序异常，3-未阻断-内网攻击暂不支持阻断，4-未阻断-安平暂不支持阻断，10-阻断成功(生效中) • DataFrom - Int - 命中规则：0-登录规则，1-情报规则 • EventType - String - 是否必填：否 - 破解状态筛选：200-破解失败(密码错误),300-破解成功,400-破解失败(账号不存在) 示例值：查看

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	该参数已废弃 示例值： http://www.ay.com/ay
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
FailedOperation.Export	导出文件失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

修改爆破阻断模式

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

修改爆破阻断模式

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：ModifyBanMode
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Mode	是	否	String	阻断模式，STANDARD_MODE：标准阻断，DEEP_MODE：深度阻断 示例值： STANDARD_MODE
Ttl	否	否	Uint64	阻断时间，用于标准阻断模式 示例值： 2

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

设置阻断开关状态

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

设置阻断开关状态

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：ModifyBanStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
OpenSmartMode	否	否	Bool	是否开启智能过白模式 示例值： true
Status	是	否	Uint64	阻断开关状态: 0 -- 关闭 1 -- 高级阻断 2 -- 基础阻断(只阻断情报库黑ip) 示例值： 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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameterValue	参数取值错误。

修改暴力破解规则

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

修改暴力破解规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：ModifyBruteAttackRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Rules	是	否	Array of BruteAttackRule	暴力破解判断规则 示例值：查看

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

不再提醒爆破阻断提示弹窗

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

不再提醒爆破阻断提示弹窗

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：StopNoticeBanTips
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息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
InternalError	内部错误。

入侵检测-异常登录相关接口
删除异地登录白名单规则

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口用于删除异地登录白名单规则。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DeleteLoginWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	白名单ID (最大 100 条) 示例值： [36040272]

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

删除异地登录记录

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (DeleteNonlocalLoginPlaces) 用于删除异地登录记录。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DeleteNonlocalLoginPlaces
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
DelType	否	否	String	删除异地登录事件的方式，可选值："Ids"、"Ip"、"All"，默认为Ids 示例值： Ip
Ids	否	否	Array of Uint64	异地登录事件ID数组。DelType为Ids或DelType未填时此项必填 示例值： [202417010656750]
Ip	否	否	Array of String	异地登录事件的Ip。DelType为Ip时必填 示例值： ["1.1.1.1"]
Uuid	否	否	String	主机Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
LimitExceeded.AreaQuota	超出批量添加数量。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取登录审计列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取登录审计列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-06 17:19:32。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeHostLoginList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序字段：LoginTime-发生时间 示例值： LoginTime
Filters	否	否	Array of Filter	过滤条件。 • Quuid - String - 是否必填：否 - 云服务器uuid • Uuid - String - 是否必填：否 - 主机安全唯一Uuid • MachineName - String - 是否必填：否 - 主机别名 • Ip - String - 是否必填：否 - 主机ip • InstanceID - String - 是否必填：否 - 主机实例ID • SrcIp - String - 是否必填：否 - 来源ip筛选 • UserName - String - 是否必填：否 - 用户名筛选 • Status - string - 是否必填：否 - 状态筛选1:正常登录；5：已加白,14:已处理，15：已忽略 • LoginTimeBegin - String - 是否必填：否 - 按照修改时间段筛选，开始时间 • LoginTimeEnd - String - 是否必填：否 - 按照修改时间段筛选，结束时间 • RiskLevel - string - 是否必填：否 - 状态筛选0:高危；1：可疑

参数名称	必选	允许NULL	类型	描述
				示例值：查看
Limit	否	否	Uint64	需要返回的数量，最大值为100 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 1
Order	否	否	String	排序方式：根据请求次数排序：asc-升序/desc-降序 示例值： asc

3. 输出参数

参数名称	类型	描述
HostLoginList	Array of HostLoginList	登录审计列表 示例值：查看
TotalCount	Uint64	总数 示例值： 12
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter.DateRange	时间区间格式错误。
InvalidParameter	参数错误。

错误码	描述
InvalidParameterValue	参数取值错误。

获取异地登录白名单合并后列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取异地登录白名单合并后列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-02-15 10:50:58。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeLoginWhiteCombinedList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 • UserName - String - 是否必填：否 - 用户名筛选 • SrcIP - String - 是否必填：否 - 来源IP筛选 • Location - String - 是否必填：否 - 登录地筛选 • ModifyBeginTime - String - 是否必填：否 - 按照修改时间段筛选，开始时间 • ModifyEndTime - String - 是否必填：否 - 按照修改时间段筛选，结束时间 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

3. 输出参数

参数名称	类型	描述
LoginWhiteCombinedInfos	Array of LoginWhiteCombinedInfo	合并后的白名单列表 示例值：查看
TotalCount	Uint64	总数量 示例值： 12
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取异地登录白名单列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取异地登录白名单列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeLoginWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • IpOrAlias - String - 是否必填：否 - 查询关键字 • UserName - String - 是否必填：否 - 用户名筛选 • ModifyBeginTime - String - 是否必填：否 - 按照修改时间段筛选，开始时间 • ModifyEndTime - String - 是否必填：否 - 按照修改时间段筛选，结束时间 示例值：查看
Limit	否	否	Uint64	返回数量，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

3. 输出参数

参数名称	类型	描述
LoginWhiteLists	Array of LoginWhiteLists	异地登录白名单数组 示例值：查看
TotalCount	Uint64	记录总数 示例值： 12
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询常用登录地

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

此接口（DescribeUsualLoginPlaces）用于查询常用登录地。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeUsualLoginPlaces
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Uuid	是	否	String	主机安全客户端UUID 示例值： d1245804-b922-4c3b-8499-f95dce26b33c

3. 输出参数

参数名称	类型	描述
UsualLoginPlaces	Array of UsualPlace	常用登录地数组 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
LimitExceeded.AreaQuota	超出批量添加数量。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

导出异地登录记录

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (ExportNonlocalLoginPlaces) 用于导出异地登录事件记录CSV文件。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：ExportNonlocalLoginPlaces
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • Quuid - String - 是否必填：否 - 云服务器uuid • Uuid - String - 是否必填：否 - 主机安全唯一Uuid • MachineName - String - 是否必填：否 - 主机别名 • Ip - String - 是否必填：否 - 主机ip • InstanceID - String - 是否必填：否 - 主机实例ID • SrcIp - String - 是否必填：否 - 来源ip筛选 • UserName - String - 是否必填：否 - 用户名筛选 • Status - string - 是否必填：否 - 状态筛选1:正常登录；5：已加白,14:已处理，15：已忽略 • LoginTimeBegin - String - 是否必填：否 - 按照修改时间段筛选，开始时间 • LoginTimeEnd - String - 是否必填：否 - 按照修改时间段筛选，结束时间 • RiskLevel - string - 是否必填：否 - 状态筛选0:高危；1：可疑 示例值：查看

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	该参数已废弃 示例值： http://www.ay.com/ay
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
FailedOperation.Export	导出文件失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

入侵检测-恶意请求相关接口
删除恶意请求记录

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (DeleteMaliciousRequests) 用于删除恶意请求记录。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DeleteMaliciousRequests
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	恶意请求记录ID数组，(最大100条) 示例值： [1002]

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
MissingParameter	缺少参数错误。
LimitExceeded.AreaQuota	超出批量添加数量。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询恶意请求白名单列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询恶意请求白名单列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMaliciousRequestWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序字段：CreateTime、LatestScanTime 示例值： CreateTime
Filters	否	否	Array of Filters	过滤条件。 • Domain - String - 域名使用Base64编码 示例值：查看
Limit	是	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
Offset	是	否	Uint64	偏移量，默认为0。 示例值： 0
Order	否	否	String	排序方式 [asc:升序

3. 输出参数

参数名称	类型	描述
List	Array of MaliciousRequestWhiteListInfo	白名单信息列表 示例值：查看
TotalCount	Uint64	分页查询记录总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取恶意请求列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

入侵检测，获取恶意请求列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-06 14:42:23。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	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：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序字段：AccessCount-请求次数。MergeTime-最近请求时间 示例值： AccessCount
Filters	否	否	Array of Filter	过滤条件。 • IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 • Url - String - 是否必填：否 - Url筛选 • Status - String - 是否必填：否 - 状态筛选0:待处理；2:信任；3:不信任 • MergeBeginTime - String - 是否必填：否 - 最近访问开始时间 • MergeEndTime - String - 是否必填：否 - 最近访问结束时间 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 10

参数名称	必选	允许NULL	类型	描述
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Order	否	否	String	排序方式：根据请求次数排序：asc-升序/desc-降序 示例值： asc

3. 输出参数

参数名称	类型	描述
RiskDnsList	Array of RiskDnsList	恶意请求列表数组 示例值：查看
TotalCount	Uint64	总数量 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

导出下载恶意请求文件

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (ExportMaliciousRequests) 用于导出下载恶意请求文件。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：ExportMaliciousRequests
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 • IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 • Url - String - 是否必填：否 - 访问域名筛选 • Status - String - 是否必填：否 - 状态筛选1 已删除、0 待处理、2 已加入白名单、 3 已取消加入白名单、4 标记已处理、 5 已忽略 • MergeBeginTime - String - 是否必填：否 - 创建时间筛选-开始时间 • MergeEndTime - String - 是否必填：否 - 创建时间筛选-结束时间 示例值：查看

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
DownloadUrl	String	该参数已废弃 示例值： http://www.ay.com/ay
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameterValue	参数取值错误。

入侵检测-文件查杀相关接口
创建网络攻击白名单

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：CreateNetAttackWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
DealOldEvents	否	否	Uint64	是否加白所有符合该规则的告警 ，1:处理,0:不处理 示例值： 1
Description	否	否	String	描述信息 示例值： any create description
EventId	否	否	Uint64	事件id 示例值： 1
QuuidList	否	否	Array of String	quuid 列表 示例值： ["5a540076-d38a-4078-aa98-qwert371d322"]
Scope	是	否	Uint64	是否全部主机； 0否，1是。 示例值： 1

参数名称	必选	允许NULL	类型	描述
SrcIp	是	否	Array of String	来源IP 单IP:1.1.1.1 IP范围:1.1.1.1-1.1.2.1 IP范围：1.1.1.0/24 示例值： ["1.1.1.1"]

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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

文件查杀检测

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

该接口可以对入侵检测-文件查杀扫描检测

默认接口请求频率限制：20次/秒。

接口更新时间：2022-11-03 19:52:53。

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：CreateScanMalwareSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
EnableMemShellScan	否	否	Int64	是否开启恶意进程查杀[0:未开启,1:开启] 示例值： 1
EngineType	否	否	Uint64	1标准模式（只报严重、高危）、2增强模式（报严重、高危、中危）、3严格模式（报严重、高、中、低、提示） 示例值： 2
HostType	是	否	Int64	服务器分类：1:专业版服务器；2:自选服务器 示例值： 1
QuuidList	否	否	Array of String	自选服务器时生效，主机quuid的string数组 示例值： ["a15a2cac-0bea-478d-a5d0-f54be8ayayay""]
ScanPattern	是	否	Uint64	扫描模式 0 全盘扫描, 1 快速扫描 示例值： 1

参数名称	必选	允许NULL	类型	描述
TimeoutPeriod	否	否	Uint64	超时时间单位 秒 默认3600 秒 示例值： 1

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	任务id 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter.DateRange	时间区间格式错误。
FailedOperation.APIServerFail	调用API服务失败。
FailedOperation.NoProfessionHost	无专业版主机。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

错误码	描述
FailedOperation	操作失败。

入侵管理-终止扫描任务

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

入侵管理-终止扫描任务

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteMalwareScanTask
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息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
InternalError	内部错误。

错误码	描述
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
FailedOperation.APIServerFail	调用API服务失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

删除木马记录

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (DeleteMalwares) 用于删除木马记录。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteMalwares
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	木马记录ID数组 (最大100条) 示例值： [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

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameterValue	参数取值错误。

删除网络攻击白名单

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DeleteNetAttackWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组，最大100条。 示例值： [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

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

查询java内存马事件列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询java内存马事件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-04-22 09:49:39。

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：DescribeJavaMemShellList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件：InstanceID、IP、 MachineName主机名模糊查询, Type，Status精确匹配，CreateBeginTime，CreateEndTime时间段 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
List	Array of JavaMemShellInfo	事件列表 示例值：查看
TotalCount	Uint64	总数 示例值： 12
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取木马列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

入侵检测获取木马列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-02-22 18:20:24。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMalWareList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	检测排序 CreateTime 示例值： CreateTime
Filters	否	否	Array of Filter	过滤条件。 • IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 • FilePath - String - 是否必填：否 - 路径筛选 • VirusName - String - 是否必填：否 - 病毒名筛选 • CreateBeginTime - String - 是否必填：否 - 创建时间筛选-开始时间 • CreateEndTime - String - 是否必填：否 - 创建时间筛选-结束时间 • Status - String - 是否必填：否 - 状态筛选 4待处理,5信任,6已隔离,10隔离中,11恢复隔离中,14 已处理 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 10

参数名称	必选	允许NULL	类型	描述
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Order	否	否	String	排序方式 ASC,DESC 示例值： ASC

3. 输出参数

参数名称	类型	描述
MalWareList	Array of MalWareList	木马列表 示例值：查看
TotalCount	Uint64	总数量 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取木马文件下载地址

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取木马文件下载地址

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMalwareFile
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	Uint64	木马记录ID 示例值： 1

3. 输出参数

参数名称	类型	描述
FileName	String	保存文件名 示例值： tmp
FileUrl	String	木马文件下载地址 示例值： www.domain.com/1.txt
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查看恶意文件详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查看恶意文件详情

默认接口请求频率限制：20次/秒。

接口更新时间：2021-12-09 20:22:45。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMalwareInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	Int64	唯一ID 示例值： 1023290

3. 输出参数

参数名称	类型	描述
MalwareInfo	MalwareInfo	恶意文件详情信息 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
FailedOperation.APIServerFail	调用API服务失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

风险预警提示

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

打开入侵检测-恶意文件检测,弹出风险预警内容

默认接口请求频率限制：20次/秒。

接口更新时间：2022-11-03 19:53:29。

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：DescribeMalwareRiskWarning
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
IsCheckRisk	Bool	是否开启自动扫描：true-开启，false-未开启 示例值： true
IsPop	Bool	是否弹出提示 true 弹出, false不弹 示例值： true
List	Array of MalwareRisk	风险文件列表信息 示例值：查看
ProcessList	Array of MalwareRisk	异常进程列表信息 示例值：查看

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	内部错误。

查询定时扫描配置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询定时扫描配置

默认接口请求频率限制：20次/秒。

接口更新时间：2022-10-25 19:31:47。

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：DescribeMalwareTimingScanSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AutoIsolation	Uint64	是否自动隔离：1-是，0-否 示例值： 1
CheckPattern	Uint64	检测模式 0 全盘检测 1快速检测 示例值： 1
ClickTimeout	Uint64	一键扫描超时时长，如：1800秒（s） 示例值： 60
Cycle	Uint64	周期 1每天 示例值： 1

参数名称	类型	描述
EnableInspiredEngine	Uint64	启发引擎 0 关闭 1开启 示例值： 1
EnableMemShellScan	Uint64	是否开启恶意进程查杀[0:未开启,1:开启] 示例值： 1
EnableScan	Int64	定时检测开关 0 关闭1 开启 示例值： 1
EndTime	String	检测周期 超时结束时间 示例值： 18:00
EngineType	Uint64	1标准模式（只报严重、高危）、2增强模式（报严重、高危、中危）、3严格模式（报严重、高、中、低、提示） 示例值： 1
Id	Int64	唯一ID 示例值： 1
IsGlobal	Uint64	是否全部服务器 1 全部 2 自选 示例值： 1
KillProcess	Uint64	是否杀掉进程 1杀掉 0不杀掉 只有开启自动隔离才生效 示例值： 1
MonitoringPattern	Uint64	监控模式 0 标准 1深度 示例值： 1
ProtectFileScope	Uint64	查杀范围 0 脚本类之外的恶意文件，1全部恶意文件 示例值： 0
ProtectMode	Uint64	防护模式 0 标准 1 重保 示例值： 0
QuuidList	Array of String	自选服务器时必须 主机quuid的string数组 示例值： ["972290ce-2e07-4689-8f92-f617239bbf82"]
RealTimeMonitoring	Int64	实时监控0 关闭 1开启 示例值： 1
StartTime	String	检测周期 开始时间 示例值： 00:00
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

获取网络攻击白名单列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeNetAttackWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [CreateTime] 示例值： CreateTime
Filters	否	否	Array of Filter	过滤条件。 • IP - String - 是否必填：否 - 主机ip查询 • SrcIP- String - 是否必填：否 - 白名单ip查询 示例值：查看
Limit	否	否	Uint64	返回数量，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	总记录数 示例值： 4
WhiteList	Array of NetAttackWhiteRule	白名单列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

查询木马扫描进度

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询木马扫描进度

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeScanMalwareSchedule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
IsSchedule	Bool	是否正在扫描中 示例值： true
RiskFileNumber	Int64	风险文件数,当进度满了以后才有该值 示例值： 1
ScanStatus	Uint64	0 从未扫描过、 1 扫描中、 2扫描完成、 3停止中、 4停止完成 示例值： 1
Schedule	Int64	扫描进度（单位：%） 示例值： 1

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	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获文件查杀概览信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取待处理风险文件数+影响服务器数+是否试用检测+最近检测时间

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeServersAndRiskAndFirstInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AddRiskFileCount	Uint64	今日新增风险文件数 示例值： 1
IsFirstCheck	Bool	是否试用：true-是，false-否 示例值： true
RiskFileCount	Uint64	风险文件数 示例值： 1
ScanTime	String	木马最近检测时间 示例值： 2024-10-28 20:23:23

参数名称	类型	描述
ServersCount	Uint64	受影响服务器台数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

导出木马记录

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (ExportMalwares) 用于导出木马记录CSV文件。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportMalwares
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序值 CreateTime、LatestScanTime 示例值： CreateTime
Filters	否	否	Array of Filters	过滤参数 • MachineName - String - 是否必填：否 - 主机名称 • FilePath - String - 是否必填：否 - 路径筛选 • VirusName - String - 是否必填：否 - 病毒名筛选 • CreateBeginTime - String - 是否必填：否 - 创建时间筛选-开始时间 • CreateEndTime - String - 是否必填：否 - 创建时间筛选-结束时间 • Status - String - 是否必填：否 - 状态筛选4 待处理、5 信任文件、6 已隔离、8 文件已删除、10 隔离中、11 恢复中、14 已处理 示例值：查看

参数名称	必选	允许NULL	类型	描述
Limit	否	否	Uint64	限制条数,默认10 示例值： 10
Offset	否	否	Uint64	偏移量 默认0 示例值： 0
Order	否	否	String	排序 方式 ，ASC，DESC 示例值： ASC

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	该参数已废弃 示例值： http://www.ay.com/ay
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
FailedOperation.Export	导出文件失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

定时扫描设置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

定时扫描设置

默认接口请求频率限制：20次/秒。

接口更新时间：2022-11-03 19:52:01。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyMalwareTimingScanSettings
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
AutoIsolation	否	否	Uint64	是否自动隔离 1隔离 0 不隔离 示例值： 1
CheckPattern	是	否	Uint64	检测模式 0 全盘检测 1快速检测 示例值： 1
Cycle	是	否	Uint64	扫描周期 默认每天 1 示例值： 1
DoClean	否	否	Uint64	1 清理, 0 不清理 • 本操作会修复被篡改的系统命令，计划任务等系统文件，操作中请确保yum/apt 可用 示例值： 1
EnableInspiredEngine	否	否	Uint64	启发引擎开关 0 关闭 1开启 示例值： 1

参数名称	必选	允许NULL	类型	描述
EnableMemShellScan	否	否	Uint64	是否开启恶意进程查杀[0:未开启,1:开启] 示例值： 1
EnableScan	是	否	Uint64	定时检测开关 0 关闭 1开启 示例值： 1
EndTime	是	否	String	检测周期 超时结束时间，如：04:00:00 示例值： 02:00:00
EngineType	否	否	Uint64	1标准模式（只报严重、高危）、2增强模式（报严重、高危、中危）、3严格模式（报严重、高、中、低、提示） 示例值： 1
IsGlobal	是	否	Uint64	是否全部服务器 1 全部 2 自选 示例值： 1
KillProcess	否	否	Uint64	是否杀掉进程 1杀掉 0不杀掉 示例值： 1
MonitoringPattern	是	否	Uint64	监控模式 0 标准 1深度 示例值： 1
ProtectFileScope	否	否	Uint64	查杀范围 0 脚本类之外的恶意文件，1全部恶意文件 示例值： 0
ProtectMode	否	否	Uint64	防护模式 0 标准 1重保 示例值： 0
QuuidList	否	否	Array of String	自选服务器时必须 主机quuid的string数组 示例值： ["5a540076-d38a-4078-aa98-q45rt371d322"]
RealTimeMonitoring	是	否	Uint64	实时监控 0 关闭 1开启 示例值： 1
StartTime	是	否	String	检测周期 开始时间，如：02:00:00 示例值： 00:00:00

3. 输出参数

参数名称	类型	描述

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	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter.DateRange	时间区间格式错误。
FailedOperation.APIServerFail	调用API服务失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

编辑网络攻击白名单

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyNetAttackWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
DealOldEvents	是	否	Uint64	是否加白所有符合该规则的告警 ，1:处理,0:不处理 示例值： 1
Description	否	否	String	规则描述 示例值： from redis node check
Id	是	否	Uint64	规则id 示例值： 1
QuuidList	否	否	Array of String	quuid 列表 示例值： ["1c26308c-5493-4eaf-a817-112ec25f499e"]
Scope	是	否	Uint64	是否全部主机； 0否，1是。 示例值： 1

参数名称	必选	允许NULL	类型	描述
SrcIp	是	否	Array of String	来源IP 单IP:1.1.1.1 IP范围:1.1.1.1-1.1.2.1 IP范围：1.1.1.0/24 示例值： ["1.1.1.1"]

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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

恢复木马文件

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口（RecoverMalwares）用于批量恢复已经被隔离的木马文件。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：RecoverMalwares
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	木马Id数组（最大100条） 示例值： [1002,1003]

3. 输出参数

参数名称	类型	描述
FailedIds	Array of Uint64	恢复失败id数组，若无则返回空数组 示例值： [1003]
SuccessIds	Array of Uint64	恢复成功id数组，若无则返回空数组 示例值： [1002]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
FailedOperation.Recover	回复木马失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

隔离木马

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口（SeparateMalwares）用于隔离木马。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：SeparateMalwares
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	木马事件ID数组。(最大100条) 示例值： [300005850594]
KillProcess	否	否	Bool	是否杀掉进程 示例值： true

3. 输出参数

参数名称	类型	描述
FailedIds	Array of Uint64	隔离失败的ID数组，若无则返回空数组 示例值： [300005850595]
SuccessIds	Array of Uint64	隔离成功的ID数组，若无则返回空数组 示例值： [300005850594]

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	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
FailedOperation.PartSeparate	多台主机隔离，部分或全部失败。
FailedOperation.SingleSeparate	单台主机隔离失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

信任木马文件

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口(TrustMalwares)将被识别木马文件设为信任。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：TrustMalwares
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	木马ID数组（单次不超过的最大条数：100） 示例值： [300005556389]

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
LimitExceeded.AreaQuota	超出批量添加数量。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

取消信任木马

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口（UntrustMalwares）用于取消信任木马文件。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：UntrustMalwares
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	木马ID数组 (最大100条) 示例值： [300005556389]

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

入侵检测-本地提权相关接口
删除本地提权事件

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据Ids删除本地提权

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DeletePrivilegeEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组. (最大100条) 示例值： [1,2,3]

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

删除本地提权规则

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除本地提权规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DeletePrivilegeRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组，最大100条。 示例值： [1,2]

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
LimitExceeded.AreaQuota	超出批量添加数量。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter.DateRange	时间区间格式错误。
InvalidParameter.RegexRuleError	正则参数格式错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取本地提权事件列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取本地提权事件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-06 15:33:40。

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：DescribePrivilegeEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序字段：CreateTime-发现时间 示例值： CreateTime
Filters	否	否	Array of Filter	过滤条件。 • CreateBeginTime - String - 是否必填：否 - 发现时间 • CreateEndTime - String - 是否必填：否 - 发现时间范围 • Status - String - 是否必填：否 - 处理状态0 待处理、2 已加白、 3 已处理、 4已忽略、5 已删除 • ParentProcName - String - 是否必填：否 - 父进程 • InstanceID - String - 是否必填：否 - 主机实例ID • IP - String - 是否必填：否 - 主机IP • MachineName - String - 是否必填：否 - 主机名称 示例值：查看
Limit	否	否	Uint64	返回数量，最大值为100。 示例值： 10

参数名称	必选	允许NULL	类型	描述
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Order	否	否	String	排序方式：根据请求次数排序：asc-升序/desc-降序 示例值： desc

3. 输出参数

参数名称	类型	描述
List	Array of PrivilegeEscalationProcess	数据列表 示例值：查看
TotalCount	Uint64	总条数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取本地提权规则列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取本地提权规则列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribePrivilegeRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • Keywords - String - 是否必填：否 - 关键字(进程名称) • SMode - String - 是否必填：否 - 是否带S 1是0否 示例值：查看
Limit	否	否	Uint64	返回数量，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
List	Array of PrivilegeRule	列表内容 示例值：查看
TotalCount	Uint64	总条数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

导出本地提权事件

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出本地提权事件

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：ExportPrivilegeEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 • CreateBeginTime - String - 是否必填：否 - 发现时间 • CreateEndTime - String - 是否必填：否 - 发现时间范围 • Status - String - 是否必填：否 - 处理状态0 待处理、2 已加白、 3 已处理、 4已忽略、5 已删除 • ParentProcName - String - 是否必填：否 - 父进程 • InstanceID - String - 是否必填：否 - 主机实例ID • IP - String - 是否必填：否 - 主机IP • MachineName - String - 是否必填：否 - 主机名称 示例值：查看

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
DownloadUrl	String	该参数已废弃 示例值： http://www.ay.com/ay
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 1596595610
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
FailedOperation.Export	导出文件失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

入侵检测-高危命令相关接口
校验高危命新增用户规则参数

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

校验高危命令用户规则新增和编辑时的参数。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：CheckBashRuleParams
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
CheckField	是	否	String	校验内容 Name或Rule ，两个都要校验时逗号分割 示例值： Name,Rule
EventId	否	否	Uint64	在事件列表中新增白名时需要提交事件ID 示例值： 10003
Id	否	否	Uint64	编辑时传的规则id 示例值： 3680
Name	否	否	String	填入的规则名称 示例值： 规则1
Rule	否	否	String	用户填入的正则表达式："正则表达式" 需与 "提交EventId对应的命令内容" 相匹配 示例值： rm -rf /tmp/tmp

3. 输出参数

参数名称	类型	描述
ErrCode	Uint64	0=校验通过 1=规则名称校验不通过 2=正则表达式校验不通过 示例值： 2
ErrMsg	String	校验信息 示例值： OK
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
InvalidParameter	参数错误。

删除高危命令事件

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据Ids删除高危命令事件

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DeleteBashEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组，最大1000条。 示例值： [1002]

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
LimitExceeded.AreaQuota	超出批量添加数量。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

删除高危命令规则

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除高危命令规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DeleteBashRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组，最大100条。 示例值： [1,23,100]

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
LimitExceeded.AreaQuota	超出批量添加数量。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter.DateRange	时间区间格式错误。
InvalidParameter.RegexRuleError	正则参数格式错误。

获取高危命令列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取高危命令列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-06 14:53:54。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBashEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序字段：CreateTime-发生时间。ModifyTime-处理时间 示例值： CreateTime
Filters	否	否	Array of Filter	过滤条件。 • HostName - String - 是否必填：否 - 主机名 • Hostip - String - 是否必填：否 - 主机内网IP • RuleCategory - Int - 是否必填：否 - 策略类型,全部或者单选(0:系统 1:用户) • RuleName - String - 是否必填：否 - 策略名称 • RuleLevel - Int - 是否必填：否 - 威胁等级,可以多选 • Status - Int - 是否必填：否 - 处理状态,可多选(0:待处理 1:已处理 2:已加白 3:已忽略 4:已删除 5:已拦截) • DetectBy - Int - 是否必填：否 - 数据来源,可多选(0:bash日志 1:实时监控) • StartTime - String - 是否必填：否 - 开始时间 • EndTime - String - 是否必填：否 - 结束时间 示例值：查看

参数名称	必选	允许NULL	类型	描述
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Order	否	否	String	排序方式：根据请求次数排序：asc-升序/desc-降序 示例值： asc

3. 输出参数

参数名称	类型	描述
List	Array of BashEvent	高危命令事件列表 示例值：查看
TotalCount	Uint64	总条数 示例值： 1021
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。

错误码	描述
InvalidParameterValue	参数取值错误。

获取高危命令列表(新)

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取高危命令列表(新)

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-19 20:56:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBashEventsNew
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序字段：CreateTime-发生时间。ModifyTime-处理时间 示例值： CreateTime

参数名称	必选	允许NULL	类型	描述
Filters	否	否	Array of Filter	过滤条件。 • HostName - String - 是否必填：否 - 主机名 • Hostip - String - 是否必填：否 - 主机内网IP • HostIp - String - 是否必填：否 - 主机内网IP • RuleCategory - Int - 是否必填：否 - 策略类型,全部或者单选(0:系统 1:用户) • RuleName - String - 是否必填：否 - 策略名称 • RuleLevel - Int - 是否必填：否 - 威胁等级,可以多选 • Status - Int - 是否必填：否 - 处理状态,可多选(0:待处理 1:已处理 2:已加白 3:已忽略 4:已删除 5:已拦截) • DetectBy - Int - 是否必填：否 - 数据来源,可多选(0:bash日志 1:实时监控) • StartTime - String - 是否必填：否 - 开始时间 • EndTime - String - 是否必填：否 - 结束时间 示例值：查看
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Order	否	否	String	排序方式：根据请求次数排序：asc-升序/desc-降序 示例值： asc

3. 输出参数

参数名称	类型	描述
List	Array of BashEventNew	高危命令事件列表 示例值：查看
TotalCount	Uint64	总条数 示例值： 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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

获取高危命令规则列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取高危命令规则列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeBashRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • Name - String - 是否必填：否 - 规则名称 • Rule - String - 是否必填：否 - 规则内容 • Level - Int - 是否必填：否 - 威胁等级 • White - Int - 是否必填：否 - 白名单类型 • RuleCategory - Int - 是否必填：否 - 策略类型 • BashAction - Int - 是否必填：否 - 操作动作 • Status - Int - 是否必填：否 - 生效状态 示例值：查看
Limit	否	否	Uint64	返回数量，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Type	是	否	Uint64	0-系统规则; 1-用户规则 示例值： 1

3. 输出参数

参数名称	类型	描述
List	Array of BashRule	列表内容 示例值：查看
TotalCount	Uint64	总条数 示例值： 12
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

新增或修改高危命令规则（支持多服务器选择）

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

新增或修改高危命令规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：EditBashRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
DealOldEvents	否	否	Uint64	是否处理旧事件为白名单 0=不处理 1=处理 示例值： 1
EventId	否	否	Uint64	事件列表点击"加入白名单"时,需要传EventId 事件的id 示例值： 10023
HostIp	否	否	String	主机IP 示例值： 1.1.1.1
Id	否	否	Uint64	规则ID（新增时不填） 示例值： 1
IsGlobal	否	否	Uint64	是否全局规则(默认否)：1-全局，0-非全局 示例值： 1

参数名称	必选	允许NULL	类型	描述
Level	否	否	Uint64	危险等级(0:无，1: 高危 2:中危 3: 低危) 示例值： 1
Name	否	否	String	规则名称，编辑时不可修改规则名称 示例值： 规则名称
Rule	否	否	String	接口已废弃，请使用新接口ModifyBashPolicy 示例值： sh cmdline
Uuids	否	否	Array of String	客户端ID数组 示例值： ["05f0bcab-726c-4ea4-8109-bcd03d5598f7"]
White	否	否	Uint64	0=黑名单， 1=白名单 示例值： 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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.RegexRuleError	正则参数格式错误。
InvalidParameter.RuleHostipErr	规则类接口，主机IP不正确。

错误码	描述
InvalidParameter.IpNoValid	IP格式不合法。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

导出高危命令事件

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出高危命令事件

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：ExportBashEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 • HostName - String - 是否必填：否 - 主机名 • Hostip - String - 是否必填：否 - 主机内网IP • RuleCategory - Int - 是否必填：否 - 策略类型,全部或者单选(0:系统 1:用户) • RuleName - String - 是否必填：否 - 策略名称 • RuleLevel - Int - 是否必填：否 - 威胁等级,可以多选 • Status - Int - 是否必填：否 - 处理状态,可多选(0:待处理 1:已处理 2:已加白 3:已忽略 4:已删除 5:已拦截) • DetectBy - Int - 是否必填：否 - 数据来源,可多选(0:bash日志 1:实时监控) • StartTime - String - 是否必填：否 - 开始时间 • EndTime - String - 是否必填：否 - 结束时间 示例值：查看

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出文件下载链接地址。 示例值： http://www.ay.com/ay
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
FailedOperation.Export	导出文件失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

设置高危命令事件状态

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

设置高危命令事件状态

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：SetBashEventsStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组，最大100条。 示例值： [1,2]
Status	是	否	Uint64	新状态(0-待处理 1-高危 2-正常) 示例值： 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
InternalError	内部错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
LimitExceeded.AreaQuota	超出批量添加数量。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameterValue	参数取值错误。

切换高危命令规则状态

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

切换高危命令规则状态

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：SwitchBashRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Disabled	是	否	Uint64	是否禁用 示例值： 1
Id	是	否	Uint64	规则ID 示例值： 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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
LimitExceeded.AreaQuota	超出批量添加数量。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter.DateRange	时间区间格式错误。
InvalidParameter.RegexRuleError	正则参数格式错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

其他接口
下发登录许可

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

下发登录许可

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：CreateLoginPermissionPush
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
InstanceId	否	否	String	主机InstanceId和uuid至少需要填一个 示例值： inst-anyinst
MemberId	否	否	Array of String	集团账号的成员id 示例值：[{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
NonceData	是	否	String	登录随机码 示例值： 8095
Uuid	否	否	String	主机InstanceId和uuid至少需要填一个 示例值： 5a540076-d38a-4078-aa98-qwert371d322

3. 输出参数

参数名称	类型	描述
ResultCode	Int64	0-成功； 1-失败--无登录权限； 2-失败--未安装agent； 3-失败--agent离线； 4-失败--发送超时，请重试； 5-失败--未知失败； 示例值： 0
ResultMessage	String	下发失败的原因 示例值： 异常信息
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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

修改日志cls投递配置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除日志cls投递配置

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DeleteLogClsDeliverInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
SecurityType	是	否	Uint64	安全模块类型 1: 入侵检测 2: 漏洞管理 3: 基线管理 4: 高级防御 5:客户端相关 6: 资产指纹 7 主机列表 8 客户端上报 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

停止扫描任务

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

DeleteScanTask 该接口可以对指定类型的扫描任务进行停止扫描;

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DeleteScanTask
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
ModuleType	是	否	String	模块类型 当前提供 Malware 木马，Vul 漏洞 示例值： Vul
QuuidList	否	否	Array of String	自选服务器时生效，主机quuid的string数组 示例值： ["17d8ad3a-afbb-44a8-8b9e-99a92160f367"]
TaskId	是	否	Uint64	任务Id 示例值： 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
InternalError	内部错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
FailedOperation.APIServerFail	调用API服务失败。
InvalidParameter	参数错误。
AuthFailure	CAM签名/鉴权错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

查询资产管理环境变量列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询资产管理环境变量列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetEnvList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime] 示例值： FirstTime
Filters	否	否	Array of AssetFilters	过滤条件。 • MachineName- String - 是否必填：否 - 主机别名筛选 • IP- String - 是否必填：否 - 主机ip筛选 • InstanceID- String - 是否必填：否 - 主机实例ID筛选 • User- string - 是否必填：否 - 用户 • Name - String - 是否必填：否 - 环境变量名 • Type- int - 是否必填：否 - 类型：0用户变量，1系统变量 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 10

参数名称	必选	允许NULL	类型	描述
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 1
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： desc
Quuid	否	否	String	服务器Quuid 示例值： 1c26308c-5493-4eaf-a817-112ec25f499e
Type	否	否	Uint64	该字段已废弃，由Filters代替 示例值： 1
Uuid	否	否	String	服务器Uuid 示例值： 1c26308c-5493-4eaf-a817-112ec25f499e

3. 输出参数

参数名称	类型	描述
Envs	Array of AssetEnvBaseInfo	列表 示例值：查看
Total	Uint64	总数量 示例值： 1021
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。

错误码	描述
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取客户端异常事件

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取客户端异常事件

默认接口请求频率限制：20次/秒。

接口更新时间：2022-11-16 10:43:36。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeClientException
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
EndTime	否	否	String	结束时间 2006-01-02 15:04:05 格式 示例值： 2006-01-02 15:04:05
ExceptionType	是	否	Int64	客户端异常类型 1:客户端离线，2:客户端卸载 示例值： 1
Limit	是	否	Uint64	分页单页限制数目，不为0，最大值100 示例值： 10
Offset	是	否	Uint64	分页的偏移量 示例值： 0
StartTime	否	否	String	起始时间 2006-01-02 15:04:05 格式 示例值： 2006-01-02 15:04:05

3. 输出参数

参数名称	类型	描述
Records	Array of RecordInfo	事件详情 示例值：查看
TotalCount	Uint64	事件总数量 示例值： 944
RequestId	String	唯一请求 ID，每次请求都会返回。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cls账户状态

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询cls账户状态

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeClsAccountStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AccountStatus	Uint64	0: 未开通，1:正常，2: 欠费， 3: 销毁 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

查询cls日志集列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询cls日志集列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeClsLogsets
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件 示例值：查看
Limit	否	否	Uint64	最大值为100 示例值： 10
LogsetRegion	是	否	String	日志集地域 示例值： ap-region1
Offset	否	否	Uint64	偏移量，默认为0 示例值： 0

3. 输出参数

参数名称	类型	描述
List	Array of	列表

参数名称	类型	描述
	ClsLogsetInfo	示例值：查看
TotalCount	Uint64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

查询cls日志集列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询cls日志主题列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeClsTopics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Limit	否	否	Uint64	最大 示例值： 10
LogsetId	否	否	String	日志集ID 示例值： any data
LogsetRegion	是	否	String	日志集地域 示例值： ap-region1
Offset	否	否	Uint64	偏移量 示例值： 0

3. 输出参数

参数名称	类型	描述
List	Array of	列表

参数名称	类型	描述
	ClsTopicInfo	示例值：查看
TotalCount	Uint64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

查询客户信息客户级别,是否企业客户

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询客户信息

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeCustomerDetail
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
IsEnterprise	Bool	是否企业客户 示例值： false
Level	String	级别 HEAD头部 WAIST腰部 TAIL尾部 示例值： HEAD
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取主机相关统计

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取主机相关统计

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-19 10:10:24。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeGeneralStat
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤参数 CloudFrom:0 云平台、1 Other、2 阿里云、3 华为云、4 亚马逊、5 微软、6 Google、7 Oracle、8 Digital Ocean、9 百度 示例值：查看
MachineRegion	否	否	String	机器所属地域 示例值： ap-region1
MachineType	否	否	String	云主机类型。 • CVM：表示云服务器 • BM：表示黑石物理机 • ECM：表示边缘计算服务器 • LH：表示轻量应用服务器 • Other：表示混合云机器 示例值： CVM

3. 输出参数

参数名称	类型	描述
AddedOnTheFifteen	Uint64	15天内新增的主机数 示例值： 12
AgentsAll	Uint64	主机安全客户端总数的总数 示例值： 2
AgentsBasic	Uint64	主机安全客户端基础版的总数 示例值： 15
AgentsOffline	Uint64	主机安全客户端 离线+关机 的总数 示例值： 4
AgentsOnline	Uint64	主机安全客户端在线的总数 示例值： 8
AgentsPro	Uint64	主机安全客户端专业版的总数 示例值： 5
AgentsProExpireWithInSevenDays	Uint64	7天内到期的预付费专业版总数 示例值： 27
FlagshipMachineCnt	Uint64	旗舰版主机数 示例值： 1
MachinesAll	Uint64	云主机总数 示例值： 100
MachinesUninstalled	Uint64	云主机没有安装主机安全客户端的总数 示例值： 3
Offline	Uint64	已离线总数 示例值： 0
ProtectDays	Uint64	保护天数 示例值： 1
RiskMachine	Uint64	风险主机总数 示例值： 6
Shutdown	Uint64	已关机总数 示例值： 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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取cls投递信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

返回cls投递配置

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeLogClsDeliverInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
DeliverTypeDetails	Array of DeliverTypeDetails	详情 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取日志存储配置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取日志存储配置

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeLogStorageConfig
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
Period	Int64	日志存储时长，3640表示不限 示例值： 3640
PeriodModifyCount	Int64	本月Period的修改次数 示例值： 2
Type	Array of String	存储类型，string数组 示例值： ["malware"]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取日志存储量记录

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取日志存储量记录

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeLogStorageRecord
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
Records	Array of LogStorageRecord	存储量记录 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

检查用户是否有指定主机登录权限

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取用户主机登录权限状态

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeLoginPermission
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
InstanceId	否	否	String	instance_id(instance_id和quuid至少要填一个) 示例值： inst-anyinst
MemberId	否	否	Array of String	集团账号的成员id 示例值： [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
Quuid	否	否	String	主机quuid列表(instance_id和quuid至少要填一个) 示例值： 5a540076-d38a-4078-aa98-qwert371d322

3. 输出参数

参数名称	类型	描述
HasLoginPermission	Bool	是否有登录权限 示例值： true

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	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取机器信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取机器信息

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMachineInfoByHashKey
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
MachineKey	否	否	String	主机HashKey 示例值： 539844622

3. 输出参数

参数名称	类型	描述
HostIp	String	内网IP 示例值： 10.0.0.11
InstanceId	String	实例ID 示例值： ins-dsdbhjqf
InstanceName	String	实例名 示例值： redis_node_cvm

参数名称	类型	描述
Quuid	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Region	String	可用区 示例值： ap-region1
Uuid	String	主机uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取主机登录方式

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取主机登录方式

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMachineLoginType
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
InstanceIds	否	否	Array of String	instance_id 示例值： ["inst-anyinst"]
MemberId	否	否	Array of String	集团账号的成员id 示例值： [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
Quuids	否	否	Array of String	主机Quuid列表 示例值： ["5a540076-d38a-4078-aa98-qwert371d322"]

3. 输出参数

参数名称	类型	描述
List	Array of MachineLoginType	登录方式 示例值：查看

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	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取主机登录方式状态

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取主机登录方式状态

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMachineLoginTypeStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
InstanceId	否	否	String	instance_id(instance_id和quuid至少要填一个) 示例值： inst-anyinst
MemberId	否	否	Array of String	集团账号的成员id 示例值： [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
Quuid	否	否	String	主机quuid列表(instance_id和quuid至少要填一个) 示例值： 5a540076-d38a-4078-aa98-qwert371d322

3. 输出参数

参数名称	类型	描述
LoginType	Uint64	登录方式：0-原始方式，1-扫码免密登录 示例值： 1

参数名称	类型	描述
ReturnCode	Uint64	无法启用扫码登录的原因： 0： 成功（可以扫码登录） 1： 未安装agent 2： agent离线 3： agent版本不支持 4：未知错误 示例值： 0
ReturnMessage	String	无法启用扫码登录的原因描述 示例值： Agent Offline
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

查询资源订单列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询订单列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeOrderList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	多个条件筛选时取交集 • ProductCode 产品编码,p_开头 • SubProductCode 子产品编码,sp_开头 • InquireKey 计费项,sv_开头 • Status 资源状态 1正常 2隔离 3销毁 • PayMode 付费模式 0 按量计费，1 包年包月 • ResourceId 资源ID • RenewFlag 自动续费标签 0 默认不需要(大客户存在自动续费的能力) 1 自动续费 2 手动设置不自动续费 • DealNames 子订单号 示例值：查看
Limit	否	否	Uint64	限制条数,默认10 ,最大100 示例值： 10
Offset	否	否	Uint64	偏移量,默认0 示例值： 0

参数名称	必选	允许NULL	类型	描述
ResourceIds	否	否	Array of String	资源ID 示例值： ["32454"]

3. 输出参数

参数名称	类型	描述
List	Array of OrderList	订单资源对象列表 示例值：查看
TotalCount	Uint64	订单总条数 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取概览统计数据

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取概览统计数据。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeOverviewStatistics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
BaseLineNum	Uint64	安全基线数。 示例值： 1
BruteAttackSuccessNum	Uint64	暴力破解成功数。 示例值： 1
MalwareNum	Uint64	木马文件数。 示例值： 1
NonlocalLoginNum	Uint64	异地登录数。 示例值： 1

参数名称	类型	描述
OnlineMachineNum	Uint64	服务器在线数。 示例值： 1
ProVersionMachineNum	Uint64	专业服务器数。 示例值： 1
VulNum	Uint64	漏洞数。 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InternalError.MainDBFail	操作数据失败。

获取专业版概览信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

用于获取专业版概览信息。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeProVersionInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
IsAutoOpenProVersion	Bool	新增主机是否自动开通专业版 示例值： true
PostPayCost	Uint64	昨日【专业版-按量付费】扣费明细,(实际已账单为准) 示例值： 1
ProVersionNum	Uint64	专业版主机数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

获取专业版状态

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

用于获取单台主机或所有主机是否开通专业版状态。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeProVersionStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Uuid	是	否	String	主机安全客户端UUID、填写"all"表示所有主机。 示例值： e8f91530-02c7-3e98-d84d-26df60d981ef

3. 输出参数

参数名称	类型	描述
Status	String	开通状态。 • UNOPENED：未开通专业版 • OPENED：已开通专业版 示例值： OPENED
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询推荐购买防护核数

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询推荐购买防护核数

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeRecommendedProtectCpu
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
Number	Int64	推荐购买数 示例值： 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

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

查询扫描状态

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

DescribeScanState 该接口能查询对应模块正在进行的扫描任务状态

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-29 09:49:27。

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：DescribeScanState
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤参数; • StrategyId 基线策略ID ,仅 ModuleType 为 Baseline 时需要 示例值：查看
ModuleType	是	否	String	模块类型 当前提供 Malware 木马 , Vul 漏洞 , Baseline 基线 示例值： Vul

3. 输出参数

参数名称	类型	描述
RiskEventCount	Uint64	扫描漏洞数 示例值： 1

参数名称	类型	描述
ScanBeginTime	String	开始扫描时间 示例值： 2021-07-09 15:04:01
ScanEndTime	String	扫描结束时间 示例值： 2021-07-09 15:04:01
ScanState	Uint64	0 从未扫描过、 1 扫描中、 2扫描完成、 3停止中、 4停止完成 示例值： 2
Schedule	Uint64	扫描进度 示例值： 10
TaskId	Uint64	任务Id 示例值： 1
Type	Uint64	0一键检测 1定时检测 示例值： 1
VulId	Array of Uint64	任务扫描的漏洞id 示例值： [1,2,4]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
AuthFailure	CAM签名/鉴权错误。

错误码	描述
InvalidParameterValue	参数取值错误。

查询扫描任务详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

DescribeScanTaskDetails 查询扫描任务详情，可以查询扫描进度信息/异常;

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-14 17:12:25。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeScanTaskDetails
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 • MachineName - String - 是否必填：否 - 主机别名 • Ip - String - 是否必填：否 - 主机ip • InstanceID - String - 是否必填：否 - 主机实例ID 示例值：查看
Limit	否	否	Uint64	需要返回的数量，最大值为100 示例值： 10
ModuleType	是	否	String	模块类型 当前提供 Malware 木马，Vul 漏洞，Baseline 基线 示例值： Vul
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
TaskId	是	否	Uint64	任务ID 示例值： 1

3. 输出参数

参数名称	类型	描述
RiskEventCount	Uint64	风险事件个数 示例值： 1
RiskMachineCount	Uint64	发现风险机器数 示例值： 1
ScanBeginTime	String	扫描开始时间 示例值： 2024-10-30 10:13:53
ScanContent	Array of String	扫描内容 示例值： ["0", "1", "2", "4", "5"]
ScanEndTime	String	扫描结束时间 示例值： 2021-02-01 12:00:00
ScanLeftTime	Uint64	扫描剩余时间 示例值： 12
ScanMachineCount	Uint64	扫描机器总数 示例值： 1
ScanProgress	Uint64	扫描进度 示例值： 10
ScanTaskDetailList	Array of ScanTaskDetails	扫描任务信息列表 示例值：查看
ScanTime	Uint64	检测时间 示例值： 19
StoppingAll	Bool	任务是否全部正在被停止 ture是 示例值： true
TotalCount	Uint64	总数 示例值： 1
Type	Uint64	0一键检测 1定时检测 示例值： 1
VulCount	Uint64	扫描出漏洞个数 示例值： 0
VulInfo	Array of VulDetailInfo	漏洞信息 示例值：查看

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	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
AuthFailure	CAM签名/鉴权错误。
InvalidParameterValue	参数取值错误。

获取安全事件动态消息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (DescribeSecurityDynamics) 用于获取安全事件动态消息数据。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeSecurityDynamics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Limit	否	否	Uint64	返回数量，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

3. 输出参数

参数名称	类型	描述
SecurityDynamics	Array of SecurityDynamic	安全事件消息数组。 示例值：查看
TotalCount	Uint64	记录总数。 示例值： 100

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	内部错误。
InvalidParameter.InvalidFormat	参数格式错误。
InvalidParameter.IllegalRequest	非法请求。

获取安全事件统计

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取安全事件统计

默认接口请求频率限制：20次/秒。

接口更新时间：2022-11-08 16:30:42。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecurityEventStat
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	该接口无过滤条件 示例值：查看

3. 输出参数

参数名称	类型	描述
AttackLogsStat	EventStat	网络攻击事件统计 示例值：查看
BaseLineTotalAffectNum	Uint64	有未处理基线安全事件的机器总数 示例值： 1
BaselineHighStat	EventStat	高危基线漏洞事件统计 示例值：查看

参数名称	类型	描述
BaselineLowStat	EventStat	低危基线漏事件统计 示例值：查看
BaselineNormalStat	EventStat	中危基线漏事件统计 示例值：查看
BaselineRiskStat	EventStat	严重基线漏洞事件统计 示例值：查看
BruteAttackStat	EventStat	爆破事件统计 示例值：查看
CyberAttackTotalAffectNum	Uint64	有未处理网络攻击安全事件的机器总数 示例值： 1
HighRiskBashStat	EventStat	高危命令事件统计 示例值：查看
HostLoginStat	EventStat	异地事件统计 示例值：查看
InvasionTotalAffectNum	Uint64	有未处理入侵安全事件的机器总数 示例值： 1
MachineTotalAffectNum	Uint64	有未处理安全事件的机器总数 示例值： 1
MaliciousRequestStat	EventStat	恶意请求事件统计 示例值：查看
MalwareStat	EventStat	木马事件统计 示例值：查看
PrivilegeStat	EventStat	本地提权事件统计 示例值：查看
ReverseShellStat	EventStat	反弹Shell事件统计 示例值：查看
Score	Uint64	安全得分 示例值： 20
VulHighStat	EventStat	高危漏洞事件统计 示例值：查看
VulLowStat	EventStat	低危漏洞事件统计 示例值：查看

参数名称	类型	描述
VulNormalStat	EventStat	中危漏洞事件统计 示例值：查看
VulRiskStat	EventStat	严重漏洞事件统计 示例值：查看
VulStat	EventStat	漏洞数统计 示例值：查看
VulTotalAffectNum	Uint64	有未处理漏洞安全事件的机器总数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
ResourceNotFound	资源不存在。

获取安全事件数统计数据

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取安全概览相关事件统计数据接口

默认接口请求频率限制：20次/秒。

接口更新时间：2022-11-08 16:30:42。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecurityEventsCnt
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AttackLogs	SecurityEventInfo	攻击检测相关风险事件 示例值：查看
BaseLine	SecurityEventInfo	安全基线相关风险事件 示例值：查看
Bash	SecurityEventInfo	高危命令相关风险事件 示例值：查看
BruteAttack	SecurityEventInfo	密码破解相关风险事件 示例值：查看

参数名称	类型	描述
EffectMachineCount	Uint64	受影响机器数 示例值： 1
EmergencyVul	SecurityEventInfo	应急漏洞相关风险事件 示例值：查看
EventsCount	Uint64	所有事件总数 示例值： 1
HostLogin	SecurityEventInfo	登录审计相关风险事件 示例值：查看
LinuxVul	SecurityEventInfo	linux系统漏洞事件总数 示例值：查看
Malware	SecurityEventInfo	木马文件相关风险事件 示例值：查看
PrivilegeRules	SecurityEventInfo	本地提权相关风险事件 示例值：查看
ReverseShell	SecurityEventInfo	反弹Shell相关风险事件 示例值：查看
RiskDns	SecurityEventInfo	恶意请求相关风险事件 示例值：查看
SysVul	SecurityEventInfo	应用漏洞风险事件 示例值：查看
WebVul	SecurityEventInfo	Web应用漏洞相关风险事件 示例值：查看
WindowVul	SecurityEventInfo	window 系统漏洞事件总数 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InternalError	内部错误。
ResourceNotFound	资源不存在。
InternalError.MainDBFail	操作数据失败。
InvalidParameter	参数错误。

获取安全事件统计数据

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (DescribeSecurityTrends) 用于获取安全事件统计数据。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeSecurityTrends
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
BeginDate	是	否	Date	开始时间，如：2021-07-10 示例值： 2021-07-10
EndDate	是	否	Date	结束时间，如：2021-07-10 示例值： 2021-09-10

3. 输出参数

参数名称	类型	描述
BaseLines	Array of SecurityTrend	基线统计数据数组。 示例值：查看
BruteAttacks	Array of SecurityTrend	密码破解事件统计数据数组。 示例值：查看

参数名称	类型	描述
CyberAttacks	Array of SecurityTrend	网络攻击统计数据数组。 示例值：查看
HighRiskBashs	Array of SecurityTrend	高危命令统计数据数组。 示例值：查看
MaliciousRequests	Array of SecurityTrend	恶意请求统计数据数组。 示例值：查看
Malwares	Array of SecurityTrend	木马事件统计数据数组。 示例值：查看
NonLocalLoginPlaces	Array of SecurityTrend	异地登录事件统计数据数组。 示例值：查看
PrivilegeEscalations	Array of SecurityTrend	本地提权统计数据数组。 示例值：查看
ReverseShells	Array of SecurityTrend	反弹shell统计数据数组。 示例值：查看
Vuls	Array of SecurityTrend	漏洞统计数据数组。 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter.DateRange	时间区间格式错误。
InvalidParameter	参数错误。

错误码	描述
InvalidParameterValue	参数取值错误。

获取任务下发时长

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取任务下发时长

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeTaskDuration
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
TimingScan	否	否	Bool	是否定时扫描 示例值： true
UuidCnt	是	否	Uint64	需要执行任务的主机数 示例值： 100

3. 输出参数

参数名称	类型	描述
Duration	Uint64	任务下发需要的时长，单位为分钟 示例值： 5
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

查询主机安全授权试用报告(仅限控制台申领的)

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询试用报告

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeTrialReport
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AddMachineCnt	Int64	新增机器数 示例值： 0
AutoBlockBruteCnt	Int64	自动阻断数(成功) 示例值： 0
AutoDefenceCnt	Int64	自动防御漏洞数(成功) 示例值： 0

参数名称	类型	描述
AutoIsolateMalwareCnt	Int64	自动隔离木马数(成功) 示例值： 0
BaselineRiskCnt	Int64	基线风险数(检测项) 示例值： 0
BruteAlarmCnt	Int64	爆破告警成功数 示例值： 0
IsShow	Bool	是否展示 示例值： true
MalwareAlarmCnt	Int64	木马告警成功数 示例值： 0
VulCnt	Int64	漏洞数 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

用于查询用户自定义配置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询用户配置

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeUsersConfig
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
ConfigName	是	否	String	配置名称 • license_monitor 授权监控配置 0 关闭, 1开启 示例值： license_mon

3. 输出参数

参数名称	类型	描述
Value	String	配置值 示例值： 35768
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取专业版和基础版机器数

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

用于统计专业版和基础版机器数。

默认接口请求频率限制：20次/秒。

接口更新时间：2023-01-09 11:35:47。

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：DescribeVersionStatistics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
BasicVersionNum	Uint64	基础版数量 示例值： 1
GeneralVersionNum	Uint64	普惠版数量 示例值： 1
ProVersionNum	Uint64	专业版数量 示例值： 1
UltimateVersionNum	Uint64	旗舰版数量 示例值： 0

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	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InternalError.MainDBFail	操作数据失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取漏洞态势信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取漏洞态势信息

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeVulTrend
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
HotVulCount	Uint64	近半年热点攻击漏洞 示例值： 134
IncreaseHotVulCount	Uint64	近半年新增热点攻击漏洞 示例值： 13
IncreaseVulEventCount	Uint64	近半年新增漏洞利用攻击事件数量 示例值： 0
VulEventCount	Uint64	近半年漏洞利用攻击事件数量 示例值： 0

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	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

导出扫描任务详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据任务id导出指定扫描任务详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：ExportScanTaskDetails
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 • MachineName - String - 是否必填：否 - 主机别名 • Ip - String - 是否必填：否 - 主机ip • InstanceID - String - 是否必填：否 - 主机实例ID 示例值：查看
ModuleType	是	否	String	模块类型，当前提供：Malware 木马，Vul 漏洞，Baseline 基线 示例值： Malware
TaskId	是	否	Uint64	本次检测的任务id（不同于出参的导出本次检测Excel的任务Id） 示例值： 1596595610

3. 输出参数

参数名称	类型	描述
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址(不同于入参的本次检测任务id) 示例值： 1615549629
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

导出风险趋势

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出风险趋势

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：ExportSecurityTrends
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
BeginDate	是	否	Date	开始时间。 示例值： 2020-06-01
EndDate	是	否	Date	结束时间。 示例值： 2020-06-02

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出文件下载链接地址。 示例值： http://www.ay.com/ay
TaskId	String	任务id 示例值： 56
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

异步导出任务

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

用于异步导出数据量大的日志文件

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：ExportTasks
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
TaskId	是	否	String	任务ID 示例值： 24563

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	下载链接 示例值： http://domain.com/anypath/x
FileName	String	保存文件名 示例值： login-6450ca41-35da-4bee-ade8-c842781ea6dd.csv
Status	String	PENDING：正在生成下载链接，FINISHED：下载链接已生成，ERROR：网络异常等异常情况 示例值： FINISHED

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	内部错误。
ResourceNotFound	资源不存在。

修改网络攻击事件状态

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyEventAttackStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
All	否	否	Bool	是否更新全部，即是否对所有的事件进行操作，当ids 不为空时，此参数无效 示例值： false
ExcludeId	否	否	Array of Uint64	排除的id 示例值： [1,2]

参数名称	必选	允许NULL	类型	描述
Filters	否	否	Array of Filters	过滤条件。 • Type - String 攻击状态 0: 尝试攻击 1: 攻击成功 - 是否必填: 否 • Status - String 事件处理状态 0：待处理 1：已处理 2： 已加白 3： 已忽略 4：已删除 - 是否必填: 否 • SrcIP - String 来源IP - 是否必填: 否 • DstPort - String 攻击目标端口 - 是否必填: 否 • MachineName - String 主机名称 - 是否必填: 否 • InstanceID - String 主机实例ID - 是否必填: 否 • Quuids - String 主机cvm uuid - 是否必填: 否 示例值：查看
Ids	否	否	Array of Uint64	需要修改的事件id 数组，支持批量 示例值： [1,2]
Status	否	否	Uint64	0：待处理 1：已处理 3： 已忽略 4：已删除 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

修改日志cls投递配置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

修改日志cls投递配置

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyLogClsDeliverInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
LogType	是	否	Array of Uint64	安全模块下的日志类型 示例值： [1]
LogsetId	否	否	String	日志集ID 示例值： 234235
LogsetName	否	否	String	日志集主题 示例值： redis_node_log
LogsetRegion	是	否	String	地域 示例值： ap-region1
SecurityType	是	否	Uint64	日志类型 1: 入侵检测、2: 漏洞管理、3: 基线管理、4: 高级防御、5: 客户端相关、6: 资产指纹、7: 主机列表、8: 客户端日志 示例值： 1
TopicId	否	否	String	主题ID 示例值： topic_redis_node_log

参数名称	必选	允许NULL	类型	描述
TopicName	否	否	String	主题名称 示例值： topic_redis_node_log

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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

修改某个日志类型的cls投递开关

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

修改cls的投递开关

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyLogClsDeliverSwitch
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
SecurityType	是	否	Uint64	安全模块类型 1: 入侵检测 2: 漏洞管理 3: 基线管理 4: 高级防御 5:客户端相关 6: 资产指纹 7 主机列表 8 客户端上报 示例值： 1
Switch	是	否	Uint64	投递开关 0关闭 1开启 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

修改日志存储配置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

修改日志存储配置

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyLogStorageConfig
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
IsModifyPeriod	是	否	Bool	是否修改有效期（已废弃） 示例值： true
Period	是	否	Int64	日志存储时长，3640表示不限 示例值： 3640
Type	否	否	Array of String	存储类型，string数组 示例值： ["malware","risk_process"]

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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

修改主机登录方式

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

修改主机登录方式

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyMachineLoginType
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
InstanceId	否	否	String	instance_id(instance_id和quuid至少要填一个) 示例值： inst-anyinst
LoginType	是	否	Uint64	登录方式：0-原始方式，1-扫码免密登录 示例值： 1
MemberId	否	否	Array of String	集团账号的成员id 示例值： [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
Quuid	否	否	String	主机quuid列表(instance_id和quuid至少要填一个) 示例值： 5a540076-d38a-4078-aa98-qwert371d322

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
ResultCode	Uint64	修改结果： 0： 成功 1： 未安装agent 2： agent离线 3： agent版本不支持 4：未知错误 示例值： 0
ResultMessage	String	修改结果描述 示例值： Agent Offline
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

新购/变配 订单

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

编辑订单

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyOrder
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Data	否	否	Array of OrderData	下单配置数组,最大长度10个, 不允许新购,变配同时进行 示例值：查看

3. 输出参数

参数名称	类型	描述
BigDealId	String	大订单号,大订单号后付费订单无返回 示例值： any data
DealNames	Array of String	子订单号 示例值： ["32454"]

参数名称	类型	描述
ResourceIds	Array of String	资源ID,后付费订单会返回,预付费(包年包月)则需要通过大订单号/子订单号去调计费支付接口支付 示例值： ["32454"]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

用于创建/修改用户自定义配置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

修改用户配置

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyUsersConfig
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
ConfigName	是	否	String	配置名称 • license_monitor 新增授权监控配置 0 关闭, 1开启 示例值： license_monitor_100
ConfigValue	是	否	String	配置值 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

安全中心漏洞防御、网络攻击开关修改

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

安全中心漏洞防御、网络攻击开关修改

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyVulDefenceSwitch
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
DefenceType	是	否	Uint64	设置类型 0 漏洞防御 1 网络攻击 示例值： 1
Enable	是	否	Uint64	开关是否开启 1开启，0关闭 示例值： 1
MemberId	否	否	Array of String	集团账号的成员id 示例值： [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]

3. 输出参数

参数名称	类型	描述

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	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

基线管理相关接口
修改事件忽略状态

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据检测项id或事件id批量忽略事件或取消忽略

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：ChangeRuleEventsIgnoreStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
EventIdList	否	否	Array of Uint64	事件id数组 示例值： [1,2]
IgnoreStatus	是	否	Uint64	忽略状态 0:取消忽略 ； 1:忽略 示例值： 1
RuleIdList	否	否	Array of Uint64	检测项id数组 示例值： [1,2]

3. 输出参数

参数名称	类型	描述

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	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

创建基线策略

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据策略信息创建基线策略

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：CreateBaselineStrategy
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
CategoryIds	是	否	Array of Uint64	该策略下选择的基线id数组. 示例: [1,3,5,7] 示例值： [1,3,5,7]
IsGlobal	是	否	Uint64	扫描范围是否全部服务器, 1:是 0:否, 为1则为全部专业版主机 示例值： 1
MachineType	是	否	String	云主机类型： CVM：虚拟主机 BM：裸金属 ECM：边缘计算主机 LH：轻量应用服务器 Other：混合云机器 示例值： CVM
Quuids	否	否	Array of String	主机id数组. 示例: ["quuid1","quuid2"] 示例值： ["657f3c29-4bc9-4c48-a8d6-de5bd14ffc67"]

参数名称	必选	允许NULL	类型	描述
RegionCode	是	否	String	主机地域 示例值： ap-region1
ScanAt	是	否	String	定期检测时间，该时间下发扫描. 示例:“22:00”, 表示在22:00下发检测 示例值： 02:00
ScanCycle	是	否	Uint64	检测周期, 表示每隔多少天进行检测.示例: 2, 表示每2天进行检测一次. 示例值： 2
StrategyName	是	否	String	策略名称 示例值： 定时扫描基线

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
FailedOperation.NoProfessionHost	无专业版主机。
FailedOperation.TooManyStrategy	创建基线策略超过上限。
InvalidParameter	参数错误。

错误码	描述
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

删除基线策略

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据基线策略id删除策略

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DeleteBaselineStrategy
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
StrategyId	是	否	Uint64	基线策略id 示例值： 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

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

基线策略概览统计数据查询

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据基线策略id查询基线策略数据概览统计

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineAnalysisData
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
StrategyId	是	否	Uint64	基线策略id 示例值： 1

3. 输出参数

参数名称	类型	描述
IfFirstScan	Uint64	是否是第一次检测 1是 0不是 示例值： 1
IsGlobal	Uint64	是否全部服务器：1-是 0-否 示例值： 1
LatestScanTime	String	最后检测时间 示例值： 2019-12-25 11:57:15

参数名称	类型	描述
ScanHostCount	Uint64	服务器总数 示例值： 1
ScanRuleCount	Uint64	检测项总数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询基线基础信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询基线基础信息列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeBaselineBasicInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
BaselineName	否	否	String	基线名称 示例值： MySQL 弱口令检测

3. 输出参数

参数名称	类型	描述
BaselineBasicInfoList	Array of BaselineBasicInfo	基线基础信息列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询基线详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据基线id查询基线详情接口

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeBaselineDetail
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
BaselineId	是	否	Uint64	基线id 示例值： 1

3. 输出参数

参数名称	类型	描述
BaselineDetail	BaselineDetail	基线详情 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

基线影响主机列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据基线id查询基线影响主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-03-28 01:21:07。

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：DescribeBaselineEffectHostList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
BaselineId	是	否	Uint64	基线id 示例值： 12
Filters	否	否	Array of Filters	过滤条件。 • AliasName- String- 主机别名 • Status- Uint- 1已通过 0未通过 5检测中 示例值：查看
Limit	是	否	Uint64	分页参数 最大100条 示例值： 10
Offset	是	否	Uint64	分页参数 示例值： 0
StrategyId	否	否	Uint64	策略id 示例值： 1124

参数名称	必选	允许NULL	类型	描述
UuidList	否	否	Array of String	主机uuid数组 示例值： ["5a540076-d38a-4078-aa98-qwert371d322"]

3. 输出参数

参数名称	类型	描述
EffectHostList	Array of BaselineEffectHost	影响服务器列表 示例值：查看
TotalCount	Uint64	记录总数 示例值： 12
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

服务器风险top接口

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

接口返回TopN的风险服务器

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeBaselineHostTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
StrategyId	是	否	Uint64	策略id 示例值： 1
Top	是	否	Uint64	动态top值 示例值： 1

3. 输出参数

参数名称	类型	描述
BaselineHostTopList	Array of BaselineHostTopList	主机基线策略事件Top 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
FailedOperation.NoProfessionHost	无专业版主机。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询基线列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询基线列表信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 • StrategyId- Uint64 - 基线策略id • Status - Uint64 - 处理状态1已通过 0未通过 • Level - Uint64[] - 威胁等级 • BaselineName - String - 基线名称 • Quuid- String - 主机quuid • Uuid- String - 主机uuid 示例值：查看
Limit	是	否	Uint64	分页参数 最大100条 示例值： 10
Offset	是	否	Uint64	分页参数 示例值： 0

3. 输出参数

参数名称	类型	描述
BaselineList	Array of BaselineInfo	基线信息列表 示例值：查看
TotalCount	Uint64	分页查询记录总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询基线检测项信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据基线id查询下属检测项信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeBaselineRule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
BaselineId	是	否	Uint64	基线id 示例值： 1
Level	否	否	Array of Uint64	基线风险等级：0低危 1中危 2高危 3严重 示例值： [1,2,3]
Limit	是	否	Uint64	分页参数 最大100条 示例值： 10
Offset	是	否	Uint64	分页参数 示例值： 0
Quuid	否	否	String	主机quuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
Status	否	否	Uint64	状态 示例值： 0

参数名称	必选	允许NULL	类型	描述
Uuid	否	否	String	主机uuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0

3. 输出参数

参数名称	类型	描述
BaselineRuleList	Array of BaselineRuleInfo	基线检测项列表 示例值：查看
ShowRuleRemark	Bool	是否显示说明列：true-是，false-否 示例值： true
TotalCount	Uint64	分页查询记录总数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

基线检测进度查询

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据任务id查询基线检测进度

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeBaselineScanSchedule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
TaskId	是	否	Uint64	任务id 示例值： 1

3. 输出参数

参数名称	类型	描述
Schedule	Uint64	检测进度(百分比) 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询基线策略详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据基线策略id查询策略详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeBaselineStrategyDetail
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
StrategyId	是	否	Uint64	用户基线策略id 示例值： 1

3. 输出参数

参数名称	类型	描述
CategoryIds	Array of String	用户该策略下所有的基线id 示例值： ["10021"]
IfScanned	Uint64	1 表示扫描过, 0没扫描过 示例值： 1
IsGlobal	Uint64	扫描范围是否全部服务器, 1:是 0:否, 为1则为全部专业版主机 示例值： 1

参数名称	类型	描述
MachineType	String	云服务器类型。 • CVM: 云服务器 • BM: 黑石物理机 • ECM: 边缘计算服务器 • LH: 轻量应用服务器 • Other: 混合云机器 示例值： CVM
PassRate	Uint64	策略扫描通过率 示例值： 1
Quuids	Array of String	用户该策略下的所有主机id 示例值： ["0096440e-9a9f-4e80-a82d-0b018637ayay"]
Region	String	主机地域 示例值： ap-bj
ScanAt	String	定期检测时间, 该时间下发扫描 示例值： 00:00:00
ScanCycle	String	策略扫描周期(天) 示例值： 1
StrategyName	String	策略名 示例值： 弱密码
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。

错误码	描述
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

用户基线策略列表查询

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询一个用户下的基线策略信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineStrategyList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Enabled	是	否	Uint64	规则开关，1：打开 0：关闭 2:全部 示例值： 1
Limit	是	否	Uint64	分页参数 最大100 示例值： 10
Offset	是	否	Uint64	分页参数 示例值： 0

3. 输出参数

参数名称	类型	描述
StrategyList	Array of Strategy	用户策略信息列表 示例值：查看

参数名称	类型	描述
TotalCount	Uint64	分页查询记录的总数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

基线检测项TOP

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据策略id查询基线检测项TOP

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
StrategyId	是	否	Uint64	策略id 示例值： 1
Top	是	否	Uint64	动态top值 示例值： 5

3. 输出参数

参数名称	类型	描述
RuleTopList	Array of BaselineRuleTopInfo	检测项Top列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
FailedOperation.NoProfessionHost	无专业版主机。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询忽略检测项信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询已经忽略的检测项信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeIgnoreBaselineRule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Limit	是	否	Uint64	分页参数 最大100条 示例值： 10
Offset	是	否	Uint64	分页参数 示例值： 0
RuleName	否	否	String	检测项名称 示例值： rulename

3. 输出参数

参数名称	类型	描述
IgnoreBaselineRuleList	Array of IgnoreBaselineRule	忽略基线检测项列表信息 示例值：查看

参数名称	类型	描述
TotalCount	Uint64	分页查询记录总数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询忽略检测项影响主机列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据检测项id与筛选条件查询忽略检测项影响主机列表信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeIgnoreRuleEffectHostList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 • AliasName- String- 主机别名 示例值：查看
Limit	是	否	Uint64	分页参数 最大100条 示例值： 10
Offset	是	否	Uint64	分页参数 示例值： 0
RuleId	是	否	Uint64	检测项id 示例值： 1
TagNames	否	否	Array of String	主机标签名 示例值： ["tag1"]

3. 输出参数

参数名称	类型	描述
IgnoreRuleEffectHostList	Array of IgnoreRuleEffectHostInfo	忽略检测项影响主机列表 示例值：查看
TotalCount	Uint64	分页查询记录总数 示例值： 12
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

根据策略名查询策略是否存在

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据策略名查询策略是否存在

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:34。

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：DescribeStrategyExist
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
StrategyName	是	否	String	策略名 示例值： sname

3. 输出参数

参数名称	类型	描述
IfExist	Uint64	策略是否存在, 1是 0否 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

基线影响主机列表导出

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出基线影响主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：ExportBaselineEffectHostList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
BaselineId	是	否	Uint64	基线id 示例值： 1
BaselineName	否	否	String	废弃字段 示例值： check_redis_cvm
Filters	否	否	Array of Filters	过滤条件。 • AliasName- String- 主机别名 • Status- Uint- 1已通过 0未通过 5检测中 示例值：查看
StrategyId	否	否	Uint64	策略id 示例值： 2
UuidList	否	否	Array of String	主机uuid数组 示例值： ["1ce68339-8828-457f-b358-d5b1b34e4fe9"]

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	该参数已废弃 示例值： http://domain.com/anypath/x
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

导出基线列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出基线列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：ExportBaselineList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 • StrategyId- Uint64 - 基线策略id • Status - Uint64 - 处理状态1已通过 0未通过 • Level - Uint64[] - 威胁等级 • BaselineName - String - 基线名称 • Quuid- String - 主机quuid • Uuid- String - 主机uuid 示例值：查看
IfDetail	否	否	Uint64	已废弃 示例值： 1

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
DownloadUrl	String	导出文件下载地址（已弃用） 示例值： http://www.ay.com/ay
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

已忽略基线检测项导出

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出已忽略基线检测项信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：ExportIgnoreBaselineRule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
RuleName	否	否	String	检测项名称 示例值： Redis 基线合规检测

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	该参数已废弃 示例值： http://www.ay.com/ay
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

忽略检测项影响主机列表导出

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据检测项id导出忽略检测项影响主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：ExportIgnoreRuleEffectHostList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 • AliasName- String- 主机别名 示例值：查看
RuleId	是	否	Uint64	检测项id 示例值： 1

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	该参数已废弃 示例值： http://domain.com/anypath/x

参数名称	类型	描述
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

更新基线策略信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据基线策略id更新策略信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：UpdateBaselineStrategy
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
CategoryIds	是	否	Array of String	该策略下选择的基线id数组 示例值： ["1002"]
IsGlobal	是	否	Uint64	扫描范围是否全部服务器, 1:是 0:否, 为1则为全部专业版主机 示例值： 1
MachineType	是	否	String	云主机类型： CVM：云服务器 BM：裸金属 ECM：边缘计算主机 LH:轻量应用服务器 OTHER:混合云机器 示例值： CVM
Quuids	是	否	Array of String	主机id数组 示例值： ["5a540076-d38a-4078-aa98-e7c86371d322"]

参数名称	必选	允许NULL	类型	描述
RegionCode	是	否	String	主机地域 示例值： ap-region1
ScanAt	是	否	String	定期检测时间，该时间下发扫描 示例值： 00:00:00
ScanCycle	是	否	Uint64	检测周期 示例值： 1
StrategyId	是	否	Uint64	策略id 示例值： 1
StrategyName	是	否	String	策略名称 示例值： redis_node_check

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
FailedOperation.NoProfessionHost	无专业版主机。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

安全运营相关接口
添加历史搜索记录

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

添加历史搜索记录

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：CreateSearchLog
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
SearchContent	是	否	String	搜索内容 示例值： success

3. 输出参数

参数名称	类型	描述
Status	Uint64	0：成功，非0：失败 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

添加检索模板

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.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：2023-02-09 16:57:33。

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：CreateSearchTemplate
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
SearchTemplate	是	否	SearchTemplate	搜索模板 示例值：查看

3. 输出参数

参数名称	类型	描述
Message	String	失败原因 示例值： A record with the same name already exists
Status	Uint64	0：成功，非0：失败 示例值： 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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
InvalidParameter.NameHasRepetition	名字已重复。

删除检索模板

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.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：2023-02-09 16:57:46。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	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：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	Uint64	模板ID 示例值： 1

3. 输出参数

参数名称	类型	描述
Status	Uint64	0：成功，非0：失败 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取ES字段聚合结果

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.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：2022-05-20 15:12:33。

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：DescribeESAggregations
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Query	是	否	String	ES聚合条件JSON 示例值： {"cwp":"dev"}

3. 输出参数

参数名称	类型	描述
Data	String	ES聚合结果JSON 示例值： {"took":12,"total":3,"aggs":{"dst_port":{},"src_port":{}},"code":0,"message":"success"}
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
FailedOperation.APIServerFail	调用API服务失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询日志检索服务信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询日志检索服务信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-02-09 16:53:15。

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：DescribeHistoryService
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息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	Uint64	1 可购买 2 只能升降配 3 只能跳到续费管理页 示例值： 1
EndTime	String	到期时间 示例值： 2020-10-29 00:00:00
InquireNum	Uint64	用户已购容量 单位 G 示例值： 1
IsAutoOpenRenew	Uint64	是否自动续费,0 初始值, 1 开通 2 没开通 示例值： 1

参数名称	类型	描述
ResourceId	String	资源ID 示例值： 1
StartTime	String	开始时间 示例值： 2020-09-29 00:00:00
Status	Uint64	0 没开通 1 正常 2隔离 3销毁 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

获取索引列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.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：2022-05-20 15:12:33。

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：DescribeIndexList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息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 示例值： {"indexSort":{"i1":["userlog-asset_component"]}
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InternalError	内部错误。
FailedOperation.APIServerFail	调用API服务失败。

获取日志检索容量使用统计

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.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：2023-02-09 16:52:41。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	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：2018-02-28
Region	是	否	String	公共参数，地域信息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：GB） 示例值： 1
UsedSize	Uint64	已使用容量（单位：GB） 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

导出ES查询文档列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.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：2022-05-20 15:12:33。

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：DescribeSearchExportList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Query	是	否	String	ES查询条件JSON 示例值： {"event_type":"vul"}

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	该参数作废 示例值： http://domain.com/anypath/x
TaskId	Uint64	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取历史搜索记录

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.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：2023-02-09 16:57:07。

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：DescribeSearchLogs
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息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	Array of String	历史搜索记录 保留最新的10条 示例值： ["yunjing","106.55.40.250","106.55.35.160"]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

获取快速检索列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.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：2023-02-09 16:57:20。

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：DescribeSearchTemplates
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

3. 输出参数

参数名称	类型	描述
List	Array of SearchTemplate	模板列表 示例值：查看
TotalCount	Uint64	总数 示例值： 1

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	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

新版基线管理相关接口
删除基线策略配置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除基线策略配置

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:02:51。

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：DeleteBaselinePolicy
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
PolicyIds	是	否	Array of Int64	策略Id 示例值： [309052]

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。

删除基线规则

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除基线规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:02:34。

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：DeleteBaselineRule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
RuleId	是	否	Int64	规则Id 示例值： 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

错误码	描述
InternalError	内部错误。
FailedOperation	操作失败。

删除基线忽略规则

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除基线忽略规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 11:59:19。

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：DeleteBaselineRuleIgnore
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
RuleIds	是	否	Array of Int64	规则Id 示例值： [44106]

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
InternalError	内部错误。
InvalidParameter	参数错误。

删除基线弱口令

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除基线弱口令

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:32:04。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteBaselineWeakPassword
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
PasswordIds	是	否	Array of Int64	弱口令Id 示例值： [1002]

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
InternalError	内部错误。
InvalidParameter	参数错误。

获取基线检测详情记录

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线检测详情记录

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:34:39。

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：DescribeBaselineDetectList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [HostCount
Filters	否	否	Array of Filter	• PolicyName - string - 是否必填：否 - 策略名称 • PolicyDetectStatus - int - 是否必填：否 - 1:检测中 2:检测完成 • FirstTime - string - 是否必填：否 - 开始时间 • LastTime - string - 是否必填：否 - 结束时间 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
List	Array of BaselinePolicyDetect	数据列表 示例值：查看
Total	Int64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。
FailedOperation	操作失败。

获取基线检测概览

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线检测概览

默认接口请求频率限制：20次/秒。

接口更新时间：2022-10-25 10:23:03。

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：DescribeBaselineDetectOverview
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
PolicyId	否	否	Int64	策略Id 示例值： 1

3. 输出参数

参数名称	类型	描述
HostCount	Int64	检测服务器数 示例值： 0
ItemCount	Int64	检测项 示例值： 0
LatestNotPassCount	Int64	最近一次检测未通过个数 示例值： 1

参数名称	类型	描述
LatestPassCount	Int64	最近一次检测通过个数 示例值： 1
PassRate	Int64	通过率*100% 示例值： 100
PolicyCount	Int64	检测策略项 示例值： 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
InternalError	内部错误。
InvalidParameter	参数错误。
FailedOperation	操作失败。

获取基线下载列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线下载列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:08:32。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineDownloadList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [StartTime
Filters	否	否	Array of Filter	• Status - int - 是否必填：否 - 0:导出中 1:已完成 • StartTime - string - 是否必填：否 - 开始时间 • EndTime - string - 是否必填：否 - 结束时间 • TaskName - string - 是否必填：否 - 任务名称 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
List	Array of BaselineDownload	数据列表 示例值：查看
Total	Int64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
FailedOperation	操作失败。
InternalError	内部错误。
InvalidParameter	参数错误。

获取基线修复列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线修复列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:08:20。

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：DescribeBaselineFixList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [CreateTime
Filters	否	否	Array of Filter	• ItemName- string - 是否必填：否 - 项名称 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
List	Array of BaselineFix	数据列表 示例值：查看
Total	Int64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。

获取基线检测主机列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线检测主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:36:16。

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：DescribeBaselineHostDetectList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [LastTime
Filters	否	否	Array of Filter	• PolicyId - int64 - 是否必填：否 - 策略Id • HostName - string - 是否必填：否 - 主机名称 • HostIp - string - 是否必填：否 - 主机Ip • ItemId - int64 - 是否必填：否 - 项Id • RuleId - int64 - 是否必填：否 - 规则Id • DetectStatus - int - 是否必填：否 - 检测状态 • Level - int - 是否必填：否 - 风险等级 • StartTime - string - 是否必填：否 - 开时时间 • EndTime - string - 是否必填：否 - 结束时间 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10

参数名称	必选	允许NULL	类型	描述
Offset	否	否	Int64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
List	Array of BaselineHostDetect	数据列表 示例值：查看
Total	Int64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。
FailedOperation	操作失败。

获取忽略规则主机列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取忽略规则主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:28:44。

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：DescribeBaselineHostIgnoreList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0
RuleID	是	否	Int64	请求的规则 示例值： 1

3. 输出参数

参数名称	类型	描述
List	Array of BaselineHost	数据列表 示例值：查看

参数名称	类型	描述
Total	Int64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
FailedOperation	操作失败。
InternalError	内部错误。
InvalidParameter	参数错误。

获取基线服务器风险TOP5

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线服务器风险TOP5

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 11:55:23。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineHostRiskTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
PolicyId	否	否	Int64	策略ID 示例值： 861027

3. 输出参数

参数名称	类型	描述
HostRiskTop5	Array of HostRiskLevelCount	风险主机top5 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。
FailedOperation	操作失败。

获取基线检测项的列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线检测项的列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-10-13 10:14:09。

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：DescribeBaselineItemDetectList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [HostCount
Filters	否	否	Array of Filter	• HostId - string - 是否必填：否 - 主机Id • RuleId - int64 - 是否必填：否 - 规则Id • PolicyId - int64 - 是否必填：否 - 规则Id • ItemName - string - 是否必填：否 - 项名称 • DetectStatus - int - 是否必填：否 - 检测状态 • Level - int - 是否必填：否 - 风险等级 • StartTime - string - 是否必填：否 - 开始时间 • EndTime - string - 是否必填：否 - 结束时间 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0

参数名称	必选	允许NULL	类型	描述
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
List	Array of BaselineItemDetect	数据列表 示例值：查看
Total	Int64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。
FailedOperation	操作失败。

获取忽略规则项列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取忽略规则项列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:03:58。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineItemIgnoreList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列 [ID] 示例值： ID
Filters	否	否	Array of Filter	• CatgoryId - int64 - 是否必填：否 - 规则Id 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	请求偏移默认0 示例值： 0
Order	否	否	String	排序方式 [ASC:升序
RuleID	是	否	Int64	忽略规则ID 示例值： 1

3. 输出参数

参数名称	类型	描述
List	Array of BaselineItemInfo	数据列表 示例值：查看
Total	Int64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。

获取基线检测项信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线检测项信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:38:03。

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：DescribeBaselineItemInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列[FirstTime
Filters	否	否	Array of Filter	• ItemId - int64 - 是否必填：否 - 项Id • Level - int - 是否必填：否 - 风险等级 • ItemName - string - 是否必填：否 - 检测项名字 • RuleId - int - 是否必填：否 - 规则Id 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 1
Offset	否	否	Int64	偏移量,默认0 示例值： 1
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
CategoryList	Array of BaselineItemsCategory	基线分类列表 示例值：查看
List	Array of BaselineItemInfo	结果列表 示例值：查看
Total	Int64	总条目数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。

获取基线项检测结果列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线项检测结果列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-10-13 10:13:14。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineItemList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列 示例值： LastTime
Filters	否	否	Array of Filter	• PolicyId - int64 - 是否必填：否 - 策略Id • RuleId - int64 - 是否必填：否 - 规则Id • HostId - string - 是否必填：否 - 主机Id • HostName - string - 是否必填：否 - 主机名 • HostIp - string - 是否必填：否 - 主机IP • ItemId - String - 是否必填：否 - 检测项Id • ItemName - String - 是否必填：否 - 项名称 • DetectStatus - int - 是否必填：否 - 检测状态[0:未通过
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
List	Array of BaselineItem	数据列表 示例值：查看
Total	Int64	总数 示例值： 100
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。

获取基线检测项TOP5

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线检测项TOP5

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:35:07。

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：DescribeBaselineItemRiskTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
PolicyId	否	否	Int64	策略ID 示例值： 1

3. 输出参数

参数名称	类型	描述
RiskItemTop5	Array of BaselineRiskItem	结果数组 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。
FailedOperation	操作失败。

获取基线策略列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线策略列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:03:23。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselinePolicyList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [RuleCount
Filters	否	否	Array of Filter	• PolicyName - String - 是否必填：否 - 策略名称 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 20
Offset	否	否	Int64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
List	Array of BaselinePolicy	数据列表 示例值：查看
Total	Int64	总数 示例值： 19
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。

获取基线分类列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线分类列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:22:40。

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：DescribeBaselineRuleCategoryList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息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	Array of BaselineCategory	数据列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

获取基线规则检测列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线规则检测列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:35:47。

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：DescribeBaselineRuleDetectList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [HostCount
Filters	否	否	Array of Filter	• PolicyId - int64 - 是否必填：否 - 策略Id • ItemId - int64 - 是否必填：否 - 策略Id • RuleName - string - 是否必填：否 - 规则名称 • DetectStatus - int - 是否必填：否 - 检测状态 • StartTime - string - 是否必填：否 - 开时时间 • EndTime - string - 是否必填：否 - 结束时间 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
List	Array of BaselineRuleDetect	数据列表 示例值：查看
Total	Int64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。

获取基线忽略规则列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线忽略规则列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-24 13:37:14。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineRuleIgnoreList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [HostCount] 示例值： HostCount
Filters	否	否	Array of Filter	• RuleName - String - 是否必填：否 - 规则名称 • ItemId- int - 是否必填：否 - 检测项Id 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
List	Array of BaselineRule	列表 示例值：查看
Total	Int64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。

获取基线规则列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线规则列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:03:09。

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：DescribeBaselineRuleList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列 示例值： ID
Filters	否	否	Array of Filter	• RuleName - String - 是否必填：否 - 规则名称 • CategoryId - int64 - 是否必填：否 自定义筛选为-1 - 规则分类 • RuleType - int - 是否必填：否 0:系统 1:自定义 - 规则类型 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
List	Array of BaselineRule	数据列表 示例值：查看
Total	Int64	总数 示例值： 98
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。

获取基线弱口令列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取基线弱口令列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:29:50。

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：DescribeBaselineWeakPasswordList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列 [CreateTime
Filters	否	否	Array of Filter	• WeakPassword - string - 是否必填：否 - 弱口令 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式 [ASC:升序

3. 输出参数

参数名称	类型	描述
List	Array of BaselineWeakPassword	列表 示例值：查看
Total	Int64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。

获取全网热点漏洞

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取全网热点漏洞

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeHotVulTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息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	Array of VulStoreListInfo	漏洞信息 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取一键忽略受影响的检测项和主机信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取一键忽略受影响的检测项和主机信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:05:46。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeIgnoreHostAndItemConfig
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	• ItemId - int64 - 是否必填：否 - 项Id • RuleId - int64 - 是否必填：否 - 规则Id • HostId - string - 是否必填：否 - 主机Id 示例值：查看

3. 输出参数

参数名称	类型	描述
HostSet	Array of BaselineHost	受影响主机 示例值：查看
ItemSet	Array of BaselineItemInfo	受影响检测项 示例值：查看

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	内部错误。
InvalidParameter	参数错误。

获取漏洞库列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取漏洞库列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeVulStoreList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [PublishDate] 示例值： PublishDate
Filters	否	否	Array of Filter	• VulName- string - 是否必填：否 - 漏洞名称 • CveId- string - 是否必填：否 - cveid • VulCategory- string - 是否必填：否 - 漏洞分类 1 Web-CMS漏洞 ,2 应用漏洞 ,4 Linux软件漏洞,5 Windows系统漏洞 • Method- string - 是否必填：否 - 检测方法 0版本对比,1 poc检测 • SupportDefense- string - 是否必填：否 - 是否支持防御 0不支持,1支持 • FixSwitch- string - 是否必填：否 - 是否支持自动修复 0不支持,1支持 示例值：查看

参数名称	必选	允许NULL	类型	描述
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 10
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
FreeSearchTimes	Uint64	免费搜索次数 示例值： 102
List	Array of VulStoreListInfo	漏洞信息 示例值：查看
Remaining	Uint64	今日剩余搜索此时 示例值： 10
TotalCount	Uint64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。

错误码	描述
InvalidParameterValue	参数取值错误。

导出修复列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出修复列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:29:02。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportBaselineFixList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
ExportAll	否	否	Int64	0:过滤的结果导出；1:全部导出 示例值： 1
Filters	否	否	Array of Filter	• ItemName- string - 是否必填：否 - 项名称 示例值：查看

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
InternalError	内部错误。
InvalidParameter	参数错误。

导出基线主机检测

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出基线主机检测

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:36:37。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportBaselineHostDetectList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
ExportAll	否	否	Int64	0:过滤的结果导出；1:全部导出 示例值： 1
Filters	否	否	Array of Filter	• PolicyId - int64 - 是否必填：否 - 策略Id • HostName - string - 是否必填：否 - 主机名称 • HostIp - string - 是否必填：否 - 主机Ip • ItemId - int64 - 是否必填：否 - 项Id • RuleId - int64 - 是否必填：否 - 规则Id • DetectStatus - int - 是否必填：否 - 检测状态 • Level - int - 是否必填：否 - 风险等级 • StartTime - string - 是否必填：否 - 开时时间 • EndTime - string - 是否必填：否 - 结束时间 示例值：查看
IsExportDetail	否	否	Int64	0:导出界面展示；1:导出全部结果事件 示例值： 0

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
InternalError	内部错误。
InvalidParameter	参数错误。

导出基线检测项

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出基线检测项

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:37:19。

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：ExportBaselineItemDetectList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
ExportAll	否	否	Int64	0:过滤的结果导出；1:全部导出 示例值： 1
Filters	否	否	Array of Filter	• HostId - string - 是否必填：否 - 主机Id • RuleId - int64 - 是否必填：否 - 规则Id • PolicyId - int64 - 是否必填：否 - 规则Id • ItemName - string - 是否必填：否 - 项名称 • DetectStatus - int - 是否必填：否 - 检测状态 • Level - int - 是否必填：否 - 风险等级 • StartTime - string - 是否必填：否 - 开始时间 • EndTime - string - 是否必填：否 - 结束时间 示例值：查看
IsExportDetail	否	否	Int64	0:导出界面展示；1:导出全部结果事件 示例值： 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
InternalError	内部错误。
InvalidParameter	参数错误。

导出检测项结果列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出检测项结果列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:38:58。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportBaselineItemList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
ExportAll	否	否	Int64	0:过滤的结果导出；1:全部导出 示例值： 1
Filters	否	否	Array of Filter	• PolicyId - int64 - 是否必填：否 - 策略Id • RuleId - int64 - 是否必填：否 - 规则Id • HostId - string - 是否必填：否 - 主机Id • HostName - string - 是否必填：否 - 主机名 • HostIp - string - 是否必填：否 - 主机IP • ItemId - String - 是否必填：否 - 检测项Id • ItemName - String - 是否必填：否 - 项名称 • DetectStatus - int - 是否必填：否 - 检测状态[0:未通过

3. 输出参数

参数名称	类型	描述

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	内部错误。
InvalidParameter	参数错误。

导出基线检测规则

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出基线检测规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:36:56。

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：ExportBaselineRuleDetectList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
ExportAll	否	否	Int64	0:过滤的结果导出；1:全部导出 示例值： 1
Filters	否	否	Array of Filter	• PolicyId - int64 - 是否必填：否 - 策略Id • ItemId - int64 - 是否必填：否 - 策略Id • RuleName - string - 是否必填：否 - 规则名称 • DetectStatus - int - 是否必填：否 - 检测状态 • StartTime - string - 是否必填：否 - 开时时间 • EndTime - string - 是否必填：否 - 结束时间 示例值：查看
IsExportDetail	否	否	Int64	0:导出界面展示；1:导出全部结果事件 示例值： 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
InternalError	内部错误。
InvalidParameter	参数错误。

导出弱口令配置列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出弱口令配置列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:05:13。

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：ExportBaselineWeakPasswordList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
ExportAll	否	否	Int64	0:过滤的结果导出；1:全部导出 示例值： 0
Filters	否	否	Array of Filter	• WeakPassword - string - 是否必填：否 - 弱口令 示例值：查看

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
InternalError	内部错误。
InvalidParameter	参数错误。

修复基线检测

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

修复基线检测

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:05:58。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：FixBaselineDetect
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Data	否	否	Array of String	修复内容 示例值： ["1ce68339-8828-457f-b358-d5b1b34e4fe9"]
HostId	是	否	String	主机Id 示例值： 1ce68339-8828-457f-b358-d5b1b34e4fe9
ItemId	是	否	Int64	项Id 示例值： 10001

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
InternalError	内部错误。
InvalidParameter	参数错误。
FailedOperation	操作失败。

修改或新增基线策略设置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

更改基线策略设置

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:07:43。

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：ModifyBaselinePolicy
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Data	是	否	BaselinePolicy	数据内容 示例值：查看
Filters	否	否	Array of Filter	• RuleName - String - 是否必填：否 - 规则名称 • CategoryId - int64 - 是否必填：否 自定义筛选为-1 - 规则分类 • RuleType - int - 是否必填：否 0:系统 1:自定义 - 规则类型 示例值：查看
SelectAll	否	否	Int64	是否按照过滤的全选 示例值： 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
InternalError	内部错误。
InvalidParameter	参数错误。
FailedOperation	操作失败。

修改或新增基线策略状态

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

更改基线策略状态

默认接口请求频率限制：20次/秒。

接口更新时间：2022-11-17 16:05:09。

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：ModifyBaselinePolicyState
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
IsEnabled	是	否	Int64	开启状态[1:开启
PolicyId	是	否	Int64	策略Id 示例值： 638392

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
InternalError	内部错误。
InvalidParameter	参数错误。

修改或新增基线检测规则

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

更改基线检测规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:06:12。

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：ModifyBaselineRule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
CategoryIds	否	否	Array of Uint64	勾选的检测项分类 示例值： [100,101]
Data	是	否	BaselineRule	数据内容 示例值：查看
ExcludeIds	否	否	Array of Uint64	需要排除的检测项id 示例值： [142]
Filters	否	否	Array of Filter	• ItemName - string - 是否必填：否 - 项名称 示例值：查看
IdType	否	否	Uint64	0:检测项，1:检测项分类 示例值： 0
SelectAll	否	否	Int64	是否过滤全选 示例值： 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
InternalError	内部错误。
InvalidParameter	参数错误。
FailedOperation	操作失败。

修改或新增基线忽略规则

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

更改基线忽略规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:06:22。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyBaselineRuleIgnore
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
AssetType	是	否	Int64	资产类型[0:所有专业版旗舰版
Filters	否	否	Array of Filter	• ItemName - string - 是否必填：否 - 项名称 示例值：查看
HostIds	否	否	Array of String	主机Id 示例值： ["4c4c4544-0053-4d10-8052-c4c04f53ayay"]
HostIps	否	否	Array of String	主机Ip 示例值： ["172.10.0.0"]
ItemIds	否	否	Array of Int64	关联项 示例值： [1000]
RuleId	否	否	Int64	规则Id 示例值： 100

参数名称	必选	允许NULL	类型	描述
RuleName	是	否	String	规则名称 示例值： Redis Check
SelectAll	否	否	Int64	是否全选过滤 示例值： 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
InternalError	内部错误。
InvalidParameter	参数错误。
FailedOperation	操作失败。

修改或新增弱口令

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

更改或新增弱口令

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:30:52。

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：ModifyBaselineWeakPassword
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Data	是	否	Array of BaselineWeakPassword	数据内容 示例值：查看

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
InternalError	内部错误。
InvalidParameter	参数错误。

检测基线

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

检测基线

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:33:13。

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：StartBaselineDetect
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Param	是	否	BaselineDetectParam	基线检测参数 示例值：查看

3. 输出参数

参数名称	类型	描述
TaskId	Int64	扫描任务ID 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。
FailedOperation	操作失败。

停止基线检测

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

停止基线检测

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:33:39。

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：StopBaselineDetect
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
TaskIds	是	否	Array of Int64	取消任务ID集合 示例值： [1106788]

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
InternalError	内部错误。
InvalidParameter	参数错误。

同步基线检测进度概要

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

同步基线检测进度概要

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:34:11。

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：SyncBaselineDetectSummary
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
TaskIds	否	否	Array of Uint64	用于计算检测中和进度的任务ID集合，一般不用传入 示例值： [1024]

3. 输出参数

参数名称	类型	描述
DetectingTaskIds	Array of Int64	正在检测的任务ID 示例值： [1002]
EndTime	String	结束时间 示例值： 2020-11-21 15:16:00
HostCount	Int64	主机总数 示例值： 0

参数名称	类型	描述
LeftMins	Int64	扫描中剩余时间(分钟) 示例值： 1
NotPassPolicyCount	Int64	未通过策略总数 示例值： 0
ProgressRate	Int64	处理进度 示例值： 70
StartTime	String	开始时间 示例值： 2020-11-21 15:16:00
WillFirstScan	Int64	1:即将进行首次扫描　0:已经扫描过了 示例值： 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
InternalError	内部错误。
FailedOperation	操作失败。

漏洞管理相关接口
取消漏洞忽略

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

取消漏洞忽略

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 14:58:05。

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：CancelIgnoreVul
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
EventIds	是	否	String	漏洞事件id串，多个用英文逗号分隔 示例值： 101,102

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

应急漏洞扫描

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

创建应急漏洞扫描任务

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：CreateEmergencyVulScan
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
TimeoutPeriod	否	否	Uint64	扫描超时时长 ，单位秒 示例值： 3600
Uuids	否	否	Array of String	自选服务器时生效，主机uuid的string数组 示例值： ["4aae2527-3030-41a5-a9f1-a2a002e848b6"]
VulId	是	否	Uint64	漏洞id 示例值： 105006

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

应急漏洞列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取应急漏洞列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 15:57:44。

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：DescribeEmergencyVulList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序字段 PublishDate LastScanTime HostCount 示例值： PublishDate
Filters	否	否	Array of Filters	过滤条件。 • Status - String - 是否必填：是 - 漏洞状态筛选，0//未检测 1有风险 ，2无风险 ，3 检查中展示progress • Level - String - 是否必填：否 - 漏洞等级筛选 1:低 2:中 3:高 4:提示 • VulName- String - 是否必填：否 - 漏洞名称搜索 • Uuids- String - 是否必填：否 - 主机uuid • IsSupportDefense - int- 是否必填：否 - 是否支持防御 0:不支持 1:支持 示例值：查看
HotspotAttack	否	否	Bool	是否热点漏洞 示例值： true

参数名称	必选	允许NULL	类型	描述
Limit	否	否	Uint64	返回数量，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Order	否	否	String	排序方式 desc，asc 示例值： desc

3. 输出参数

参数名称	类型	描述
ExistsRisk	Bool	是否存在风险 示例值： true
List	Array of EmergencyVul	漏洞列表 示例值：查看
TotalCount	Uint64	漏洞总条数 示例值： 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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询java内存马和rasp的是否注入风险服务配置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询java内存马和rasp是否注入风险服务配置

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeInjectRiskyServiceSwitch
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
JavaShellInjectRiskyServiceStatus	Uint64	内存马是否注入风险服务配置，0: 用户没有操作过，默认不注入 1: 注入,2:用户指定不注入 示例值： 1
List	Array of RiskMainClass	风险服务列表 示例值：查看
RaspInjectRiskyServiceStatus	Uint64	主机rasp是否注入风险服务配置，0: 用户没有操作过，默认不注入 1: 注入,2:用户指定不注入 示例值： 1

参数名称	类型	描述
TotalCount	Uint64	风险服务总条数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

查询检测进度

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

根据taskid查询检测进度

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeScanSchedule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
TaskId	是	否	Uint64	任务id 示例值： 1

3. 输出参数

参数名称	类型	描述
Schedule	Uint64	检测进度 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

定期检测配置查询

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询定期检测的配置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-03-06 19:25:22。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeScanVulSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
ClickTimeout	Uint64	一键扫描超时时长，如：1800秒（s） 示例值： 600
EnableScan	Uint64	是否开启 示例值： 1
EndTime	String	结束时间 示例值： 05:00
ScanMethod	Uint64	0版本比对,2版本比对+poc 示例值： 0

参数名称	类型	描述
StartTime	String	开始时间 示例值： 00:00
TimerInterval	Uint64	定期检测间隔时间（天） 示例值： 1
TimerTime	String	定期检测时间，如：00:00 示例值： 00:00
Uuids	Array of String	为空默认扫描全部专业版、旗舰版、普惠版主机，不为空只扫描选中主机 示例值： ["d99a1b46-cc2d-4633-a11f-4a7663d25ay*"]
VulCategories	String	漏洞类型：1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 示例值： 1
VulEmergency	Uint64	是否紧急漏洞：0-否 1-是 示例值： 1
VulLevels	String	危害等级：1-低危；2-中危；3-高危；4-严重 (多选英文逗号分隔) 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InternalError.MainDBFail	操作数据失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取指定漏洞分类统计数

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取漏洞管理模块指定类型的待处理漏洞数、主机数和非专业版主机数量

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeUndoVulCounts
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
IfEmergency	否	否	String	是否应急漏洞筛选, 是yes 其它否 示例值： yes
VulCategory	否	否	Uint64	漏洞分类，1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 示例值： 1

3. 输出参数

参数名称	类型	描述
NotProfessionCount	Uint64	普通版主机数 示例值： 1
UndoHostCount	Int64	未处理的主机数 示例值： 1

参数名称	类型	描述
UndoVulCount	Uint64	未处理的漏洞数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取近日指定类型的漏洞数量和主机数量

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

漏洞管理模块，获取近日指定类型的漏洞数量和主机数量

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulCountByDates
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
IfEmergency	否	否	String	是否为应急漏洞筛选 是: yes 示例值： 0
LastDays	否	否	Array of Uint64	需要查询最近几天的数据，需要天数都减去1后传入 示例值： [1]
VulCategory	否	否	Uint64	漏洞的分类: 1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 示例值： 1

3. 输出参数

参数名称	类型	描述
HostCount	Array of Uint64	批量获得对应天数的主机数量 示例值： [39]

参数名称	类型	描述
VulCount	Array of Uint64	批量获得对应天数的漏洞数量 示例值： [167]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取漏洞防御策略和事件统计

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取漏洞防御策略和事件统计

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeVulDefenceOverviewCount
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
MemberId	否	否	Array of String	集团账号的成员id 示例值： [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]

3. 输出参数

参数名称	类型	描述
StrategyCount	Uint64	策略数 示例值： 1
StrategyOpenCount	Uint64	开启的策略数 示例值： 1
SupportDefenceVulCount	Uint64	支持的防御漏洞个数 示例值： 2

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	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

查询漏洞防御设置列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询漏洞防御设置列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeVulDefenceSettingList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件：Switch、Keywords 示例值：查看
Limit	否	否	Uint64	数据限制 示例值： 20
MemberId	否	否	Array of String	集团账号的成员id 示例值： [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
Offset	否	否	Uint64	数据偏移 示例值： 12

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
List	Array of VulDefenceSetting	漏洞防御设置列表 示例值：查看
TotalCount	Uint64	数据总数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

漏洞影响主机列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

漏洞影响主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-07-25 15:56:07。

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：DescribeVulEffectHostList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件： • AliasName - String - 主机名筛选 • IP - String - 主机IP筛选 • InstanceID - String - 主机实例ID筛选 • TagIds - String - 主机标签id串，多个用英文用逗号分隔 • Status - String - 状态：0-待处理 1-忽略 3-已修复 5-检测中 6-修复中 8-修复失败 • Uuid - String数组 - Uuid串数组 • Version - String数组 - 付费版本数组："Flagship"-旗舰版 "PRO_VERSION"-专业版 "BASIC_VERSION"-基础版 • InstanceState - String数组 - 实例状态数组："PENDING"-创建中 "LAUNCH_FAILED"-创建失败 "RUNNING"-运行中 "STOPPED"-关机 "STARTING"-开机中 "STOPPING"-关机中 "REBOOTING"-重启中 "SHUTDOWN"-待销毁 "TERMINATING"-销毁中 "UNKNOWN"-未知（针对非云机器，且客户端离线的场景） 示例值：查看

参数名称	必选	允许NULL	类型	描述
Limit	是	否	Uint64	分页limit 最大100 示例值： 10
Offset	是	否	Uint64	分页Offset 示例值： 0
VulId	是	否	Uint64	漏洞id 示例值： 1

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	列表总数量 示例值： 1
VulEffectHostList	Array of VulEffectHostList	影响主机列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取待处理漏洞数+影响主机数

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取待处理漏洞数+影响主机数

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-27 19:13:29。

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：DescribeVulHostCountScanTime
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
IfFirstScan	Bool	是否第一次检测 示例值： true
LastFixTime	String	最后一次修复漏洞的时间 示例值： 2021-07-09 15:04:01
ScanTime	String	扫描时间 示例值： 2021-02-01 12:00:00
TaskId	Uint64	运行中的任务号, 没有任务则为0 示例值： 1

参数名称	类型	描述
TotalVulCount	Uint64	总漏洞数 示例值： 1
VulHostCount	Uint64	漏洞影响主机数 示例值： 1
hadAutoFixVul	Bool	是否有支持自动修复的漏洞事件 示例值： true
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

获取服务器风险top列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取服务器风险top列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 14:58:32。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulHostTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
IsFollowVul	否	否	Uint64	是否仅统计重点关注漏洞 1=仅统计重点关注漏洞, 0=统计全部漏洞 示例值： 1
Top	是	否	Uint64	获取top值，1-100 示例值： 1
VulCategory	否	否	Uint64	1:web-cms 漏洞，2.应用漏洞 4: Linux软件漏洞 5: windows系统漏洞 6:应急漏洞，不填或者填0时返回 1，2，4，5 的总统计数据 示例值： 2

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
VulHostTopList	Array of VulHostTopInfo	服务器风险top列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

漏洞详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

漏洞详情，带CVSS版本

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-18 10:31:53。

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：DescribeVulInfoCvss
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
VulId	是	否	Uint64	漏洞id 示例值： 1

3. 输出参数

参数名称	类型	描述
CVSS	String	CVSS信息 示例值： AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CveId	String	漏洞CVEID 示例值： CVE-2023-44487
CveInfo	String	cvss详情 示例值： AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

参数名称	类型	描述
CvssScore	Uint64	Cvss分数 示例值： 7.5
CvssScoreFloat	Float	cvss 分数 浮点型 示例值： 1
DefenseAttackCount	Uint64	已防御的攻击次数 示例值： 12
Description	String	漏洞描述信息 示例值： Apache OFBiz是美国阿帕奇（Apache）基金会的一套企业资源计划（ERP）系统。该系统提供了一整套基于Java的Web应用程序组件和工具。 Apache OFBiz 18.12.16之前版本存在代码问题漏洞，该漏洞源于容易受到服务端请求伪造和代码注入攻击。
FixSwitch	Int64	修复是否支持：0-windows/linux均不支持修复 ;1-windows/linux 均支持修复 ;2-仅linux支持修复;3-仅windows支持修复 示例值： 1
Labels	String	漏洞标签 多个逗号分割 示例值： 标签1,标签2
PublicDate	String	发布时间 示例值： 2024-09-04
Reference	String	参考链接 示例值： https://ofbiz.apache.org/download.html https://ofbiz.apache.org/security.html https://issues.apache.org/jira/browse/OFBIZ-13132
RepairPlan	String	修复方案 示例值： 官方已发布漏洞补丁及修复版本，请您评估您的业务是否受到影响，酌情升级至安全版本。\n【注意】：建议您升级前备份数据，以免发生意外。\nhttps://ofbiz.apache.org/download.html
SuccessFixCount	Uint64	全网修复成功次数, 不支持自动修复的漏洞默认返回0 示例值： 1
VulId	Uint64	漏洞id 示例值： 1

参数名称	类型	描述
VulLevel	Uint64	危害等级：1-低危；2-中危；3-高危；4-严重 示例值： 1
VulName	String	漏洞名称 示例值： Apache OFBiz SSRF到远程代码执行漏洞（CVE-2024-45507）
VulType	Uint64	漏洞分类 1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询漏洞数量等级分布统计

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

漏洞数量等级分布统计

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 14:59:07。

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：DescribeVulLevelCount
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
IsFollowVul	否	否	Uint64	是否仅统计重点关注漏洞 1=仅统计重点关注漏洞, 0=统计全部漏洞 示例值： 1
VulCategory	否	否	Uint64	1:web-cms 漏洞，2.应用漏洞 4: Linux软件漏洞 5: windows系统漏洞 6:应急漏洞，不填或者填0时返回 1，2，4，5 的总统计数据 示例值： 1

3. 输出参数

参数名称	类型	描述
VulLevelList	Array of VulLevelInfo	统计结果 示例值：查看

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	内部错误。

漏洞列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取漏洞列表数据

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-14 18:26:56。

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：DescribeVulList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序字段 Level，LastTime，HostCount 示例值： Level
Filters	否	否	Array of Filters	过滤条件。 • Status - String - 是否必填：否 - 处理状态 0-待处理 1-已加白 2-已删除 3-已修复 5-检测中 6-修复中 8-修复失败 • ModifyTime - String - 是否必填：否 - 最近发生时间 • Uuid- String - 是否必填：否 - 主机uuid查询 • VulName- string - • VulCategory- string - 是否必填：否 - 漏洞类别 1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 • IsSupportDefense - int- 是否必填：否 - 是否支持防御 0:不支持 1:支持 • Labels- string- 是否必填：否 - 标签搜索 • IsSupportAutoFix- string- 是否必填：否 - 是否支持自动修复 0:不支持 1:支持 • CvssScore- string- 是否必填：否 - CvssScore大于多少 • AttackLevel- string- 是否必填：否 - 攻击热度大于多少

参数名称	必选	允许NULL	类型	描述
				示例值：查看
Limit	否	否	Uint64	返回数量，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Order	否	否	String	排序顺序：desc 默认asc 示例值： desc

3. 输出参数

参数名称	类型	描述
FollowVulCount	Uint64	重点关注漏洞总数 示例值： 23
TotalCount	Uint64	漏洞总条数 示例值： 1
VulInfoList	Array of VulInfoList	漏洞列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。

错误码	描述
InvalidParameterValue	参数取值错误。

获取漏洞top统计

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

漏洞top统计

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 14:58:45。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
IsFollowVul	否	否	Uint64	是否仅统计重点关注漏洞 1=仅统计重点关注漏洞, 0=统计全部漏洞 示例值： 1
Top	是	否	Uint64	漏洞风险服务器top，1-100 示例值： 1
VulCategory	否	否	Uint64	1:web-cms 漏洞，2.应用漏洞 4: Linux软件漏洞 5: windows系统漏洞 6:应急漏洞，不填或者填0时返回 1，2，4，5 的总统计数据 示例值： 2

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
VulTopList	Array of VulTopInfo	漏洞top列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

导出本次漏洞检测Excel

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出本次漏洞检测Excel

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 14:55:06。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportVulDetectionExcel
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
TaskId	是	否	Uint64	本次漏洞检测任务id（不同于出参的导出本次漏洞检测Excel的任务Id） 示例值： 1596595610

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	该参数已废弃 示例值： http://1.2.3.4/result.zip
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址（不同于入参的本次漏洞检测任务id） 示例值： 1615549629
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

导出漏洞检测报告

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出漏洞检测报告。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：ExportVulDetectionReport
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤参数 • MachineName - String - 是否必填：否 - 主机别名 \n • Ip - String - 是否必填：否 - 主机ip \n • InstanceID - String - 是否必填：否 - 主机实例ID • Status - String - 是否必填：否 - 事件状态：0 待修复、1 忽略、3 已修复、5 检测中 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

参数名称	必选	允许NULL	类型	描述
TaskId	是	否	Uint64	漏洞扫描任务id（不同于出参的导出检测报告的任务Id） 示例值： 1596595610

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出文件下载链接地址 示例值： http://1.2.3.4/result.zip
TaskId	String	导出检测报告的任务Id（不同于入参的漏洞扫描任务id） 示例值： 1615549629
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

导出漏洞影响主机列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出漏洞影响主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 14:54:52。

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：ExportVulEffectHostList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件： • AliasName - String - 主机名筛选 • IP - String - 主机IP筛选 • InstanceID - String - 主机实例ID筛选 • TagIds - String - 主机标签id串，多个用英文用逗号分隔 • Status - String - 状态：0-待处理 1-忽略 3-已修复 5-检测中 6-修复中 8-修复失败 • Uuid - String数组 - Uuid串数组 • Version - String数组 - 付费版本数组："Flagship"-旗舰版 "PRO_VERSION"-专业版 "BASIC_VERSION"-基础版 • InstanceState - String数组 - 实例状态数组："PENDING"-创建中 "LAUNCH_FAILED"-创建失败 "RUNNING"-运行中 "STOPPED"-关机 "STARTING"-开机中 "STOPPING"-关机中 "REBOOTING"-重启中 "SHUTDOWN"-待销毁 "TERMINATING"-销毁中 "UNKNOWN"-未知（针对非云机器，且客户端离线的场景） 示例值：查看

参数名称	必选	允许NULL	类型	描述
VulId	是	否	Uint64	漏洞id 示例值： 1

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	已废弃 示例值： url
TaskId	String	导出任务Id，可通过ExportTasks 接口下载 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

漏洞管理-导出漏洞列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

漏洞管理-导出漏洞列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-03-21 10:26:24。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportVulList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • Status - String - 是否必填：否 - 处理状态 0 -- 待处理 1 -- 已加白 2 -- 已删除 3 - 已忽略 • ModifyTime - String - 是否必填：否 - 最近发生时间 • Uuid- String - 是否必填：否 - 主机uuid查询 • VulName- string - • VulCategory- string - 是否必填：否 - 漏洞类别 1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 • IsSupportDefense - int- 是否必填：否 - 是否支持防御 0:不支持 1:支持 • Labels- string- 是否必填：否 - 标签搜索 • IsSupportAutoFix- string- 是否必填：否 - 是否支持自动修复 0:不支持 1:支持 • CvssScore- string- 是否必填：否 - CvssScore大于多少 • AttackLevel- string- 是否必填：否 - 攻击热度大于多少

参数名称	必选	允许NULL	类型	描述
				示例值：查看
IfDetail	否	否	Uint64	是否导出详情,1是 0不是 示例值： 1

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出的文件下载url（已弃用！） 示例值： http://www.ay.com/ay
TaskId	String	导出文件Id 可通过ExportTasks接口下载 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

忽略漏洞

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (IgnoreImpactedHosts) 用于忽略漏洞。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 14:57:53。

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：IgnoreImpactedHosts
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	漏洞ID数组。 示例值： [545521374]

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
LimitExceeded.AreaQuota	超出批量添加数量。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

是否注入风险服务开关，包括内存马、rasp都是这个接口，容器rasp的开关在容器服务里

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

内存马和rasp是否注入风险服务开关

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyInjectRiskyServiceSwitch
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
JavaShellInjectRiskyServiceStatus	否	否	Uint64	内存马是否注入风险服务配置，0: 用户没有操作过，默认不注入 1: 注入,2: 用户指定不注入 示例值： 1
RaspInjectRiskyServiceStatus	否	否	Uint64	主机rasp是否注入风险服务配置，0: 用户没有操作过，默认不注入 1: 注入,2:用户指定不注入 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

一键检测

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

一键检测

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ScanVul
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
HostType	是	否	Uint64	服务器分类：1:专业版服务器；2:自选服务器 示例值： 1
QuuidList	否	否	Array of String	自选服务器时生效，主机quuid的string数组 示例值： ["69796250-2a3a-40ef-b418-676e677019a4"]
ScanMethod	否	否	Uint64	0版本比对，2版本比对+poc 示例值： 0
TimeoutPeriod	否	否	Uint64	超时时长 单位秒 默认 3600 秒 示例值： 180
VulCategories	否	否	String	漏洞类型：1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 (多选英文;分隔) 示例值： 1
VulEmergency	否	否	Uint64	是否是应急漏洞 0 否 1 是 示例值： 1

参数名称	必选	允许NULL	类型	描述
VulIds	否	否	Array of Uint64	需要扫描的漏洞id 示例值： [1]
VulLevels	是	否	String	危害等级：1-低危；2-中危；3-高危；4-严重 (多选英文;分隔) 示例值： 1

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	任务id 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
FailedOperation.APIServerFail	调用API服务失败。
FailedOperation.NoProfessionHost	无专业版主机。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

错误码	描述
FailedOperation	操作失败。

漏洞管理-重新检测接口

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

漏洞管理-重新检测接口

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ScanVulAgain
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
EventIds	是	否	String	漏洞事件id串，多个用英文逗号分隔 示例值： 1
Uuids	否	否	String	重新检查的机器uuid,多个逗号分隔 示例值： 05f0bcab-726c-4ea4-8109-bcd03d5598f7

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
ResourceNotFound	资源不存在。
FailedOperation.RescanVul	重新检测漏洞失败。
InvalidParameter.IllegalRequest	非法请求。
FailedOperation.APIServerFail	调用API服务失败。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

定期扫描漏洞设置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

定期扫描漏洞设置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-03-06 19:25:31。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ScanVulSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
EnableScan	否	否	Uint64	是否开启扫描 1开启 0不开启 示例值： 1
EndTime	否	否	String	扫描结束时间，如：08:00 示例值： 01:59
ScanMethod	否	否	Uint64	0版本比对，2版本比对+poc 示例值： 0
StartTime	否	否	String	扫描开始时间，如：00:00 示例值： 00:00
TimerInterval	是	否	Uint64	定期检测间隔时间（天） 示例值： 1
TimerTime	否	否	String	定期检测时间，如：02:10:50 示例值： 02:10:50

参数名称	必选	允许NULL	类型	描述
Uuids	否	否	Array of String	为空默认扫描全部专业版、旗舰版、普惠版主机，不为空只扫描选中主机 示例值： ["5a540076-d38a-4078-aa98-q45rt371d322"]
VulCategories	否	否	Array of Uint64	漏洞类型：1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞, 以数组方式传参[1,2] 示例值： [1]
VulEmergency	否	否	Uint64	是否是应急漏洞 0 否 1 是 示例值： 1
VulLevels	否	否	Array of Uint64	危害等级：1-低危；2-中危；3-高危；4-严重,以数组方式传参[1,2,3] 示例值： [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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

设置中心相关接口
创建安装主机安全agent任务

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

创建安装主机安全agent任务

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：CreateAgentInstallTask
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
AssetInfos	否	否	Array of AssetInfo	主机列表，全部安装时不必填 示例值：查看
MemberId	否	否	Array of String	集团账号的成员id 示例值：[{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
OpenAll	是	否	Bool	是否全部安装 示例值： true
OpenProtection	是	否	Bool	是否需要在安装完成后开启防护 示例值： true

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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

创建授权订单

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

CreateLicenseOrder 该接口可以创建专业版/旗舰版订单
支持预付费后付费创建
后付费订单直接创建成功
预付费订单仅下单不支付,需要调用计费支付接口进行支付

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-12 15:20:33。

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：CreateLicenseOrder
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
AutoProtectOpenConfig	否	否	String	该字段作废 示例值： "no config"
AutoRenewFlag	否	否	Bool	是否自动续费, 默认不自动续费. 该参数仅包年包月生效 示例值： false
BillingDefineParams	否	否	BillingDefineParams	业务自定义参数 示例值：查看

参数名称	必选	允许NULL	类型	描述
LicenseNum	否	否	Uint64	授权数量，需要购买的数量. 默认为1 示例值： 1
LicenseType	否	否	Uint64	授权类型 0 专业版, 5 旗舰版 示例值： 0
ModifyConfig	否	否	OrderModifyObject	变配参数 示例值：查看
ProjectId	否	否	Uint64	项目ID . 默认为0 示例值： 0
RegionId	否	否	Uint64	计费价格所属地域code 示例值： 1
Tags	否	否	Array of Tags	标签数组, 空则表示不需要绑定标签 示例值：查看
TimeSpan	否	否	Uint64	未使用字段 示例值： 1

3. 输出参数

参数名称	类型	描述
BigDealId	String	大订单号，后付费该字段空值 示例值： order-vmqkfmayay
DealNames	Array of String	订单号列表 示例值： ["cwp-313dfay*", "cwp-vi4d8ay*"]
ResourceIds	Array of String	资源ID列表,预付费订单该字段空值 示例值： ["cwp-313dfay*", "cwp-vi4d8ay*"]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

删除授权记录

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

对授权管理-订单列表内已过期的订单进行删除.(删除后的订单不在统计范畴内)

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-09 10:49:46。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteLicenseRecord
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
LicenseId	是	否	Uint64	授权ID ,可以用授权订单列表获取. 示例值： 1
LicenseType	是	否	Uint64	授权类型 0 专业版, 5 旗舰版 示例值： 0
ResourceId	是	否	String	资源ID 示例值： cwplic-9090ayay

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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取机器安装结果

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取机器安装结果

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeAgentInstallResult
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
AssetInfos	否	否	Array of AssetInfo	主机列表 示例值：查看
MemberId	否	否	Array of String	集团账号的成员id 示例值：[{"mem-6wfo0fzks3","mem-85fo0fzks4"}]

3. 输出参数

参数名称	类型	描述
AgentInstallResults	Array of AgentInstallResult	安装结果列表 示例值：查看

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	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取ageng安装任务完成情况

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取ageng安装任务完成情况

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeAgentInstallTaskResult
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
MemberId	否	否	Array of String	集团账号的成员id 示例值： [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
TaskIds	是	否	Array of Uint64	agent安装任务ID 示例值： [1]

3. 输出参数

参数名称	类型	描述
Assets	Array of AgentInstallTaskResult	agent安装任务详情 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取修改中的主机列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取修改中的主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeChangingAssetInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
MemberId	否	否	Array of String	集团账号的成员id 示例值：[{"mem-6wfo0fzks3","mem-85fo0fzks4"}]

3. 输出参数

参数名称	类型	描述
AssetInfos	Array of AssetChangeInfo	资产列表 示例值：查看
TaskIds	Array of Uint64	agent安装任务ID列表 示例值： [1]

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	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

查看授权绑定列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

该接口可以获取设置中心-授权管理,某个授权下已绑定的授权机器列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-09 10:50:08。

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：DescribeLicenseBindList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	• InstanceID、IP、 MachineName 模糊查询 • Keywords 主机名或ip模糊查询 • AgentStatus 状态：在线ONLINE、离线OFFLINE、未防护UNINSTALLED、关机SHUTDOWN、开通专业版并且机器已销毁TERMINATED_PRO_VERSION 示例值：查看
LicenseId	是	否	Uint64	授权ID 示例值： 1
LicenseType	是	否	Uint64	授权类型, 0 专业版, 5 旗舰版 示例值： 0
Limit	否	否	Uint64	限制条数,默认10. 示例值： 10

参数名称	必选	允许NULL	类型	描述
Offset	否	否	Uint64	偏移量,默认0. 示例值： 0
ResourceId	是	否	String	资源ID 示例值： any data

3. 输出参数

参数名称	类型	描述
List	Array of LicenseBindDetail	绑定机器列表信息 示例值：查看
TotalCount	Uint64	总条数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameterValue	参数取值错误。

查询授权绑定进度

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询授权绑定任务的进度

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:09:36。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeLicenseBindSchedule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤参数 Status 绑定进度状态 0 进行中 1 已完成 2 失败 示例值：查看
Limit	否	否	Uint64	限制条数,默认10. 示例值： 10
Offset	否	否	Uint64	偏移量,默认0 示例值： 0
TaskId	是	否	Uint64	任务ID 示例值： 1

3. 输出参数

参数名称	类型	描述
List	Array of LicenseBindTaskDetail	绑定任务详情 示例值：查看
Schedule	Uint64	进度 示例值： 20
TotalCount	Uint64	总条数 示例值： 12
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。

授权概览信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

授权管理-授权概览信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-12 15:17:14。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeLicenseGeneral
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AutoOpenStatus	Bool	自动升级开关状态,默认 false，true 开启, false 关闭 示例值： false
AutoRepurchaseRenewSwitch	Bool	自动加购订单是否自动续费 ,true 开启, false 关闭 示例值： false
AutoRepurchaseSwitch	Bool	自动加购开关, true 开启, false 关闭 示例值： false
AvailableFlagshipVersionLicenseCnt	Uint64	可用旗舰版授权数 示例值： 1

参数名称	类型	描述
AvailableLHLicenseCnt	Uint64	可用惠普版授权数 示例值： 0
AvailableLicenseCnt	Uint64	可用授权数 示例值： 3
AvailableProVersionLicenseCnt	Uint64	可用专业版授权数(包含后付费). 示例值： 2
CwpVersionLicenseCnt	Uint64	普惠版总授权数(有效订单的授权数) 示例值： 0
DestroyOrderNum	Uint64	已销毁订单数 示例值： 0
ExpireLicenseCnt	Uint64	已到期授权数(不包含已删除的记录) 示例值： 0
FlagshipVersionLicenseCnt	Uint64	旗舰版总授权数(有效订单) 示例值： 1
IsOpenStatusHistory	Bool	历史是否开通过自动升级开关 示例值： false
LicenseCnt	Uint64	总授权数 (包含隔离,过期等不可用状态) 示例值： 3
NearExpiryLicenseCnt	Uint64	即将到期授权数 (15天内到期的) 示例值： 0
NotExpiredLicenseCnt	Uint64	未到期授权数 示例值： 3
ProVersionLicenseCnt	Uint64	专业版总授权数(有效订单) 示例值： 2
ProtectType	String	PROVERSION_POSTPAY 专业版-后付费, PROVERSION_PREPAY 专业版-预付费, FLAGSHIP_PREPAY 旗舰版-预付费 示例值： PROVERSION_POSTPAY
RepurchaseRenewSwitch	Bool	自动加购是否自动续费开关,true 开启,false 关闭 示例值： false
UsedLicenseCnt	Uint64	已使用授权数 示例值： 0

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	内部错误。

获取授权订单列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取用户所有授权订单信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-12 15:20:20。

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：DescribeLicenseList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	多个条件筛选时取交集 • LicenseStatus 授权状态信息,0 未使用,1 部分使用, 2 已用完, 3 不可用 4 可使用 • BuyTime 购买时间 • LicenseType 授权类型, 0 专业版, 5 旗舰版/li> • DeadlineStatus 到期状态 NotExpired 未过期, Expire 已过期(包含已销毁) NearExpiry 即将到期 • ResourceId 资源ID • Keywords IP筛选 • PayMode 付费模式 0 按量计费，1 包年包月 • OrderStatus 订单状态 1 正常 2 隔离 3 销毁 • DealNames 子订单号,最大长度10个,超出会失败 示例值：查看
Limit	否	否	Uint64	限制条数,默认10. 示例值： 10

参数名称	必选	允许NULL	类型	描述
Offset	否	否	Uint64	偏移量,默认0. 示例值： 0
ResourceIds	否	否	Array of String	资源ID列表筛选(与Filters.ResourceId 不能共存,同时出现则优先使用ResourceIds) 示例值： ["cwp-1sd324s"]
Tags	否	否	Array of Tags	标签筛选,平台标签能力,这里传入 标签键,标签值作为一个对象 示例值：查看

3. 输出参数

参数名称	类型	描述
List	Array of LicenseDetail	授权数列表信息 示例值：查看
TotalCount	Uint64	总条数 示例值： 12
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

更新用户告警设置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

更新或者插入用户告警设置(该接口废弃,请调用 ModifyWarningSetting)

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeSaveOrUpdateWarnings
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
WarningObjects	否	否	Array of WarningObject	告警设置的修改内容 示例值：查看

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

获取当前用户告警列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取当前用户告警列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-23 11:47:34。

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：DescribeWarningList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
WarningInfoList	Array of WarningInfoObj	获取告警列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

获取告警服务IP名单

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取告警服务IP名单

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeWarningServiceIPList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息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	Array of String	列表 示例值： ["192.168.0.204"]
UpdateTime	String	最近更新时间 示例值： 2024-08-01
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

销毁订单

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

DestroyOrder 该接口可以对资源销毁.

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-27 11:44:19。

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：DestroyOrder
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
LicenseType	是	否	Uint64	授权类型, 0 专业版, 5 旗舰版 示例值： 0
ResourceId	是	否	String	资源ID 示例值： resource_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
InvalidParameterValue	参数取值错误。
InternalError	内部错误。
ResourceNotFound	资源不存在。
OperationDenied	操作被拒绝。

导出授权详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出授权列表对应的绑定信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-01 11:06:27。

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：ExportLicenseDetail
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
ExportMonth	否	否	String	导出月份, 该参数仅在IsHistory 时可选. 示例值： 2022-03
Filters	否	否	Array of Filters	条件 • LicenseType 授权类型, 0 专业版, 5 旗舰版 • ResourceId 资源ID 示例值：查看
IsHistory	否	否	Bool	是否导出全部授权详情 示例值： false
Tags	否	否	Array of Tags	标签筛选,平台标签能力,这里传入 标签键,标签值作为一个对象 示例值：查看

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	下载地址,该字段废弃 示例值： url
TaskId	Uint64	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
ResourceNotFound	资源不存在。

修改主机防护状态

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

修改主机防护状态

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyAssetsProtectionStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
AssetInfos	否	否	Array of AssetInfo	主机列表，OpenAll参数为True时不必填 示例值：查看
MemberId	否	否	Array of String	集团账号的成员id 示例值：[{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
OpenAll	是	否	Bool	是否全部开通 示例值： true
Status	是	否	Uint64	开启状态：0-关闭，1-开启 示例值： 1

3. 输出参数

参数名称	类型	描述
Assets	Array of AgentInstallResult	操作结果列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

设置自动开通配置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

用于设置新增主机自动开通专业防护配置。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-12 15:15:05。

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：ModifyAutoOpenProVersionConfig
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
AutoRepurchaseRenewSwitch	否	否	Uint64	自动加购的订单是否自动续费,默认0 ,0关闭, 1开启 示例值： 1
AutoRepurchaseSwitch	否	否	Uint64	自动加购/扩容授权开关,默认 1, 0关闭, 1开启 示例值： 1
ProtectType	否	否	String	加固防护模式 PROVERSION_POSTPAY 专业版-按量计费 PROVERSION_PREPAY 专业版-包年包月 FLAGSHIP_PREPAY 旗舰版-包年包月 示例值： PROVERSION_POSTPAY

参数名称	必选	允许NULL	类型	描述
RepurchaseRenewSwitch	否	否	Uint64	手动购买的订单是否自动续费,默认0, 0关闭 ,1 开启 示例值： 0
Status	是	否	String	设置自动开通状态。 • CLOSE：关闭 • OPEN：打开 示例值： OPEN

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
InternalError	内部错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

授权批量绑定

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

设置中心-授权管理 对某个授权批量绑定机器

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-27 11:43:44。

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：ModifyLicenseBinds
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
IsAll	否	否	Bool	是否全部机器(当全部机器数大于当前订单可用授权数时,多余机器会被跳过) 示例值： true
LicenseType	是	否	Uint64	授权类型 0 专业版, 5 旗舰版 示例值： 0
QuuidList	否	否	Array of String	需要绑定的机器quuid列表, 当IsAll = false 时必填,反之忽略该参数. 最大长度=2000 示例值： ["4c4c4544-004c-5410-805a-cac04f46ayay"]
ResourceId	是	否	String	资源ID 示例值： 1

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	任务ID 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

编辑《主机安全-按量计费》授权订单

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

编辑授权订单

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyLicenseOrder
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Alias	否	否	String	资源别名,不修改则输入原值. 示例值： use_for_redis
InquireNum	否	否	Uint64	预期值,如果当前为10,扩容则输入原来大的值, 缩容则比原来小的值(缩容时不允许预期值比使用量小),如果保持不变则填写原值, 示例值： 1
ProjectId	否	否	Uint64	项目ID,不修改则输入原值. 示例值： 1
ResourceId	是	否	String	资源ID 示例值： cwplic-dwsds

3. 输出参数

参数名称	类型	描述
DealNames	Array of String	订单号 示例值：["6723561253"]
ResourceIds	Array of String	资源ID 示例值：["cwplic-dwsds"]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

授权批量解绑

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

设置中心-授权管理 对某个授权批量解绑机器

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-27 11:43:31。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyLicenseUnBinds
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
IsAll	否	否	Bool	是否全部机器(当全部机器数大于当前订单可用授权数时,多余机器会被跳过) 示例值： true
IsShrink	否	否	Bool	是否自动缩容,如果授权数剩余1,则销毁订单 示例值： false
LicenseType	是	否	Uint64	授权类型 0 专业版, 5 旗舰版 示例值： 0
QuuidList	否	否	Array of String	需要绑定的机器quuid列表, 当IsAll = false 时必填,反之忽略该参数. 最大长度=100 示例值： ["4c4c4544-0053-4d10-8052-c4c04f53ayay"]
ResourceId	是	否	String	资源ID 示例值： cwplic-92c9ayay

3. 输出参数

参数名称	类型	描述
ErrMsg	Array of LicenseUnBindRsp	只有解绑失败的才有该值. 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

编辑订单属性

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

对订单属性编辑

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-27 11:37:33。

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：ModifyOrderAttribute
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
AttrName	是	否	String	可编辑的属性名称 ,当前支持的有: alias 资源别名 projectId 项目ID 示例值： alias
AttrValue	是	否	String	属性值 AttrName=alias时,任意字符串,最大字符15长度 AttrName=projectId时,项目ID必须是真实存在的 示例值： 资源名称
LicenseType	是	否	Uint64	授权类型 0 专业版, 5 旗舰版 示例值： 1
ResourceId	是	否	String	资源ID 示例值： resource_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
InternalError	内部错误。
InvalidParameter.MissingParameter	参数缺失。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

修改告警设置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

修改告警设置

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-23 11:48:21。

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：ModifyWarningSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
WarningObjects	是	否	Array of WarningObject	修改告警设置的内容 示例值：查看

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

资产管理相关接口
对旗舰版机器单次触发事件调查及告警回溯

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

触发事件调查回溯

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：CreateIncidentBacktracking
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Quuid	是	否	String	主机安全quuid 示例值： c973997a-36ad-4374-860a-fa462281ayay

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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

删除AK配置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除AK记录

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DeleteCloudVendorAccountAK
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	Int64	记录ID 示例值： 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

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

卸载云镜客户端

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口（DeleteMachine）用于卸载云镜客户端。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-26 17:06:53。

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：DeleteMachine
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
MemberId	否	否	Array of String	集团账号的成员id 示例值： [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
Uuid	是	否	String	主机安全客户端Uuid。 示例值： 97d7cec6-0f2a-b636-e340-43f212dbb33c

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
FailedOperation.MachineDelete	卸载主机。
InternalError.MainDBFail	操作数据失败。
FailedOperation.APIServerFail	调用API服务失败。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

删除服务器关联的标签

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除服务器关联的标签

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DeleteMachineTag
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Rid	是	否	Uint64	关联的标签ID 示例值： 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

错误码	描述
InternalError	内部错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

删除标签

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除标签

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DeleteTags
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	标签ID (最大100 条) 示例值： [16500]

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
FailedOperation	操作失败。

获取帐号统计列表数据

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (DescribeAccountStatistics) 用于获取帐号统计列表数据。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeAccountStatistics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • Username - String - 是否必填：否 - 帐号用户名 示例值：查看
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
AccountStatistics	Array of AccountStatistics	帐号统计列表。 示例值：查看
TotalCount	Uint64	帐号统计列表记录总数。 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询应用列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询应用列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetAppList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime
Filters	否	否	Array of AssetFilters	过滤条件。 • AppName- string - 是否必填：否 - 应用名搜索 • IP - String - 是否必填：否 - 主机ip • MachineName - String - 是否必填：否 - 主机名称 • InstanceID - string - 是否必填：否 - 实例ID • Type - int - 是否必填：否 - 类型：仅linux 0: 全部 1: 运维 2：数据库 3：安全 4：可疑应用 5：系统架构 6：系统应用 7：WEB服务 99:其他 • OsType - String - 是否必填：否 - windows/linux • OsName -String 是否必填: 否 - 操作系统

参数名称	必选	允许NULL	类型	描述
				（DescribeMachineOsList 接口 值） 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 1
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 1
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： asc
Quuid	否	否	String	查询指定Quuid主机的信息 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
Apps	Array of AssetAppBaseInfo	应用列表 示例值：查看
Total	Uint64	总数量 示例值： 1021
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。

错误码	描述
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取软件关联进程列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取软件关联进程列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetAppProcessList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息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 示例值： 1
Name	是	否	String	App名 示例值： mysql
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 1
Quuid	是	否	String	主机Quuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	是	否	String	主机Uuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
Process	Array of AssetAppProcessInfo	进程列表 示例值：查看
Total	Uint64	分区总数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取内核模块详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取内核模块详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetCoreModuleInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	String	内核模块ID 示例值： 1001
Quuid	是	否	String	服务器Quuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	是	否	String	服务器Uuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
Module	AssetCoreModuleDetail	内核模块详情 示例值：查看

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	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询资产管理内核模块列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询资产管理内核模块列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetCoreModuleList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序依据[Size
Filters	否	否	Array of AssetFilters	过滤条件。 • IP - String - 是否必填：否 - 主机ip • MachineName - String - 是否必填：否 - 主机名称 • InstanceID - string - 是否必填：否 - 实例ID • Name- string - 是否必填：否 - 包名 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

参数名称	必选	允许NULL	类型	描述
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： asc
Quuid	否	否	String	服务器Quuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	否	否	String	服务器Uuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
Modules	Array of AssetCoreModuleBaseInfo	列表 示例值：查看
Total	Uint64	总数量 示例值： 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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。

错误码	描述
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取资产管理数据库详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取资产管理数据库详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetDatabaseInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	String	数据库ID 示例值： 1
Quuid	是	否	String	服务器Quuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	是	否	String	服务器Uuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
Database	AssetDatabaseDetail	数据库详情 示例值：查看

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	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询资产管理数据库列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询资产管理数据库列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetDatabaseList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime] 示例值： FirstTime
Filters	否	否	Array of AssetFilters	过滤条件。 • MachineName- String - 是否必填：否 - 主机别名筛选 • IP- String - 是否必填：否 - 主机ip筛选 • InstanceID- String - 是否必填：否 - 主机实例ID筛选 • User- string - 是否必填：否 - 运行用户 • Port - Int - 是否必填：否 - 端口 • Name - Int - 是否必填：否 - 数据库名称 0:全部 1:MySQL 2:Redis 3:Oracle 4:MongoDB 5:MemCache 6:PostgreSQL 7:HBase

参数名称	必选	允许NULL	类型	描述
				8:DB2 9:Sybase 10:TiDB • Proto - String - 是否必填：否 - 协议：1:TCP, 2:UDP, 3:未知 • OsType - String - 是否必填：否 - 操作系统: linux/windows • OsName -String 是否必填: 否 - 操作系统（DescribeMachineOsList 接口 值） 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 1
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 1
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： desc
Quuid	否	否	String	查询指定Quuid主机的信息 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
Databases	Array of AssetDatabaseBaseInfo	列表 示例值：查看
Total	Uint64	总数量 示例值： 21
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取主机所有资源数量

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取主机所有资源数量

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetHostTotalCount
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Quuid	是	否	String	主机Quuid 示例值： ed12c76b-2f65-4d44-a001-8f60cce9ayay
Uuid	是	否	String	主机Uuid 示例值： ed12c76b-2f65-4d44-a001-8f60cce9ayay

3. 输出参数

参数名称	类型	描述
Types	Array of AssetKeyVal	各项资源数量 system : 资源监控 account: 账号 port: 端口 process: 进程 app: 应用软件 database:数据库

参数名称	类型	描述
		webapp: Web应用 webframe: Web框架 webservice: Web服务 weblocation: Web站点 systempackage: 系统安装包 jar: jar包 initservice:启动服务 env: 环境变量 coremodule: 内核模块 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取资产数量概况

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取资产数量： 主机数、账号数、端口数、进程数、软件数、数据库数、Web应用数、Web框架数、Web服务数、Web站点数

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:54:33。

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：DescribeAssetInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AccountCount	Uint64	账号数 示例值： 1
AccountNewCount	Int64	账号今日新增 示例值： 1
DatabaseCount	Uint64	数据库数 示例值： 1
DatabaseNewCount	Int64	数据库今日新增 示例值： 1

参数名称	类型	描述
MachineCount	Uint64	主机数 示例值： 1
MachineNewCount	Int64	主机今日新增 示例值： 1
PortCount	Uint64	端口数 示例值： 1
PortNewCount	Int64	端口今日新增 示例值： 1
ProcessCount	Uint64	进程数 示例值： 1
ProcessNewCount	Int64	进程今日新增 示例值： 1
SoftwareCount	Uint64	软件数 示例值： 1
SoftwareNewCount	Int64	软件今日新增 示例值： 1
WebAppCount	Uint64	Web应用数 示例值： 1
WebAppNewCount	Int64	Web应用今日新增 示例值： 1
WebFrameCount	Uint64	Web框架数 示例值： 1
WebFrameNewCount	Int64	Web框架今日新增 示例值： 1
WebLocationCount	Uint64	Web站点数 示例值： 1
WebLocationNewCount	Int64	Web站点今日新增 示例值： 1
WebServiceCount	Uint64	Web服务数 示例值： 1
WebServiceNewCount	Int64	Web服务今日新增 示例值： 1

版权所有：TCloudFinanceZone

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	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询资产管理启动服务列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询资产管理启动服务列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetInitServiceList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime] 示例值： FirstTime
Filters	否	否	Array of AssetFilters	过滤条件。 • IP - String - 是否必填：否 - 主机ip • MachineName - String - 是否必填：否 - 主机名称 • InstanceID - string - 是否必填：否 - 实例ID • Name- string - 是否必填：否 - 包名 • User- string - 是否必填：否 - 用户 • IsAutoRun - string - 是否必填：否 - 是否开机自启动：0否，1是 • Status- string - 是否必填：否 - 默认启用状态：0未启用， 1启用 仅linux • Type- string - 是否必填：否 - 类型：类型 仅windows： 1:编码器 2:IE插件 3:网络提供者

参数名称	必选	允许NULL	类型	描述
				4:镜像劫持 5:LSA提供者 6:KnownDLLs 7:启动执行 8:WMI 9:计划任务 10:Winsock提供者 11:打印监控器 12:资源管理器 13:驱动服务 14:登录 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 1
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 11
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： desc
Quuid	否	否	String	服务器Quuid 示例值： 1
Uuid	否	否	String	服务器Uuid 示例值： 1

3. 输出参数

参数名称	类型	描述
Services	Array of AssetInitServiceBaseInfo	列表 示例值：查看
Total	Uint64	总数量 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
ResourceNotFound	资源不存在。

获取Jar包详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取Jar包详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetJarInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	String	Jar包ID 示例值： 1
Quuid	是	否	String	服务器Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Uuid	是	否	String	服务器Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

3. 输出参数

参数名称	类型	描述
Jar	AssetJarDetail	Jar包详情 示例值：查看

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
ResourceNotFound	资源不存在。
InternalError	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询Jar包列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询Jar包列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetJarList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime] 示例值： FirstTime
Filters	否	否	Array of AssetFilters	过滤条件。 • IP - String - 是否必填：否 - 主机ip • MachineName - String - 是否必填：否 - 主机名称 • InstanceID - string - 是否必填：否 - 实例ID • Name- string - 是否必填：否 - 包名 • Type- uint - 是否必填：否 - 类型 1: 应用程序 2 : 系统类库 3 : Web服务自带库 4 : 其他依赖包 • Status- string - 是否必填：否 - 是否可执行：0否，1是 示例值：查看

参数名称	必选	允许NULL	类型	描述
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 1
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 1
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： desc
Quuid	否	否	String	服务器Quuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	否	否	String	服务器Uuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
Jars	Array of AssetJarBaseInfo	应用列表 示例值：查看
Total	Uint64	总数量 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。

错误码	描述
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取资产管理主机资源详细信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取资产管理主机资源详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetMachineDetail
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Quuid	是	否	String	服务器Quuid 示例值： de92dec8-d312-49c5-b3e4-505584eeayay
Uuid	是	否	String	服务器Uuid 示例值： de92dec8-d312-49c5-b3e4-505584eeayay

3. 输出参数

参数名称	类型	描述
MachineDetail	AssetMachineDetail	主机详情 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取资源监控列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取资产指纹页面的资源监控列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetMachineList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序[FirstTime
Filters	否	否	Array of Filter	过滤条件。 • MachineName 主机名称 • InstanceID 实例ID • IP 内网IP或公网IP • OsType - String - 是否必填：否 - windows或linux • CpuLoad - Int - 是否必填：否 - 0: 未知 1: 低负载 2: 中负载 3: 高负载 • DiskLoad - Int - 是否必填：否 - 0: 0%或未知 1: 0%～20% 2: 20%～50% 3: 50%～80% 4: 80%～100% • MemLoad - Int - 是否必填：否 - 0: 0%或未知 1: 0%～20% 2: 20%～50% 3: 50%～80% 4: 80%～100% • Quuid：主机Quuid

参数名称	必选	允许NULL	类型	描述
				• OsName -String 是否必填: 否 - 操作系统（DescribeMachineOsList 接口 值） 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： asc

3. 输出参数

参数名称	类型	描述
Machines	Array of AssetMachineBaseInfo	记录列表 示例值：查看
Total	Uint64	总数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询资产管理计划任务列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询资产管理计划任务列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetPlanTaskList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime] 示例值： FirstTime
Filters	否	否	Array of AssetFilters	过滤条件。 • IP - String - 是否必填：否 - 主机ip • MachineName - String - 是否必填：否 - 主机名称 • InstanceID - string - 是否必填：否 - 实例ID • User- string - 是否必填：否 - 用户 • Status- int - 是否必填：否 - 默认启用状态：0未启用， 1启用 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 1
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 1

参数名称	必选	允许NULL	类型	描述
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： desc
Quuid	否	否	String	服务器Quuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	否	否	String	服务器Uuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
Tasks	Array of AssetPlanTask	列表 示例值：查看
Total	Uint64	总数量 示例值： 12
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。

错误码	描述
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取资产管理端口列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取资产管理端口列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetPortInfoList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime
Filters	否	否	Array of Filter	过滤条件。 • Port - uint64 - 是否必填：否 - 端口 • IP - String - 是否必填：否 - 主机ip • MachineName - String - 是否必填：否 - 主机名称 • InstanceID - string - 是否必填：否 - 实例ID • ProcessName - String - 是否必填：否 - 监听进程 • Pid - uint64 - 是否必填：否 - PID • User - String - 是否必填：否 - 运行用户 • Group - String - 是否必填：否 - 所属用户组 • Ppid - uint64 - 是否必填：否 - PPID • Proto - string - 是否必填：否 - 端口协议tcp/udp/unknow • OsType - string - 是否必填：否 - windows/linux • RunTimeStart - String - 是否必填：否 - 运行开始时间 • RunTimeEnd - String - 是否必填：否 - 运行结束时间 • BindIp - String - 是否必填：否 - 绑定IP

参数名称	必选	允许NULL	类型	描述
				• OsName -String 是否必填: 否 - 操作系统（DescribeMachineOsList 接口 值） 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 1
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： asc
Quuid	否	否	String	查询指定Quuid主机的信息 示例值： 37b6df34-68f1-4ab8-a3d8-7b89de604c82

3. 输出参数

参数名称	类型	描述
Ports	Array of AssetPortBaseInfo	列表 示例值：查看
Total	Uint64	记录总数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。

错误码	描述
InvalidParameterValue	参数取值错误。

获取资产管理进程列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取资产管理进程列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetProcessInfoList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime
Filters	否	否	Array of Filter	过滤条件。 • IP - String - 是否必填：否 - 主机ip • MachineName - String - 是否必填：否 - 主机名称 • InstanceID - string - 是否必填：否 - 实例ID • Name - String - 是否必填：否 - 进程名 • User - String - 是否必填：否 - 进程用户 • Group - String - 是否必填：否 - 进程用户组 • Pid - uint64 - 是否必填：否 - 进程ID • Ppid - uint64 - 是否必填：否 - 父进程ID • OsType - string - 是否必填：否 - windows/linux • Status - string - 是否必填：否 - 进程状态： 1:R 可执行 2:S 可中断 3:D 不可中断 4:T 暂停状态或跟踪状态 5:Z 僵尸状态 6:X 将被销毁

参数名称	必选	允许NULL	类型	描述
				• RunTimeStart - String - 是否必填：否 - 运行开始时间 • RunTimeEnd - String - 是否必填：否 - 运行结束时间 • InstallByPackage - uint64 - 是否必填：否 - 是否包安装：0否，1是 • OsName -String 是否必填: 否 - 操作系统（DescribeMachineOsList 接口 值） 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 12
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 100
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： asc
Quuid	否	否	String	查询指定Quuid主机的信息 示例值： 392f05bd-bf86-4911-8cf9-b8c2ac0f62ab

3. 输出参数

参数名称	类型	描述
Process	Array of AssetProcessBaseInfo	列表 示例值：查看
Total	Uint64	记录总数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

错误码	描述
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取主机概况趋势

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取主机最近趋势情况

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetRecentMachineInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
BeginDate	是	否	Date	开始时间，如：2020-09-22 示例值： 2020-10-10
EndDate	是	否	Date	结束时间，如：2020-09-22 示例值： 2020-10-10

3. 输出参数

参数名称	类型	描述
LiveList	Array of AssetKeyVal	在线数量列表 示例值：查看
OfflineList	Array of AssetKeyVal	离线数量列表 示例值：查看

参数名称	类型	描述
RiskList	Array of AssetKeyVal	风险数量列表 示例值：查看
TotalList	Array of AssetKeyVal	总数量列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter.DateRange	时间区间格式错误。
UnknownParameter	未知参数错误。

获取资产管理系统安装包列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取资产管理系统安装包列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetSystemPackageList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序方式可选：[FistTime
Filters	否	否	Array of Filter	过滤条件。 • IP - String - 是否必填：否 - 主机ip • MachineName - String - 是否必填：否 - 主机名称 • InstanceID - string - 是否必填：否 - 实例ID • Name - String - 是否必填：否 - 包 名 • StartTime - String - 是否必填：否 - 安装开始时间 • EndTime - String - 是否必填：否 - 安装开始时间 • Type - int - 是否必填：否 - 安装包类型： 1:rpm 2:dpkg 3:java 4:system 示例值：查看

参数名称	必选	允许NULL	类型	描述
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 1
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 11
Order	否	否	String	排序方式，asc-升序 或 desc-降序。默认：desc-降序 示例值： asc
Quuid	是	否	String	主机Quuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	是	否	String	主机Uuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
Packages	Array of AssetSystemPackageInfo	列表 示例值：查看
Total	Uint64	记录总数 示例值： 12
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取主机账号详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取主机账号详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetUserInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Name	是	否	String	账户名 示例值： any_user
Quuid	是	否	String	云服务器UUID 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	是	否	String	主机安全UUID 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
User	AssetUserDetail	用户详细信息 示例值：查看

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	内部错误。
InvalidParameter.MissingParameter	参数缺失。
InternalError.MainDBFail	操作数据失败。

获取账号列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取账号列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetUserList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序：[FirstTime
Filters	否	否	Array of Filter	过滤条件。 • IP - String - 是否必填：否 - 主机ip • MachineName - String - 是否必填：否 - 主机名称 • InstanceID - string - 是否必填：否 - 实例ID • Name - String - 是否必填：否 - 账户名（模糊匹配） • NameStrict - String - 是否必填：否 - 账户名（严格匹配） • Uid - uint64 - 是否必填：否 - Uid • Gid - uint64 - 是否必填：否 - Gid • LoginTimeStart - String - 是否必填：否 - 开始时间，如：2021-01-11 • LoginTimeEnd - String - 是否必填：否 - 结束时间，如：2021-01-11 • LoginType - uint64 - 是否必填：否 - 0-不可登录；1-只允许key登录；2只允许密码登录；3-允许key和密码 仅linux • OsType - String - 是否必填：否 - windows或linux • Status - uint64 - 是否必填：否 - 账号状态：0-禁用；1-启用

参数名称	必选	允许NULL	类型	描述
				• UserType - uint64 - 是否必填：否 - 账号类型：0访客用户，1标准用户，2管理员用户 仅windows • IsDomain - uint64 - 是否必填：否 - 是否域账号：0 不是，1是 仅windows • IsRoot - uint64 - 是否必填：否 - 是否Root权限：0 不是，1是 仅linux • IsSudo - uint64 - 是否必填：否 - 是否Sudo权限：0 不是，1是 仅linux • IsSshLogin - uint64 - 是否必填：否 - 是否ssh登录：0 不是，1是 仅linux • ShellLoginStatus - uint64 - 是否必填：否 - 是否shell登录性，0不是；1是 仅linux • PasswordStatus - uint64 - 是否必填：否 - 密码状态：1正常 2即将过期 3已过期 4已锁定 仅linux • OsName -String 是否必填: 否 - 操作系统（DescribeMachineOsList 接口 值） 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 1
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 1
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： asc
Quuid	否	否	String	查询指定Quuid主机的信息 示例值： 1

3. 输出参数

参数名称	类型	描述
Total	Uint64	记录总数 示例值： 1
Users	Array of AssetUserBaseInfo	账号列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.DateRange	时间区间格式错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取资产管理Web应用列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取资产管理Web应用列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetWebAppList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序：[FirstTime
Filters	否	否	Array of Filter	过滤条件。 • IP - String - 是否必填：否 - 主机ip • MachineName - String - 是否必填：否 - 主机名称 • InstanceID - string - 是否必填：否 - 实例ID • Name - String - 是否必填：否 - 应用名 • Domain - String - 是否必填：否 - 站点域名 • Type - int - 是否必填：否 - 服务类型： 0：全部 1:Tomcat 2:Apache 3:Nginx 4:WebLogic 5:Websphere 6:JBoss 7:Jetty 8:IHS 9:Tengine

参数名称	必选	允许NULL	类型	描述
				• OsType - String - 是否必填：否 - windows/linux • OsName -String 是否必填: 否 - 操作系统 （DescribeMachineOsList 接口 值） 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： asc
Quuid	否	否	String	查询指定Quuid主机的信息 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
Total	Uint64	记录总数 示例值： 12
WebApps	Array of AssetWebAppBaseInfo	列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。

错误码	描述
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取资产管理Web应用插件列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取资产管理Web应用插件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetWebAppPluginList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	String	Web应用ID 示例值： 23210436
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 1
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 1
Quuid	是	否	String	主机Quuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	是	否	String	主机Uuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
Plugins	Array of AssetWebAppPluginInfo	列表 示例值：查看
Total	Uint64	分区总数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
ResourceNotFound	资源不存在。
InternalError	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取资产管理Web框架列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取资产管理Web框架列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetWebFrameList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序：[FirstTime
Filters	否	否	Array of Filter	过滤条件。 • IP - String - 是否必填：否 - 主机ip • MachineName - String - 是否必填：否 - 主机名称 • InstanceID - string - 是否必填：否 - 实例ID • Name - String - 是否必填：否 - 框架名 • NameStrict - String - 是否必填：否 - 框架名（严格匹配） • Lang - String - 是否必填：否 - 框架语言:java/python • Type - String - 是否必填：否 - 服务类型： 0：全部 1:Tomcat 2:Apache 3:Nginx 4:WebLogic 5:Websphere 6:JBoss 7:WildFly 8:Jetty

参数名称	必选	允许NULL	类型	描述
				9:IHS 10:Tengine • OsType - String - 是否必填：否 - windows/linux • OsName -String 是否必填: 否 - 操作系统 （DescribeMachineOsList 接口 值） 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： asc
Quuid	否	否	String	查询指定Quuid主机的信息 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
Total	Uint64	记录总数 示例值： 12
WebFrames	Array of AssetWebFrameBaseInfo	列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。

错误码	描述
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取Web站点详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取Web站点详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetWebLocationInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	String	站点Id 示例值： 1
Quuid	是	否	String	服务器Quuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	是	否	String	服务器Uuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
WebLocation	AssetWebLocationInfo	站点信息 示例值：查看

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	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取Web站点列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取Web站点列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetWebLocationList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序：[FirstTime
Filters	否	否	Array of Filter	过滤条件。 • IP - String - 是否必填：否 - 主机ip • MachineName - String - 是否必填：否 - 主机名称 • InstanceID - string - 是否必填：否 - 实例ID • Name - String - 是否必填：否 - 域名 • User - String - 是否必填：否 - 运行用户 • Port - uint64 - 是否必填：否 - 站点端口 • Proto - uint64 - 是否必填：否 - 站点协议：1:HTTP,2:HTTPS • ServiceType - uint64 - 是否必填：否 - 服务类型：1:Tomcat 2：Apache 3:Nginx 4:WebLogic 5:Websphere 6:JBoss 7:WildFly

参数名称	必选	允许NULL	类型	描述
				8:Jetty 9:IHS 10:Tengine • OsType - String - 是否必填：否 - windows/linux • OsName -String 是否必填: 否 - 操作系统 （DescribeMachineOsList 接口 值） 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 12
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： asc
Quuid	否	否	String	查询指定Quuid主机的信息 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

3. 输出参数

参数名称	类型	描述
Locations	Array of AssetWebLocationBaseInfo	站点列表 示例值：查看
Total	Uint64	记录总数 示例值： 12
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

错误码	描述
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询资产管理Web服务列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询资产管理Web服务列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetWebServiceInfoList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序：[FirstTime
Filters	否	否	Array of AssetFilters	过滤条件。 • IP - String - 是否必填：否 - 主机ip • MachineName - String - 是否必填：否 - 主机名称 • InstanceID - string - 是否必填：否 - 实例ID • User- string - 是否必填：否 - 运行用户 • Name- string - 是否必填：否 - Web服务名： 1:Tomcat 2:Apache 3:Nginx 4:WebLogic 5:Websphere 6:JBoss 7:WildFly 8:Jetty 9:IHS 10:Tengine

参数名称	必选	允许NULL	类型	描述
				• OsType- string - 是否必填：否 - Windows/linux • OsName -String 是否必填: 否 - 操作系统（DescribeMachineOsList 接口 值） 示例值：查看
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 • IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 示例值： 0
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： asc
Quuid	否	否	String	查询指定Quuid主机的信息 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
Total	Uint64	总数量 示例值： 1
WebServices	Array of AssetWebServiceBaseInfo	列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

错误码	描述
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取Web服务关联进程列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取Web服务关联进程列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetWebServiceProcessList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	String	Web服务ID 示例值： 12869
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Quuid	是	否	String	主机Quuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	是	否	String	主机Uuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684

3. 输出参数

参数名称	类型	描述
Process	Array of AssetAppProcessInfo	进程列表 示例值：查看
Total	Uint64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取用户添加的云厂商AK列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取用户添加的云厂商AK列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeCloudVendorAccountAKList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
CloudVendorAccountAKs	Array of CloudVendorAccountAK	AK列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取组件统计列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (DescribeComponentStatistics) 用于获取组件统计列表数据。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeComponentStatistics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 ComponentName - String - 是否必填：否 - 组件名称 示例值：查看
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
ComponentStatistics	Array of ComponentStatistics	组件统计列表数据数组。 示例值：查看
TotalCount	Uint64	组件统计列表记录总数。 示例值： 100
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

本接口 (DescribeComponents) 用于获取组件列表数据。

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取组件列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeComponents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
ComponentId	否	否	Uint64	组件ID。Uuid和ComponentId必填其一，使用ComponentId表示，查询该组件列表信息。 示例值： 1
Filters	否	否	Array of Filter	过滤条件。 • ComponentVersion - String - 是否必填：否 - 组件版本号 • MachineIp - String - 是否必填：否 - 主机内网IP 示例值：查看
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

参数名称	必选	允许NULL	类型	描述
Uuid	否	否	String	云镜客户端唯一Uuid。Uuid和ComponentId必填其一，使用Uuid表示，查询该主机列表信息。 示例值： 5a540076-d38a-4078-aa98-qwert371d322

3. 输出参数

参数名称	类型	描述
Components	Array of Component	组件列表数据。 示例值：查看
TotalCount	Uint64	组件列表记录总数。 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

导出区域主机列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (DescribeExportMachines) 用于导出区域主机列表。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:00:52。

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：DescribeExportMachines
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • Keywords - String - 是否必填：否 - 查询关键字 • Status - String - 是否必填：否 - 客户端在线状态（OFFLINE: 离线
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
MachineRegion	是	否	String	机器所属地域 示例值： ap-region1
MachineType	是	否	String	云主机类型。 • CVM：表示虚拟主机 • BM: 表示黑石物理机 示例值： CVM

参数名称	必选	允许NULL	类型	描述
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
ProjectIds	否	否	Array of Uint64	机器所属业务ID列表 示例值： [1002,1003]

3. 输出参数

参数名称	类型	描述
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 12
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameterValue	参数取值错误。

获取帐号变更历史列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (DescribeHistoryAccounts) 用于获取帐号变更历史列表数据。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeHistoryAccounts
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • Username - String - 是否必填：否 - 帐号名 示例值：查看
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Uuid	是	否	String	云镜客户端唯一Uuid。 示例值： 5a540076-d38a-4078-aa98-qwert371d322

3. 输出参数

参数名称	类型	描述
HistoryAccounts	Array of HistoryAccount	帐号变更历史数据数组。 示例值：查看
TotalCount	Uint64	帐号变更历史列表记录总数。 示例值： 100
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询批量导入机器信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询批量导入机器信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-16 12:16:37。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeImportMachineInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件： • Version - String 是否必填：否 - 当前防护版本（ PRO_VERSION：专业版
ImportType	是	否	String	批量导入的数据类型：Ip、Name、Id 三选一 示例值： Ip
IsQueryProMachine	否	否	Bool	该参数已作废. 示例值： true
MachineList	是	否	Array of String	服务器内网IP（默认）/ 服务器名称 / 服务器 ID 数组 (最大 1000条) 示例值： ["192.168.0.204"]

3. 输出参数

参数名称	类型	描述
EffectiveMachineInfoList	Array of EffectiveMachineInfo	有效的机器信息列表：机器名称、机器公网/内网ip、机器标签 示例值：查看
InvalidMachineList	Array of String	用户批量导入失败的机器列表（例如机器不存在等...） 示例值：[""a9fe0359-04d9-417f-ab6d-ayay""]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取机器详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口（DescribeMachineInfo）用于获取机器详细信息。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMachineInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Quuid	否	否	String	Quuid，Uuid 必填一项 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
Uuid	否	否	String	主机安全客户端唯一Uuid。 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0

3. 输出参数

参数名称	类型	描述
AgentVersion	String	agent版本号 示例值： 10
FreeMalwaresLeft	Uint64	免费木马剩余检测数量。 示例值： 1

参数名称	类型	描述
FreeVulsLeft	Uint64	免费漏洞剩余检测数量。 示例值： 1
HasAssetScan	Uint64	是否有资产扫描记录，0无，1有 示例值： 1
InstanceId	String	CVM或BM主机唯一标识。 示例值： CVM
IsProVersion	Bool	是否开通专业版。 • true：是 • false：否 示例值： false
MachineIp	String	机器ip。 示例值： 10.0.0.0
MachineName	String	主机名称。 示例值： redis_node_cvm
MachineOs	String	操作系统。 示例值： Windows Server 2022
MachineRegion	String	机器所属地域 示例值： ap-region1
MachineStatus	String	在线状态。 • ONLINE： 在线 • OFFLINE：离线 示例值： OFFLINE
MachineType	String	云服务器类型。 • CVM: 云服务器 • BM: 黑石物理机 • ECM: 边缘计算服务器 • LH: 轻量应用服务器 • Other: 混合云机器 示例值： CVM
MachineWanIp	String	主机外网IP。 示例值： 10.0.0.0

参数名称	类型	描述
PayMode	String	主机状态。 • POSTPAY: 表示后付费，即按量计费 • PREPAY: 表示预付费，即包年包月 示例值： PREPAY
ProVersionDeadline	String	专业版到期时间(仅预付费) 示例值： 2025-10-17 20:08:03
ProVersionOpenDate	String	专业版开通时间。 示例值： 2024-10-17 20:08:03
ProtectDays	Uint64	受主机安全保护天数。 示例值： 1
ProtectType	String	防护版本：BASIC_VERSION 基础版，PRO_VERSION 专业版，Flagship 旗舰版，GENERAL_DISCOUNT 普惠版 示例值： BASIC_VERSION
Quuid	String	CVM或BM主机唯一Uuid。 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
Uuid	String	主机安全客户端唯一Uuid。 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
ResourceNotFound	资源不存在。
InvalidParameterValue	参数取值错误。

查询机器操作系统列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询可筛选操作系统列表.

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeMachineOsList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息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	Array of OsName	操作系统列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

查询主机地域列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询机器地域列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMachineRegionList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
RegionList	Array of RegionListDetail	云服务器类型地域列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取机器地域列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取机器地域列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeMachineRegions
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
ALL	Array of RegionInfo	所有地域列表(包含以上所有地域) 示例值：查看
BM	Array of RegionInfo	BM 黑石机器地域列表 示例值：查看
CVM	Array of RegionInfo	CVM 云服务器地域列表 示例值：查看
ECM	Array of RegionInfo	ECM 边缘计算服务器地域列表 示例值：查看

参数名称	类型	描述
LH	Array of RegionInfo	LH 轻量应用服务器地域列表 示例值：查看
Other	Array of RegionInfo	Other 混合云地域列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameterValue	参数取值错误。

获取区域主机列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (DescribeMachines) 用于获取区域主机列表。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-10-18 17:27:47。

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：DescribeMachines
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • Ips - String - 是否必填：否 - 通过ip查询 • Names - String - 是否必填：否 - 通过实例名查询 • InstanceIds - String - 是否必填：否 - 通过实例id查询 • Status - String - 是否必填：否 - 客户端在线状态（OFFLINE: 离线/关机
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
MachineRegion	是	否	String	机器所属地域 示例值： ap-region1
MachineType	是	否	String	机器所属专区类型 CVM 云服务器 BM 黑石 ECM 边缘计算

参数名称	必选	允许NULL	类型	描述
				LH 轻量应用服务器 Other 混合云专区 示例值： CVM
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
ProjectIds	否	否	Array of Uint64	机器所属业务ID列表 示例值： [1]

3. 输出参数

参数名称	类型	描述
Machines	Array of Machine	主机列表 示例值：查看
TotalCount	Uint64	主机数量 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取端口统计列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (DescribeOpenPortStatistics) 用于获取端口统计列表。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeOpenPortStatistics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • Port - Uint64 - 是否必填：否 - 端口号 示例值：查看
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
OpenPortStatistics	Array of OpenPortStatistics	端口统计数据列表 示例值：查看
TotalCount	Uint64	端口统计列表总数 示例值： 100
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取进程统计列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

本接口 (DescribeProcessStatistics) 用于获取进程统计列表数据。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-07-28 23:46:05。

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：DescribeProcessStatistics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • ProcessName - String - 是否必填：否 - 进程名 示例值：查看
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
ProcessStatistics	Array of ProcessStatistics	进程统计列表数据数组。 示例值：查看
TotalCount	Uint64	进程统计列表记录总数。 示例值： 100
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameterValue	参数取值错误。

获取指定标签关联的服务器信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取指定标签关联的服务器信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeTagMachines
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	Uint64	标签ID 示例值： 1

3. 输出参数

参数名称	类型	描述
List	Array of TagMachine	列表数据 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

获取所有主机标签

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取所有主机标签

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-29 09:47:48。

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：DescribeTags
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 • AddedOnTheFifteen - String - 是否必填：否 - 是否最近15天的，存在任意值即为是 示例值：查看
MachineRegion	否	否	String	机器所属地域。 示例值： ap-region1
MachineType	否	否	String	云主机类型。 • CVM：表示云服务器 • BM：表示黑石物理机 • ECM：表示边缘计算服务器 • LH：表示轻量应用服务器 • Other：表示混合云服务器 示例值： CVM

3. 输出参数

参数名称	类型	描述
List	Array of Tag	列表信息 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

新增或编辑标签

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

新增或编辑标签

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：EditTags
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	否	否	Uint64	标签ID 示例值： 1
Name	是	否	String	标签名 示例值： tag-name
Quuids	否	否	Array of String	Quuid 示例值： ["dd90a245-ca7a-4268-9051-1fce4291ayay"]

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
MissingParameter	缺少参数错误。
LimitExceeded.AreaQuota	超出批量添加数量。
ResourceNotFound	资源不存在。
InvalidParameterValue.TagNameLengthLimit	标签名称长度不能超过15个字符。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

导出资产管理内核模块列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出资产管理内核模块列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportAssetCoreModuleList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序依据[FirstTime
Filters	否	否	Array of AssetFilters	过滤条件。 • IP - String - 是否必填：否 - 主机ip • MachineName - String - 是否必填：否 - 主机名称 • InstanceID - string - 是否必填：否 - 实例ID • Name- string - 是否必填：否 - 包名 示例值：查看
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： asc
Quuid	否	否	String	服务器Quuid 示例值： 1ce68339-8828-457f-b358-d5b1b34e4fe9

参数名称	必选	允许NULL	类型	描述
Uuid	否	否	String	服务器Uuid 示例值： 1ce68339-8828-457f-b358-d5b1b34e4fe9

3. 输出参数

参数名称	类型	描述
TaskId	String	异步下载任务ID，需要配合ExportTasks接口使用 示例值： 10001
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

导出资产管理Web服务列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出资产管理Web服务列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportAssetWebServiceInfoList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序：[FirstTime
Filters	否	否	Array of AssetFilters	过滤条件。 • IP - String - 是否必填：否 - 主机ip • MachineName - String - 是否必填：否 - 主机名称 • InstanceID - string - 是否必填：否 - 实例ID • User- string - 是否必填：否 - 运行用户 • Name- string - 是否必填：否 - Web服务名： 1:Tomcat 2:Apache 3:Nginx 4:WebLogic 5:Websphere 6:JBoss 7:WildFly 8:Jetty 9:IHS 10:Tengine

参数名称	必选	允许NULL	类型	描述
				• OsType- string - 是否必填：否 - Windows/linux • OsName -String 是否必填: 否 - 操作系统（DescribeMachineOsList 接口 值） 示例值：查看
Order	否	否	String	排序方式，asc升序 或 desc降序 示例值： asc
Quuid	否	否	String	查询指定Quuid主机的信息 示例值： 1

3. 输出参数

参数名称	类型	描述
TaskId	String	异步下载任务ID，需要配合ExportTasks接口使用 示例值： 10001
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameterValue	参数取值错误。

修改主机备注信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

修改主机备注信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-02-15 10:32:23。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyMachineRemark
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Quuid	是	否	String	主机Quuid 示例值： 5a540076-d38a-4078-aa98-e7c86371d322
Remark	否	否	String	备注信息 示例值： mark redis cvm

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

资产指纹启动扫描

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

资产指纹启动扫描

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ScanAsset
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
AssetTypeIds	否	否	Array of Uint64	资产指纹类型id列表 示例值： [102]
Quuids	否	否	Array of String	Quuid列表 示例值： ["5a540076-d38a-4078-aa98-q45rt371d322"]

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	任务id 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InternalError.MainDBFail	操作数据失败。
FailedOperation.NoProfessionHost	无专业版主机。
OperationDenied	操作被拒绝。
FailedOperation	操作失败。

同步资产扫描信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

同步资产扫描信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：SyncAssetScan
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Sync	是	否	Bool	是否同步：true-是 false-否；默认false 示例值： true

3. 输出参数

参数名称	类型	描述
LatestEndTime	String	最新结束同步时间 示例值： 2021-01-01 11:22:11
LatestStartTime	String	最新开始同步时间 示例值： 2021-01-01 11:22:11
State	String	枚举值有(大写)：NOTASK（没有同步任务），SYNCING（同步中），FINISHED（同步完成） 示例值： NOTASK

参数名称	类型	描述
TaskId	Uint64	任务ID 示例值： 88
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.MissingParameter	参数缺失。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InternalError.MainDBFail	操作数据失败。
FailedOperation.APIServerFail	调用API服务失败。
FailedOperation	操作失败。

关联机器标签列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

关联机器标签列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：UpdateMachineTags
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
MachineArea	是	否	String	服务器类型(CVM
MachineRegion	是	否	String	服务器地区 示例值： ap-region1
Quuid	是	否	String	机器 Quuid 示例值： 24c9be55-c743-4a75-a5c7-2a2936843684
TagIds	否	否	Array of Uint64	标签ID，该操作会覆盖原有的标签列表 示例值： [115]

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

高级防御相关接口
创建微告警负载标签

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

创建微告警负载标签

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：CreateMaWorkloadLabel
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
LabelIds	是	否	Array of Int64	标签ID列表 示例值： [1]
WorkloadIds	是	否	Array of Int64	负载ID列表 示例值： [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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

添加网站防护服务器

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

添加网站防护服务器

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：CreateProtectServer
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
ProtectDir	是	否	String	防护目录地址 示例值： /var/www
ProtectHostConfig	是	否	Array of ProtectHostConfig	防护机器 信息 示例值：查看

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

删除网络攻击日志

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除网络攻击日志

默认接口请求频率限制：20次/秒。

接口更新时间：2023-02-10 10:14:54。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteAttackLogs
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	否	否	Array of Uint64	日志ID数组，最大100条。 示例值： [1]
IsAll	否	否	Bool	是否全部删除 示例值： true

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
LimitExceeded.AreaQuota	超出批量添加数量。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

删除微告警访问事件

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除微告警访问事件

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DeleteMaConnEvent
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
DeleteIds	是	否	Array of Uint64	删除的事件ID集合 示例值： [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

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

删除微告警自定义白名单

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除微告警自定义白名单

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DeleteMaCustomPolicy
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
DeleteIds	是	否	Array of Uint64	删除的自定义白名单策略列表 示例值： [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

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

删除微告警标签

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除微告警标签

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DeleteMaLabel
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Int64	标签ID 示例值： [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

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

删除微告警自学习子策略

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除微告警自学习子策略

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DeleteMaSelfLearnPolicy
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
DeleteUniqueIds	是	否	Array of String	删除的自学习子子策略唯一ID集合 示例值： ["32454"]

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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

删除微告警全局白名单

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除微告警全局白名单

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DeleteMaWhitelist
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
DeleteIds	是	否	Array of Uint64	删除的全局过滤白名单配置ID集合 示例值： [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

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

删除防护网站

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

删除防护网站

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DeleteProtectDir
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of String	删除的目录ID 最大100条 示例值： ["/root/","/tmp"]

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

删除事件记录

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

网站防篡改-删除事件记录

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DeleteWebPageEventLog
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	需要删除的事件ID 集合 最大100条 示例值： [1,2,3,4]

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
InternalError	内部错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

网络攻击事件详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeAttackEventInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	Uint64	事件id 示例值： 49754647

3. 输出参数

参数名称	类型	描述
NetAttackEventInfo	NetAttackEventInfo	网络攻击事件详情 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

按分页形式展示网络攻击检测事件列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeAttackEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序 使用Count或MergeTime 示例值： MergeTime
Filters	否	否	Array of Filter	过滤条件。 • Type - String 攻击状态 0: 尝试攻击 1: 攻击成功 - 是否必填: 否 • Status - String 事件处理状态 0：待处理 1：已处理 2： 已加白 3： 已忽略 4：已删除 - 是否必填: 否 • SrcIP - String 来源IP - 是否必填: 否 • Uuids - String 主机安全uuid - 是否必填: 否 • Quuids - String cvm uuid - 是否必填: 否 • DstPort - String 攻击目标端口 - 是否必填: 否 • MachineName - String 主机名称 - 是否必填: 否 • InstanceID - String 主机实例ID - 是否必填: 否 • AttackTimeBegin - String 攻击开始时间 - 是否必填: 否 • AttackTimeEnd - String 攻击结束时间 - 是否必填: 否 • VulSupportDefense - String 漏洞是否支持防御 0不支持，1支持 - 是否必填: 否

参数名称	必选	允许NULL	类型	描述
				示例值：查看
Limit	否	否	Uint64	返回数量，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Order	否	否	String	排序方式 ASC,DESC 示例值： DESC

3. 输出参数

参数名称	类型	描述
List	Array of NetAttackEvent	攻击事件列表 示例值：查看
TotalCount	Uint64	总条数 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

网络攻击日志详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

网络攻击日志详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-10-31 15:59:56。

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：DescribeAttackLogInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	Uint64	日志ID 示例值： 1

3. 输出参数

参数名称	类型	描述
CreatedAt	String	攻击时间 示例值： 2020-12-12 10:10:00
DstIp	String	攻击目标IP 示例值： 192.168.0.1
DstPort	Uint64	攻击目标端口 示例值： 8080

参数名称	类型	描述
HttpCgi	String	攻击路径 示例值： any attack path
HttpContent	String	攻击内容 示例值： any content
HttpHead	String	攻击头信息 示例值： POST /was-wsdft/CoofatorPorasdtType ..
HttpHost	String	攻击目标主机 示例值： domain.com
HttpMethod	String	攻击方法 示例值： POST
HttpParam	String	攻击参数 示例值： anyp=anyv
HttpReferer	String	请求源 示例值： http://domian.com/any
HttpUserAgent	String	攻击者浏览器标识 示例值： ie
Id	Uint64	日志ID 示例值： 1
Quuid	String	主机ID 示例值： 1
SrcIp	String	攻击来源IP 示例值： 192.168.0.1
SrcPort	Uint64	攻击来源端口 示例值： 8080
VulType	String	威胁类型 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

网络攻击日志列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

按分页形式展示网络攻击日志列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeAttackLogs
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • HttpMethod - String - 是否必填：否 - 攻击方法(POST
Limit	否	否	Uint64	返回数量，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0
Quuid	否	否	String	云主机机器ID 示例值： quuid
Uuid	否	否	String	主机安全客户端ID 示例值： uuid

3. 输出参数

参数名称	类型	描述
AttackLogs	Array of DefendAttackLog	日志列表 示例值：查看
TotalCount	Uint64	总条数 示例值： 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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

网络攻击数据统计

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeAttackStatistics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AttackSrcIpCount	Uint64	总攻击来源ip数量 示例值： 0
AttackedAssetCount	Uint64	总受攻击资产数量 示例值： 0
AttackedPortCount	Uint64	总受攻击端口数量 示例值： 0
NewAttackSrcIpCount	Uint64	今日新增攻击来源ip数量 示例值： 0

参数名称	类型	描述
NewAttackedAssetCount	Uint64	今日新增受攻击资产数量 示例值： 0
NewAttackedPortCount	Uint64	今日新增受攻击端口数量 示例值： 0
PendingAttackCount	Uint64	总攻击次数 示例值： 0
PendingNewAttackCount	Uint64	今日新增攻击次数 示例值： 0
PendingSuccAttackCount	Uint64	总攻击成功次数 示例值： 0
PendingTryAttackCount	Uint64	总尝试攻击次数 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

网络攻击top5数据列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeAttackTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • BeginTime - String 起始时间,默认近7天- 是否必填: 否 示例值：查看

3. 输出参数

参数名称	类型	描述
NetAttackTopInfo	NetAttackTopInfo	top统计数据 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

网络攻击趋势数据

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeAttackTrends
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 • BeginTime - String 起始时间,默认近7天- 是否必填: 否 示例值：查看

3. 输出参数

参数名称	类型	描述
NetAttackTrend	Array of NetAttackTrend	攻击趋势统计数据（天） 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取网络攻击威胁类型列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取网络攻击威胁类型列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeAttackVulTypeList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息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	Array of String	威胁类型列表 示例值：["命令注入", "fastjson命令执行", "非正常的威胁类型"]
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
InternalError	内部错误。

获取微告警访问事件

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取微告警访问事件

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMaConnEventList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [CreateTime
Filters	否	否	Array of Filter	• Type - int64 - 是否必填：是 - 访问类型 • WorkloadName - string - 是否必填：否 - 负载名 • SrcWorkloadName - string - 是否必填：否 - 源负载名 • DestWorkloadName - string - 是否必填：否 - 目标负载名 • SrcIP - string - 是否必填：否 - 源IP • DestIP - string - 是否必填：否 - 目标IP • StartTime string - 是否必填：否 - 开始时间 • EndTime string - 是否必填：否 - 结束时间 • TimeMode int - 是否必填：是 - 时间选择[0:今日 1:本周 2:上周 3:上上周 4:近半年] 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10

参数名称	必选	允许NULL	类型	描述
Offset	否	否	Int64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
List	Array of MaConnEvent	访问事件集合 示例值：查看
TotalCount	Int64	总数 示例值： 100
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取微告警自定义白名单

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取微告警自定义白名单

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMaCustomPolicyList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [CreateTime
Filters	否	否	Array of Filter	• SrcLabelId - string - 是否必填：否 - 源标签id • SrcLabelKey - string - 是否必填：否 - 源标签key • SrcLabelValue - string - 是否必填：否 - 源标签value • DestLabelId - string - 是否必填：否 - 目标标签id • DestLabelKey - string - 是否必填：否 - 目标标签key • DestLabelValue - string - 是否必填：否 - 目标标签value • SrcIP - string - 是否必填：否 - 源IP • DestIP - string - 是否必填：否 - 目标IP • Enable - int64 - 是否必填：否 - 是否开启 • Updater- string - 是否必填：否 - 创建人/更新人 • Name - string - 是否必填：否 - 自定义白名单名称 示例值：查看

参数名称	必选	允许NULL	类型	描述
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
List	Array of MaCustomPolicy	自定义白名单策略集 示例值：查看
TotalCount	Int64	总数 示例值： 100
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取微告警全局配置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取微告警全局配置

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMaGlobalConf
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息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	MaGlobalConf	全局配置 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取微告警主机列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取微告警主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMaHostList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [CreateTime] 示例值： CreateTime
Filters	否	否	Array of Filter	• Name - string - 是否必填：否 - 主机名称 • Id - string - 是否必填：否 - 主机ID • InstanceId - string - 是否必填：否 - 实例ID • Ip - string - 是否必填：否 - IP地址 • OsType - string - 是否必填：否 - 操作系统 • VpcId - string - 是否必填：否 - 所属网络 • Region - string - 是否必填：否 - 地域 • Label - string - 是否必填：否 - 关联标签 • IsEnable - string - 是否必填：否 - 监控状态 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10

参数名称	必选	允许NULL	类型	描述
Offset	否	否	Int64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
List	Array of MaHost	主机列表 示例值：查看
TotalCount	Int64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取微告警标签信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取微告警标签信息

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMaLabel
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	Int64	标签ID 示例值： 1

3. 输出参数

参数名称	类型	描述
Label	MaLabel	标签信息 示例值：查看
WorkloadIds	Array of Int64	标签关连负载ID列表 示例值： [1]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取微告警标签列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取微告警标签列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMaLabelList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	• Source - string - 是否必填：否 - 标签来源 • Id - string - 是否必填：否 - 标签ID • Label - string - 是否必填：否 - 标签KEY或VALUE 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
List	Array of MaLabel	标签列表 示例值：查看
TotalCount	Int64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取微告警标签来源列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取微告警标签来源列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMaLabelSourceList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息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	Array of String	标签来源列表 示例值： ["any-source"]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取微告警POD列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取微告警POD列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMaPodList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [CreateTime] 示例值： CreateTime
Filters	否	否	Array of Filters	• Name - string - 是否必填：否 - POD名称 • Id - string - 是否必填：否 - POD ID • Ip - string - 是否必填：否 - IP地址 • Status - string - 是否必填：否 - POD状态 • ClusterId - string - 是否必填：否 - 集群ID • ClusterName - string - 是否必填：否 - 集群名称 • Label - string - 是否必填：否 - 关联标签 • IsEnabled - string - 是否必填：否 - 监控状态 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0

参数名称	必选	允许NULL	类型	描述
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
List	Array of MaPod	Pod列表 示例值：查看
TotalCount	Int64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取微告警自学习策略

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取微告警自学习策略

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMaSelfLearnConfig
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息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	Uint64	是否开启自学习 • 0 : 未开启 • 1 : 开启 示例值： 1
HostCount	Uint64	开启学习的主机负载数 示例值： 1
LearnConfID	Uint64	自学习配置ID 示例值： 1

参数名称	类型	描述
LearnEndDate	String	学习结束时间 示例值： 2023-10-11
LearnStartDate	String	学习开始时间 示例值： 2023-10-10
PodCount	Uint64	开启学习的POD负载数 示例值： 1
RemainingDay	Float	学习剩余天数 示例值： 1.0
Status	Uint64	自学习状态 • 0： 学习中 • 1：学习完成 示例值： 1
SubPolicyCount	Uint64	自学习的子策略数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取微告警自学习子策略列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取微告警自学习子策略列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMaSelfLearnPolicyList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [CreateTime
Filters	否	否	Array of Filter	• SrcLabelId - string - 是否必填：否 - 源标签id • SrcLabelKey - string - 是否必填：否 - 源标签key • SrcLabelValue - string - 是否必填：否 - 源标签value • DestLabelId - string - 是否必填：否 - 目标标签id • DestLabelKey - string - 是否必填：否 - 目标标签key • DestLabelValue - string - 是否必填：否 - 目标标签value • SrcIP - string - 是否必填：否 - 源IP • DestIP - string - 是否必填：否 - 目标IP • UniqueId - string - 是否必填：否 - 自学习子策略唯一ID 示例值：查看

参数名称	必选	允许NULL	类型	描述
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
List	Array of MaSelfLearnPolicy	自学习子策略集 示例值：查看
TotalCount	Int64	总数 示例值： 100
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取微告警整体概要

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取微告警整体概要

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMaSummary
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
CustomPolicyCount	Uint64	自定义白名单策略个数，废弃 示例值： 1
EnableCustomPolicyCount	Uint64	开启自定义白名单策略总数 示例值： 0
EnableHostWorkloadCount	Uint64	开启监控的主机工作负载个数 示例值： 1
EnablePodWorkloadCount	Uint64	开启监控的pod工作负载个数 示例值： 1

参数名称	类型	描述
EnableWorkloadCount	Uint64	开启监控的工作负载个数 示例值： 1
GlobalWhitelistEnable	Uint64	全局过滤白名单是否开启 • 0 关闭 • 1 开启 示例值： 1
HostWorkloadCount	Uint64	主机工作负载数 示例值： 1
MonitorEnable	Uint64	访问监控开关是否开启 • 0 关闭 • 1 开启 示例值： 1
PodWorkloadCount	Uint64	Pod工作负载数 示例值： 1
SelfLearnEnable	Uint64	自学习是否开启 • 0 关闭 • 1 开启 示例值： 1
TodayNewAlarmEventCount	Uint64	今日新增告警事件数 示例值： 0
TotalCustomPolicyCount	Uint64	开启和关闭的自定义白名单策略总数 示例值： 1
WhitelistCount	Uint64	全局过滤白名单个数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取微告警全局白名单设置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取微告警全局白名单

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMaWhitelist
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [CreateTime
Filters	否	否	Array of Filter	• From - string - 是否必填：否 - 白名单来源 • Enable - int64 - 是否必填：否 - 是否开启 • Updater - string - 是否必填：否 - 创建人 • Name - string - 是否必填：否 - 白名单名称 示例值：查看
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
Enable	Int64	是否整体开启 • 0：未开启 • 1：开启 示例值： 1
List	Array of MaWhitelist	全局过滤白名单配置集 示例值：查看
TotalCount	Int64	总数 示例值： 100
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取微告警负载标签

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取微告警负载标签

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMaWorkloadLabel
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	Int64	负载ID 示例值： 1

3. 输出参数

参数名称	类型	描述
List	Array of MaLabel	标签列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

获取微告警负载列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

获取微告警负载列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeMaWorkloadList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	• Name - string - 是否必填：否 - 负载名称 • Type - string - 是否必填：否 - 负载类型[0:主机
Limit	否	否	Int64	限制条数,默认10,最大100 示例值： 10
Offset	否	否	Int64	偏移量,默认0 示例值： 0

3. 输出参数

参数名称	类型	描述
List	Array of MaWorkload	列表 示例值：查看

参数名称	类型	描述
TotalCount	Int64	总数 示例值： 10
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

网页防篡改获取区域主机列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

用于网页防篡改获取区域主机列表。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeMachineList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of AssetFilters	过滤条件。 • Keywords - String - 是否必填：否 - 查询关键字 • Status - String - 是否必填：否 - 客户端在线状态（OFFLINE: 离线
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
MachineRegion	是	否	String	机器所属地域 示例值： ap-region1
MachineType	是	否	String	云主机类型。 • CVM：表示虚拟主机 • BM：表示黑石物理机 • ECM：表示边缘计算服务器 • LH：表示轻量应用服务器

参数名称	必选	允许NULL	类型	描述
				• Other：表示混合云机器 示例值： CVM
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

3. 输出参数

参数名称	类型	描述
Machines	Array of Machine	主机列表 示例值：查看
TotalCount	Uint64	主机数量 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
FailedOperation.APIServerFail	调用API服务失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询网络攻击设置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DescribeNetAttackSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
MemberId	否	否	Array of String	集团账号的成员id 示例值： [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]

3. 输出参数

参数名称	类型	描述
AutoInclude	Uint64	新增资产自动包含 0 不包含 1包含 示例值： 1
ExcludeInstanceIds	Array of String	自选排除主机 示例值： ["d92d7"]
InstanceIds	Array of String	自选主机 示例值： ["ins-d92d72"]

参数名称	类型	描述
NetAttackAlarmStatus	Uint64	0 新增告警事件默认待处理，1新增告警事件默认已处理，3新增告警事件默认忽略 示例值： 1
NetAttackEnable	Uint64	0 关闭网络攻击检测，1开启网络攻击检测 示例值： 1
Scope	Uint64	1 全部旗舰版主机，0 InstanceIds列表主机 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

防护目录列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

网页防篡改防护目录列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeProtectDirList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序字 段 ProtectServerNum, NoProtectServerNum, LatestProtectTime, RelatedServerNum 示例值： ProtectServerNum
Filters	否	否	Array of AssetFilters	DirName 网站名称 DirPath 网站防护目录地址 示例值：查看
Limit	是	否	Uint64	分页条数 最大100条 示例值： 10
Offset	是	否	Uint64	偏移量 示例值： 1
Order	否	否	String	asc：升序/desc：降序 示例值： asc

3. 输出参数

参数名称	类型	描述
List	Array of ProtectDirInfo	防护目录列表信息 示例值：查看
TotalCount	Uint64	总数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询防护目录关联服务器

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询防护目录关联服务器列表信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeProtectDirRelatedServer
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序值 示例值： LatestProtectTime
Filters	否	否	Array of Filter	过滤参数 ProtectStatus 示例值：查看
Id	是	否	String	唯一ID 示例值： 1
Limit	是	否	Uint64	分页条数 最大100条 示例值： 10
Offset	是	否	Uint64	偏移量 示例值： 0
Order	否	否	String	排序方式 示例值： asc

3. 输出参数

参数名称	类型	描述
List	Array of ProtectDirRelatedServer	网站关联服务器列表信息 示例值：查看
ProtectServerCount	Uint64	已开启防护总数 示例值： 12
TotalCount	Uint64	总数 示例值： 12
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询服务器关联目录详情

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询服务区关联目录详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeServerRelatedDirInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	Uint64	唯一ID 示例值： 1

3. 输出参数

参数名称	类型	描述
HostIp	String	服务器IP 示例值： 10.0.0.1
HostName	String	服务器名称 示例值： redis_node_cvm
ProtectDirNum	Uint64	防护目录数量 示例值： 1

参数名称	类型	描述
ProtectFileNum	Uint64	防护文件数量 示例值： 1
ProtectLinkNum	Uint64	防护软链数量 示例值： 1
ProtectTamperNum	Uint64	防篡改数量 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询篡改事件列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询篡改事件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeWebPageEventList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序方式：CreateTime 或 RestoreTime，默认为 CreateTime 示例值： CreateTime
Filters	否	否	Array of AssetFilters	过滤条件 • IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 • EventType - String - 是否必填：否 - 事件类型 • EventStatus - String - 是否必填：否 - 事件状态 示例值：查看
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。 示例值： 10
Offset	否	否	Uint64	偏移量，默认为0。 示例值： 0

参数名称	必选	允许NULL	类型	描述
Order	否	否	Uint64	排序方式，0降序，1升序，默认为0 示例值： 0

3. 输出参数

参数名称	类型	描述
List	Array of ProtectEventLists	防护事件列表信息 示例值：查看
TotalCount	Uint64	总数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

查询网页防篡改概览信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

查询网站防篡改概览信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：DescribeWebPageGeneralize
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
ProtectDirNum	Uint64	防护目录数 示例值： 1
ProtectFileNum	Uint64	防护文件数 示例值： 1
ProtectHostNum	Uint64	防护主机数 示例值： 1
ProtectMonitor	Uint64	防护监测 0 未开启 1 已开启 2 异常 示例值： 1

参数名称	类型	描述
ProtectToday	Uint64	今日防护数 示例值： 1
TamperFileNum	Uint64	篡改文件数 示例值： 1
TamperNum	Uint64	篡改数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

查询网页防篡改防护统计

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

网站防篡改-查询动态防护信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeWebPageProtectStat
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
FileTamperNum	Array of ProtectStat	文件篡改信息 示例值：查看
ProtectFileType	Array of ProtectStat	防护文件分类信息 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

查询网站防篡改服务信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

网站防篡改-查询网页防篡改服务器购买信息及服务器信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：DescribeWebPageServiceInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AllAuthorizedMachines	Array of ProtectMachineInfo	所有授权机器信息 示例值：查看
BuyNum	Uint64	已购授权数 示例值： 1
ExpireAuthorizedMachines	Array of ProtectMachine	临近到期授权机器信息 示例值：查看
ExpireNum	Uint64	临近到期数量 示例值： 1

参数名称	类型	描述
ExpiredNum	Uint64	已过期授权数 示例值： 1
ProtectDirNum	Uint64	防护目录数 示例值： 1
ResidueNum	Uint64	剩余授权数 示例值： 1
Status	Bool	是否已购服务：true-是，false-否 示例值： true
UsedNum	Uint64	已使用授权数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

关闭微告警自学习

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

关闭微告警自学习

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：DisableSelfLearn
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
CloseMonitor	是	否	Uint64	是否同步关闭监控开关 • 0 不关闭 • 1 关闭 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

导出网络攻击事件

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ExportAttackEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序值 CreateTime 示例值： CreateTime
Filters	否	否	Array of Filters	过滤条件。 • Type - String 攻击状态 0: 尝试攻击 1: 攻击成功 - 是否必填: 否 • Status - String 事件处理状态 0：待处理 1：已处理 2： 已加白 3： 已忽略 4：已删除 - 是否必填: 否 • SrcIP - String 来源IP - 是否必填: 否 • Uuids - String 主机安全uuid - 是否必填: 否 • Quuids - String cvm uuid - 是否必填: 否 • DstPort - String 攻击目标端口 - 是否必填: 否 • MachineName - String 主机名称 - 是否必填: 否 • InstanceID - String 主机实例ID - 是否必填: 否 • AttackTimeBegin - String 攻击开始时间 - 是否必填: 否 • AttackTimeEnd - String 攻击结束时间 - 是否必填: 否 • VulSupportDefense - String 漏洞是否支持防御 0不支持，1支持 - 是否必填: 否

参数名称	必选	允许NULL	类型	描述
				示例值：查看
Order	否	否	String	排序 方式 ，ASC，DESC 示例值： ASC

3. 输出参数

参数名称	类型	描述
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

导出网络攻击日志

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出网络攻击日志

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:34。

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：ExportAttackLogs
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 • HttpMethod - String - 是否必填：否 - 攻击方法 (POST
Quuid	否	否	String	云主机机器ID 示例值： 5a540076-d38a-4078-aa98-qwert371d322
Uuid	否	否	String	主机安全客户端ID 示例值： 5a540076-d38a-4078-aa98-qwert371d322

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
DownloadUrl	String	已废弃 示例值： http://domain.com/anypath/x
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 101
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
FailedOperation.Export	导出文件失败。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

导出微告警访问事件

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出微告警访问事件

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ExportMaConnEventList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [CreateTime
Filters	否	否	Array of Filter	• Type - int64 - 是否必填：是 - 访问类型 • WorkloadName - string - 是否必填：否 - 负载名 • SrcWorkloadName - string - 是否必填：否 - 源负载名 • DestWorkloadName - string - 是否必填：否 - 目标负载名 • SrcIP - string - 是否必填：否 - 源IP • DestIP - string - 是否必填：否 - 目标IP • StartTime string - 是否必填：否 - 开始时间 • EndTime string - 是否必填：否 - 结束时间 • TimeMode int - 是否必填：是 - 时间选择[0:今日 1:本周 2:上周 3:上上周 4:近半年] 示例值：查看
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 101
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

导出微告警自定义白名单

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出微告警自定义白名单

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ExportMaCustomPolicyList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [CreateTime
Filters	否	否	Array of Filter	• SrcLabelId - string - 是否必填：否 - 源标签id • SrcLabelKey - string - 是否必填：否 - 源标签key • SrcLabelValue - string - 是否必填：否 - 源标签value • DestLabelId - string - 是否必填：否 - 目标标签id • DestLabelKey - string - 是否必填：否 - 目标标签key • DestLabelValue - string - 是否必填：否 - 目标标签value • SrcIP - string - 是否必填：否 - 源IP • DestIP - string - 是否必填：否 - 目标IP • Enable - int64 - 是否必填：否 - 是否开启 • Updater- string - 是否必填：否 - 创建人/更新人 • Name - string - 是否必填：否 - 自定义白名单名称 示例值：查看
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 101
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

导出微告警主机列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出微告警主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ExportMaHostList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	• Name - string - 是否必填：否 - 主机名称 • Id - string - 是否必填：否 - 主机ID • InstanceId - string - 是否必填：否 - 实例ID • Ip - string - 是否必填：否 - IP地址 • OsType - string - 是否必填：否 - 操作系统 • VpcId - string - 是否必填：否 - 所属网络 • Region - string - 是否必填：否 - 地域 • Label - string - 是否必填：否 - 关联标签 • IsEnable - string - 是否必填：否 - 监控状态 示例值：查看

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
TaskId	Int64	导出任务ID 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

导出微告警POD列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出微告警POD列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ExportMaPodList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Filters	否	否	Array of Filter	• Name - string - 是否必填：否 - POD名称 • Id - string - 是否必填：否 - POD ID • Ip - string - 是否必填：否 - IP地址 • Status - string - 是否必填：否 - POD状态 • ClusterId - string - 是否必填：否 - 集群ID • ClusterName - string - 是否必填：否 - 集群名称 • Label - string - 是否必填：否 - 关联标签 • IsEnabled - string - 是否必填：否 - 监控状态 示例值：查看

3. 输出参数

参数名称	类型	描述
TaskId	Int64	导出任务ID

参数名称	类型	描述
		示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

导出微告警自学习子策略

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出微告警自学习子策略

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ExportMaSelfLearnPolicyList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [CreateTime
Filters	否	否	Array of Filter	• SrcLabelId - string - 是否必填：否 - 源标签id • SrcLabelKey - string - 是否必填：否 - 源标签key • SrcLabelValue - string - 是否必填：否 - 源标签value • DestLabelId - string - 是否必填：否 - 目标标签id • DestLabelKey - string - 是否必填：否 - 目标标签key • DestLabelValue - string - 是否必填：否 - 目标标签value • SrcIP - string - 是否必填：否 - 源IP • DestIP - string - 是否必填：否 - 目标IP • UniqueId - string - 是否必填：否 - 自学习子策略唯一ID 示例值：查看
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 101
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

导出微告警全局白名单

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出微告警全局白名单

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ExportMaWhitelist
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	可选排序列: [CreateTime
Filters	否	否	Array of Filter	• From - string - 是否必填：否 - 白名单来源 • Enable - int64 - 是否必填：否 - 是否开启 • Updater - string - 是否必填：否 - 创建人 • Name - string - 是否必填：否 - 白名单名称 示例值：查看
Order	否	否	String	排序方式: [ASC:升序

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 101
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

导出防护目录列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出网页防篡改防护目录列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：ExportProtectDirList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序字 段 ProtectServerNum, NoProtectServerNum, LatestProtectTime, RelatedServerNum 示例值： ProtectServerNum
Filters	否	否	Array of AssetFilters	DirName 网站名称 DirPath 网站防护目录地址 示例值：查看
Order	否	否	String	asc：升序/desc：降序 示例值： asc

3. 输出参数

参数名称	类型	描述
TaskId	String	任务ID,需要到接口“异步导出任务”ExportTasks获取DownloadUrl下载地址 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

错误码	描述
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

导出篡改事件列表

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

导出篡改事件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：ExportWebPageEventList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
By	否	否	String	排序方式：CreateTime 或 RestoreTime，默认为 CreateTime 示例值： CreateTime
Filters	否	否	Array of AssetFilters	过滤条件 • IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 • EventType - String - 是否必填：否 - 事件类型 • EventStatus - String - 是否必填：否 - 事件状态 示例值：查看
Order	否	否	Uint64	排序方式，0降序，1升序，默认为0 示例值： 0

3. 输出参数

参数名称	类型	描述
TaskId	String	任务id 可通过 ExportTasks接口下载 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter.MissingParameter	参数缺失。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。

更改微告警访问事件类型，可实现取消加白

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

更改微告警访问事件类型

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyMaConnEventType
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
ModifyEventIds	是	否	Array of Uint64	更改的事件ID 示例值： [1]
Type	是	否	Uint64	事件类型 • 0 正常 • 1 异常 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

创建或者更改微告警自定义白名单

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

创建或者更改微告警自定义白名单

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyMaCustomPolicy
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Policy	是	否	MaCustomPolicy	自定义白名单策略 示例值：查看

3. 输出参数

参数名称	类型	描述
Id	Uint64	创建的自定义白名ID 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

更微告警自定义白名单状态

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

更微告警自定义白名单状态

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyMaCustomPolicyStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of Uint64	自定义白名单策略ID集 示例值： [1]
Status	是	否	Uint64	自定义白名单状态 • 0 关闭 • 1 开启 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

修改微告警全局配置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

修改微告警全局配置

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyMaGlobalConf
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Data	是	否	MaGlobalConf	全局监控配置 示例值：查看

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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

新增或更改标签信息

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

新增或更改标签信息

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyMaLabel
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Label	是	否	MaLabel	标签信息 示例值：查看
WorkloadIds	否	否	Array of Int64	标签关联负载ID列表 示例值： [1]
WorkloadScope	否	否	Int64	负载范围[0:全部

3. 输出参数

参数名称	类型	描述
Id	Int64	标签ID 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

配置自学习策略

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

配置自学习策略

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyMaSelfLearnConfig
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
LearnEndDate	是	否	String	学习结束时间 示例值： 2023-10-11
LearnStartDate	是	否	String	学习开始时间 示例值： 2023-10-10

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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

更改微告警全局白名单设置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

更改微告警全局白名单

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyMaWhitelist
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Whitelist	是	否	MaWhitelist	白名单配置 示例值：查看

3. 输出参数

参数名称	类型	描述
Id	Uint64	新建白名单的Id 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

更改微告警全局白名单状态

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

更改微告警全局白名单状态

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyMaWhitelistStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
All	是	否	Uint64	是否全部 • 0 部分 • 1 全部 示例值： 0
Ids	否	否	Array of Uint64	不是全部时，选择的全局过滤白名单配置ID集合。全部时候只操作最外层开关 示例值： [1]
Status	是	否	Uint64	状态 • 0 关闭 • 1 开启 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

更改微告警负载标签

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

更改微告警负载标签

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyMaWorkloadLabel
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
LabelIds	是	否	Array of Int64	标签列表 示例值： [1]
WorkloadId	是	否	Int64	负载ID 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

更改微告警负载监控

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

更改微告警负载监控

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyMaWorkloadMonitor
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
EndTime	否	否	Datetime_iso	自学习结束日期 示例值： 2023-12-10 23:59:59
Ids	是	否	Array of Int64	负载ID列表 示例值： [1]
IsEnabled	是	否	Int64	监控是否开启[1:开启
StartTime	否	否	Datetime_iso	自学习开始日期 示例值： 2023-10-10 00:00:00

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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

编辑或者创建java内存马白名单

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

编辑或者创建java内存马白名单规则

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyMemShellRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
AnnotationsRegexp	否	否	String	注释正则表达式，为空则不匹配 base64编码 示例值： cmVkaXMuY2Zn
ClassNameRegexp	否	否	String	类名正则表达式，为空则不匹配 base64编码 示例值： LW5vcmcuYXBhY2hlLmNhdGFsaW5hLnN0YXJ0dXAuQm9vdHN0cmFwCg==
GroupID	否	否	String	批次id 示例值： 85c909fe-c87c-11e9-a100-5cb90191ae78
GroupName	否	否	String	策略名称 示例值： groupname
HandleHistory	否	否	Uint64	处理历史事件， 0:不处理 1:处理 示例值： 1
Id	否	否	Uint64	规则自增ID(新增时请留空) 示例值： 1302396215
InterfacesRegexp	否	否	String	继承的接口正则表达式，为空则不匹配，base64编码 示例值： LW5vcmcuYXBhY2hlLmNhdGFsaW5hLnN0YXJ0dXAuQm9vdHN0cmFwCg==
IsGlobal	否	否	Uint64	是否全局规则(是否对appid下所有主机有效， 0:单台uuid 1:全局，默认否) 示例值： 1
LoaderClassNameRegexp	否	否	String	所属的类加载器正则表达式，为空则不匹配，base64编码 示例值： LW5vcmcuYXBhY2hlLmNhdGFsaW5hLnN0YXJ0dXAuQm9vdHN0cmFwCg
LogicalSymbol	否	否	Uint64	逻辑运算符，0: 下面5个有效的正则逻辑与 1: 逻辑或 示例值： 0
MemshellListID	否	否	Uint64	事件列表和详情点击加白时关联的事件id (新增规则时请留空) 示例值： 12

参数名称	必选	允许NULL	类型	描述
SuperClassNameRegexp	否	否	String	父类名正则表达式，为空则不匹配，base64编码 示例值： LW5vcmcuYXBhY2hlLmNhdGFsaW5hLnN0YXJ0dXAuQm9vdHN0cmFwCg
Uuids	否	否	Array of String	客户端ID数组 示例值：["0039803a-ca13-40cc-8b39-bd3b103765ec"]

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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

修改网络攻击设置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

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：ModifyNetAttackSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
AutoInclude	否	否	Uint64	新增资产自动包含 0 不包含 1包含 示例值： 1
ExcludeInstanceIds	否	否	Array of String	自选排除的主机 示例值： ["inst-d92d"]
InstanceIds	否	否	Array of String	自选主机 示例值： ["inst-d92d"]
MemberId	否	否	Array of String	集团账号的成员id 示例值：[{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
NetAttackAlarmStatus	是	否	Uint64	0 新增告警事件默认待处理，1新增告警事件默认已处理，3新增告警事件默认忽略 示例值： 1

参数名称	必选	允许NULL	类型	描述
NetAttackEnable	是	否	Uint64	0 关闭网络攻击检测，1开启网络攻击检测 示例值： 1
Scope	否	否	Uint64	1 全部旗舰版主机，0 Quuids列表主机 示例值： 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
InternalError	内部错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。

创建网站防护目录

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

创建/修改网站防护目录

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

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：ModifyWebPageProtectDir
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
HostConfig	是	否	Array of ProtectHostConfig	防护机器列表信息 示例值：查看
ProtectDirAddr	是	否	String	网站防护目录地址 示例值： /var/www
ProtectDirName	是	否	String	网站防护目录名称 示例值： www防护
ProtectFileType	是	否	String	防护文件类型,分号分割； 示例值： .html;.php

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.MissingParameter	参数缺失。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter.IllegalRequest	非法请求。
FailedOperation.AgentOffline	客户端已离线。
FailedOperation.APIServerFail	调用API服务失败。
FailedOperation.LicenseExceeded	可用license数量不足，缺少1个license，请购买新license。
InvalidParameter	参数错误。
OperationDenied	操作被拒绝。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。
FailedOperation.ProtectStartFail	开启防护失败。

修改网站防护设置

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

修改网站防护设置

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：ModifyWebPageProtectSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Id	是	否	String	配置对应的protect_path 示例值： var
ModifyType	是	否	Uint64	需要操作的类型1 目录名称 2 防护文件类型 示例值： 1
Value	是	否	String	提交值 示例值： redis_node_protect

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
InternalError	内部错误。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
FailedOperation	操作失败。

网站防护设置开关

1. 接口描述

接口请求域名： cwp.api3.finance.cloud.tencent.com。

网站防篡改防护设置开关

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

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：ModifyWebPageProtectSwitch
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Ids	是	否	Array of String	需要操作开关的网站 最大100条 示例值： ["101"]
Status	否	否	Uint64	1 开启 0 关闭 SwitchType 为 1
SwitchType	是	否	Uint64	开关类型 1 防护开关 2 自动恢复开关 3 移除防护目录 示例值： 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
InternalError	内部错误。
InvalidParameter.InvalidFormat	参数格式错误。
MissingParameter	缺少参数错误。
ResourceNotFound	资源不存在。
FailedOperation.AgentOffline	客户端已离线。
FailedOperation.APIServerFail	调用API服务失败。
FailedOperation.LicenseExceeded	可用license数量不足，缺少1个license，请购买新license。
InvalidParameter	参数错误。
LimitExceeded	超过配额限制。
OperationDenied	操作被拒绝。
FailedOperation	操作失败。

数据结构

ProtectStat

防护信息统计

被如下接口引用：DescribeWebPageProtectStat

名称	必选	允许NULL	类型	描述
Name	是	否	String	名称 示例值： /tmp
Num	是	否	Uint64	数量 示例值： 56

ScanTaskDetails

扫描任务详情列表信息

被如下接口引用：DescribeScanTaskDetails

名称	必选	允许NULL	类型	描述
Description	否	否	String	描述信息 示例值： 失败
FailType	否	否	Uint64	失败类型 3离线、4超时、5失败、8agent版本过低 示例值： 4
HostIp	否	否	String	服务器IP 示例值： 10.0.0.1
HostName	否	否	String	服务器名称 示例值： any-agent
Id	否	否	Uint64	id唯一 示例值： 1
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineWanIp	否	否	String	外网ip 示例值： 172.22.11.12
OsName	否	否	String	操作系统 示例值： win64
Quuid	否	否	String	唯一Quuid 示例值： badea25d-d702-4f68-8906-0580c0a13170
RiskNum	否	否	Uint64	风险数量 示例值： 1
ScanBeginTime	否	否	String	扫描开始时间 示例值： 2024-10-29 10:35:50
ScanEndTime	否	否	String	扫描结束时间 示例值： 2024-10-29 10:39:50
Status	否	否	String	状态码Scanning、Ok、Fail 示例值： Fail
Uuid	否	否	String	唯一Uuid 示例值： badea25d-d702-4f68-8906-0580c0a13170

RansomDefenseStrategyDetail

主机列表查询接口相应数据HostList的TagList节点

被如下接口引用：DescribeRansomDefenseStrategyDetail

名称	必选	允许NULL	类型	描述
BackupType	是	是	Uint64	备份模式： 0按周，1按天 示例值： 0
CreateTime	是	是	String	创建时间 示例值： 2022-12-12 12:12:12
Description	是	是	String	策略备注 示例值： subtitle
EventCount	是	是	Uint64	策略关联事件数 示例值： 11
ExcludeDir	是	是	String	包含目录，用;分隔 示例值： /usr
Hour	是	否	String	备份执行时间点(0-23): 11:00;12:00 示例值： 11:00
Id	是	否	Int64	策略id 示例值： 666
IncludeDir	是	是	String	包含目录，用;分隔 示例值： /root
IsAll	是	否	Uint64	是否对所有主机生效 示例值： 1
MachineCount	是	是	Uint64	绑定机器数 示例值： 12
ModifyTime	是	是	String	最近修改时间 示例值： 2022-12-12 12:12:12
Name	是	否	String	策略名称 示例值： policy-1
SaveDay	是	否	Uint64	保存天数，0永久保存 示例值： 5
Status	是	否	Uint64	开启状态：0关闭，1开启 示例值： 1
Uin	是	是	String	操作uin 示例值： 666
Weekday	是	是	String	备份星期天数（1-7）：1;2;3;4 示例值： 1;2;3

OrderModifyObject

订单变配参数对象

被如下接口引用：CreateLicenseOrder

名称	必选	允许NULL	类型	描述
InquireNum	否	否	Int64	扩容/缩容数,变配子产品忽略该参数 示例值： 1242
NewSubProductCode	否	否	String	新产品标识,这里支持PRO_VERSION 专业版,FLAGSHIP 旗舰版 示例值： PRO_VERSION
ResourceId	否	否	String	资源ID 示例值： 'cakf-4mrnxayayay'

VulDefenceSetting

漏洞防御设置

被如下接口引用：DescribeVulDefenceSettingList

名称	必选	允许NULL	类型	描述
AppId	否	是	Uint64	用户appid 示例值： 1255080011
DefenceType	否	是	Uint64	防护类型 0漏洞防御 1攻击检测 示例值： 0
Enable	否	是	Uint64	0 关闭 1 开启 示例值： 0
InstanceNum	否	是	Uint64	自选主机数量 示例值： 10
MemberId	否	是	String	用户MemberId 示例值： qq
Nickname	否	是	String	用户昵称 示例值： Alice
Scope	否	是	Uint64	1全部旗舰版主机 0自选主机 示例值： 1
StrategyAction	否	是	Uint64	策略动作 0告警 1防御 示例值： 0
StrategyId	否	是	String	策略id 示例值： any data
StrategyName	否	是	String	策略名称 示例值： defence_redis_cvm
StrategyType	否	是	Uint64	0系统策略 1自定义策略 示例值： 0
SupportVulNum	否	是	Uint64	支持的漏洞个数 示例值： 180
ThreatLevel	否	是	Uint64	威胁等级 示例值： 1
Uin	否	是	String	用户uin 示例值： 101223435

BaselineItemInfo

基线信息

被如下接口引用：DescribeBaselineItemIgnoreList、DescribeBaselineItemInfo、DescribeIgnoreHostAndItemConfig

名称	必选	允许NULL	类型	描述
FixMethod	是	否	String	检测项的修复方法 示例值： 弱口令修复
ItemDesc	是	否	String	检测项描述 示例值： 弱口令
ItemId	是	否	Int64	基线检测项ID 示例值： 1
ItemName	是	否	String	检测项名字 示例值： 设置密码失效时间
Level	是	否	Int64	基线风险等级：0低危 1中危 2高危 3严重 示例值： 1
RelatedCustomRuleInfo	是	是	Array of BaselineCustomRuleIdName	被引自定义规则信息 示例值：查看
RuleId	是	是	Uint64	检测项所属规则的ID 示例值： 43617
RuleName	是	否	String	检测项所属规则名字 示例值： 弱密码
SysRuleId	是	是	Int64	系统规则ID 示例值： 1

FieldValueRatioInfo

快速分析统计信息

被如下接口引用：DescribeFastAnalysis

名称	必选	允许NULL	类型	描述
Count	是	否	Int64	个数 示例值： 0
Ratio	是	否	Float	比例 示例值： 0.5
Value	是	否	String	值 示例值： value

LicenseBindDetail

授权绑定详情信息

被如下接口引用：DescribeLicenseBindList

名称	必选	允许NULL	类型	描述
AgentStatus	否	否	String	主机安全客户端状态,OFFLINE 离线,ONLINE 在线,UNINSTALL 未安装 示例值： OFFLINE
IsSwitchBind	否	否	Bool	是否允许换绑,false 不允许换绑 示例值： false
IsUnBind	否	否	Bool	是否允许解绑,false 不允许解绑 示例值： false
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
MachineIp	否	否	String	机器内网IP 示例值： 1.1.1.1
MachineName	否	否	String	机器别名 示例值： redis_node_cvm
MachineWanIp	否	否	String	机器公网IP 示例值： 1.1.1.1
Quuid	否	否	String	云服务器UUID 示例值： 935e27b1-d675-4509-80bf-96fbf0764237
Tags	否	否	Array of String	标签信息 示例值： ["redis_cvm_01"]
Uuid	否	否	String	主机安全客户端UUID 示例值： 935e27b1-d675-4509-80bf-96fbf0764237

AssetInitServiceBaseInfo

资产管理启动服务列表

被如下接口引用：DescribeAssetInitServiceList

名称	必选	允许NULL	类型	描述
FirstTime	否	否	String	首次采集时间 示例值： 2022-07-15 11:27:01
IsAutoRun	否	是	Int64	开机自启动[0:否
IsNew	否	否	Int64	是否新增[0:否
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	否	String	服务器IP 示例值： 192.168.0.1
MachineName	否	否	String	服务器名称 示例值： redis_node_cvm
MachineWanIp	否	否	String	服务器外网IP 示例值： 43.156.40.46
Name	否	否	String	名称 示例值： bootlocal
OsInfo	否	否	String	操作系统 示例值： 1
Path	否	否	String	路径 示例值： 1
Quuid	否	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Status	否	否	Uint64	默认启用状态：0未启用，1启用 示例值： 1
Type	否	否	Uint64	类型： 1:编码器 2:IE插件 3:网络提供者 4:镜像劫持 5:LSA提供者 6:KnownDLLs 7:启动执行 8:WMI 9:计划任务 10:Winsock提供者 11:打印监控器 12:资源管理器 13:驱动服务 14:登录 示例值： 1
UpdateTime	否	否	String	数据更新时间 示例值： 2011-11-11 12:12:12
User	否	否	String	启动用户 示例值： root
Uuid	否	否	String	主机uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

Component

组件列表数据。

被如下接口引用：DescribeComponents

名称	必选	允许NULL	类型	描述
ComponentName	否	是	String	组件名称。 示例值： redis
ComponentType	否	是	String	组件类型。 • SYSTEM：系统组件 • WEB：Web组件 示例值： SYSTEM

名称	必选	允许NULL	类型	描述
ComponentVersion	否	是	String	组件版本号。 示例值： 1.0.0.1
Id	否	是	Uint64	唯一ID。 示例值： 1
MachineIp	否	是	String	主机内网IP。 示例值： 192.168.0.1
MachineName	否	是	String	主机名。 示例值： redis_cvm
ModifyTime	否	是	Datetime	组件检测更新时间。 示例值： 2020-02-01 12:00:00
Uuid	否	是	String	云镜客户端唯一Uuid。 示例值： 5a540076-d38a-4078-aa98-qwert371d322

FileTamperEvent

核心文件监控事件

被如下接口引用：DescribeFileTamperEvents

名称	必选	允许NULL	类型	描述
CreateTime	否	否	String	发生时间 示例值： 2024-10-28 20:23:23
Description	否	否	String	危害描述 示例值： 检测到用户配置文件'/opt/redis/redis.cfg'被篡改
EventCount	否	否	Uint64	事件产生次数 示例值： 1
ExeMd5	否	否	String	进程名 示例值： 0c0f9309e69d2912ae5242d144bcayay
ExeName	否	是	String	进程名称 示例值： vim
ExePermission	否	否	String	进程权限 示例值： rwx
ExePid	否	否	Uint64	进程pid 示例值： 1
ExeSize	否	否	Uint64	进程文件大小 示例值： 100
ExeTime	否	否	Uint64	进程执行时长 示例值： 1000
FileAction	否	是	String	文件威胁行为 • read 读取文件 • write 修改文件 示例值： read
HostIp	否	否	String	机器IP 示例值： 10.0.0.1
HostName	否	否	String	机器名称 示例值： redis_node_cvm
Id	否	否	Uint64	事件id 示例值： 1
Level	否	否	Uint64	风险等级 0：无， 1: 高危， 2:中危， 3: 低危 示例值： 1
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
MachineStatus	否	否	String	主机在线信息 ONLINE、OFFLINE 示例值： ONLINE
ModifyTime	否	否	String	最近发生时间 示例值： 2024-10-28 20:23:23
PrivateIp	否	否	String	内网ip 示例值： 10.0.0.1
ProcessArgv	否	否	String	进程参数 示例值： vim /home/seadmin/.bashrc
ProcessExe	否	否	String	进程路径 示例值： /tmp/any
Pstree	否	否	String	事件详情: json格式 示例值： [{"pid":2403140,"exe":"/usr/bin/vim","account":"1000:1000","cmdline":"vim /home/seadmin/.bashrc","ssh_service":"10.31.132.68:22"}]
Quuid	否	否	String	cvm id 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
Reference	否	否	String	参考链接 示例值： http://www.ay.com/ay
RuleCategory	否	否	Uint64	规则类型 0系统规则 1自定义规则 示例值： 0
RuleId	否	否	Uint64	规则id 示例值： 1
RuleName	否	否	String	规则名称 示例值： redis_node_check
Status	否	否	Uint64	处理状态 0 -- 待处理 1 -- 已加白 2 -- 已删除 3 - 已忽略 4-已手动处理 示例值： 0
Suggestion	否	否	String	修护建议 示例值： 排查是否为正常业务需要的变更
Target	否	否	String	目标文件路径 示例值： /home/seadmin/.bashrc
TargetCreatTime	否	是	String	目标文件创建时间 示例值： 2021-01-02 15:04:05
TargetModifyTime	否	是	String	目标文件更新时间 示例值： 2021-01-02 15:04:05
TargetName	否	否	String	文件名称 示例值： .bashrc
TargetPermission	否	否	String	目标文件权限 示例值： rwx

名称	必选	允许NULL	类型	描述
TargetSize	否	否	Uint64	目标文件大小 示例值： 1000
Type	否	否	Uint64	事件类型/动作 0 -- 告警 示例值： 0
UserGroup	否	否	String	用户组 示例值： root
UserName	否	否	String	用户名 示例值： root
Uuid	否	否	String	主机uuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0

ShellPolicyList

反弹shell列表数据详情

被如下接口引用：DescribeShellPolicyList

名称	必选	允许NULL	类型	描述
HostScope	否	是	Uint64	主机范围:[0: 一组quuid 1: 所有专业版 2: 旗舰版 3: 所有主机] 示例值： 2
IsEnabled	否	是	Uint64	0 开启, 1关闭 示例值： 0
PolicyAction	否	是	Uint64	策略动作[0:告警,1:放行,2:拦截+告警] 示例值： 0
PolicyDesc	否	是	String	策略描述 示例值： any policy desc
PolicyId	否	是	Uint64	策略ID 示例值： 2001
PolicyName	否	是	String	策略名称 示例值： 系统自动拦截策略
PolicyType	否	是	Uint64	0 系统策略, 1 用户自定义策略 示例值： 0
UpdateTime	否	是	String	更新时间 示例值： 0000-00-00 00:00:00

AssetDatabaseDetail

资源管理数据库列表信息

被如下接口引用：DescribeAssetDatabaseInfo

名称	必选	允许NULL	类型	描述
BinPath	是	否	String	二进制路径 示例值： /usr/local/bin
ConfigPath	是	否	String	配置文件路径 示例值： /etc/mysqld
DataPath	是	否	String	数据路径 示例值： /data/mysql
ErrorLogPath	是	否	String	错误日志路径 示例值： /var/log
Ip	是	否	String	绑定IP 示例值： 0.0.0.0
LogPath	是	否	String	日志文件路径 示例值： /data/log
MachineIp	是	否	String	主机内网IP 示例值： 10.0.0.11
MachineWanIp	是	否	String	主机外网IP 示例值： 1.1.1.1
Name	是	否	String	数据库名 示例值： MySQL
OsInfo	是	否	String	操作系统信息 示例值： Centos 64Bit
Param	是	否	String	启动参数 示例值： --configsvr --port 27019 --keyFile /etc/mongodb/key --dbpath /data/db --replSet d1j49h6z --wiredTigerCacheSizeGB 0.43 --maxConns 10000 --auth --bind_ip_all
Permission	是	否	String	运行权限 示例值： polkitd
PlugInPath	是	否	String	插件路径 示例值： /etc/mysql
Port	是	否	String	监听端口 示例值： 3306
Proto	是	否	String	协议 示例值： tcp
Quuid	是	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
UpdateTime	是	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
User	是	否	String	运行用户 示例值： nginx
Uuid	是	否	String	主机Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Version	是	否	String	版本 示例值： 5.6.7

Filter

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。

- 最多只能有5个Filter

- 同一个Filter存在多个Values，Values值数量最多不能超过5个。

被如下接口引用：DescribeAccountStatistics、DescribeAssetMachineList、DescribeAssetPortInfoList、DescribeAssetProcessInfoList、DescribeAssetSystemPackageList、DescribeAssetUserList、DescribeAssetWebAppList、DescribeAssetWebFrameList、DescribeAssetWebLocationList、DescribeAttackEvents、DescribeAttackLogs、DescribeAttackTop、DescribeAttackTrends、DescribeBanWhiteList、DescribeBaselineDetectList、DescribeBaselineDownloadList、DescribeBaselineFixList、DescribeBaselineHostDetectList、DescribeBaselineItemDetectList、DescribeBaselineItemIgnoreList、DescribeBaselineItemInfo、DescribeBaselineItemList、DescribeBaselinePolicyList、DescribeBaselineRuleDetectList、DescribeBaselineRuleIgnoreList、DescribeBaselineRuleList、DescribeBaselineWeakPasswordList、DescribeBashEvents、DescribeBashEventsNew、DescribeBashPolicies、DescribeBashRules、DescribeBruteAttackList、DescribeClsLogsets、DescribeComponentStatistics、DescribeComponents、DescribeEventList、DescribeExportMachines、DescribeHistoryAccounts、DescribeHostLoginList、DescribeIgnoreHostAndItemConfig、DescribeLicenseBindSchedule、DescribeLoginWhiteCombinedList、DescribeLoginWhiteList、DescribeLoginWhiteListNew、DescribeMaConnEventList、DescribeMaCustomPolicyList、DescribeMaHostList、DescribeMaLabelList、DescribeMaSelfLearnPolicyList、DescribeMaWhitelist、DescribeMaWorkloadList、DescribeMachineDefenseCnt、DescribeMachineRiskCnt、DescribeMachines、DescribeMachinesSimple、DescribeMalWareList、DescribeMalwareWhiteList、DescribeMalwareWhiteListAffectList、DescribeMemShellRules、DescribeNetAttackWhiteList、DescribeOpenPortStatistics、DescribePrivilegeEvents、DescribePrivilegeRules、DescribeProcessStatistics、DescribeProtectDirRelatedServer、DescribeReverseShellEvents、DescribeReverseShellRules、DescribeReverseShellRulesAggregation、DescribeRiskDnsEventList、DescribeRiskDnsList、DescribeRiskDnsPolicyList、DescribeRiskProcessEvents、DescribeSecurityEventStat、DescribeVulDefenceEvent、DescribeVulDefenceList、DescribeVulDefencePluginDetail、DescribeVulDefencePluginStatus、DescribeVulDefenceSettingList、DescribeVulEffectHostList、DescribeVulEffectModules、DescribeVulStoreList、DescribeVuls、ExportAssetMachineList、ExportAssetPortInfoList、ExportAssetProcessInfoList、ExportAssetSystemPackageList、ExportAssetUserList、ExportAssetWebAppList、ExportAssetWebFrameList、ExportAssetWebLocationList、ExportBaselineFixList、ExportBaselineHostDetectList、ExportBaselineItemDetectList、ExportBaselineItemList、ExportBaselineRuleDetectList、ExportBaselineWeakPasswordList、ExportFileTamperRules、ExportJavaMemShellPlugins、ExportJavaMemShells、ExportMaConnEventList、ExportMaCustomPolicyList、ExportMaHostList、ExportMaPodList、ExportMaSelfLearnPolicyList、ExportMaWhitelist、ExportNonlocalLoginPlaces、ExportRiskDnsEventList、ExportRiskDnsPolicyList、ExportRiskProcessEvents、ExportVulDefenceEvent、ExportVulDefenceList、ExportVulDefencePluginEvent、ExportVulEffectHostList、ExportVulList、ModifyBaselinePolicy、ModifyBaselineRule、ModifyBaselineRuleIgnore

名称	必选	允许NULL	类型	描述
ExactMatch	否	否	Bool	模糊搜索 示例值： false
Name	是	否	String	过滤键的名称。 示例值： Keywords
Values	是	否	Array of String	一个或者多个过滤值。 示例值： ["1.1.1.1"]

NetAttackTrend

被如下接口引用：DescribeAttackTrends

名称	必选	允许NULL	类型	描述
AttackCount	否	是	Uint64	攻击次数 示例值： 1
DateTime	否	是	String	时间点，如 2023-05-06 示例值： 2023-05-06
SuccAttackCount	否	是	Uint64	攻击成功次数 示例值： 0
TryAttackCount	否	是	Uint64	尝试攻击次数 示例值： 1

LogInfo

日志详情

被如下接口引用：SearchLog

名称	必选	允许NULL	类型	描述
Content	是	否	String	日志内容的Json序列化字符串 示例值： {"quuid":"fb934eba-1f06-491a-a9c6-ca679fd733dd","recv_time":"1730423894","hostip":"192.168.11.19","count":"1","pid":"5820","appid":"1258352045","cls_event_type":"dns_log"}
FileName	是	否	String	日志文件名称 示例值： fielaName.txt
Source	是	否	String	日志来源IP 示例值： 1.1.1.1
TimeStamp	是	否	Int64	日志时间，单位ms 示例值： 0

MachineSimple

主机列表穿梭框

被如下接口引用：DescribeMachinesSimple

名称	必选	允许NULL	类型	描述
CloudFrom	否	是	Uint64	云服务器厂商类型 0 云 1 IDC机房 2 阿里云 3 华为云 4 亚马逊 5 微软 6 Google 7 Oracle 8 Digital Ocean 示例值： 0
CloudTags	否	是	Array of Tags	云标签信息 示例值：查看
InstanceId	否	是	String	实例ID 示例值： ins-ddsdsay
InstanceState	否	否	String	实例状态： PENDING表示创建中、LAUNCH_FAILED表示创建失败、RUNNING 表示运行中、STOPPED表示关机、STARTING表示开机中、STOPPING表示关机中、REBOOTING表示重启中、SHUTDOWN表示停止待销毁、TERMINATING表示销毁中、TERMINATED已销毁中、TERMINATED_PRO_VERSION已销毁云镜专业版未到期 示例值： RUNNING
IsProVersion	否	否	Bool	是否是专业版。 • true： 是 • false：否 示例值： false
KernelVersion	否	否	String	内核版本 示例值： 3.10.0-1127.19.1.el7.x86_64
LicenseOrder	否	是	LicenseOrder	授权订单对象 示例值：查看
MachineIp	否	否	String	主机IP。 示例值： 10.0.0.2
MachineName	否	否	String	主机名称。 示例值： redis_node_cvm
MachineOs	否	否	String	主机系统。 示例值： centos
MachineType	否	否	String	机器所属专区类型 CVM 云服务器, BM 黑石, ECM 边缘计算, LH 轻量应用服务器 ,Other 混合云专区 示例值： CVM

名称	必选	允许NULL	类型	描述
MachineWanIp	否	否	String	主机外网IP。 示例值： 1.1.1.1
PayMode	否	否	String	主机状态。 • POSTPAY: 表示后付费，即按量计费 • PREPAY: 表示预付费，即包年包月 示例值： PREPAY
ProjectId	否	否	Int64	项目ID 示例值： 1
ProtectType	否	否	String	防护版本 BASIC_VERSION 基础版， PRO_VERSION 专业版，Flagship 旗舰版，GENERAL_DISCOUNT 普惠版. 示例值： BASIC_VERSION
Quuid	否	否	String	CVM或BM机器唯一Uuid。 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
RegionInfo	否	否	RegionInfo	地域信息 示例值：查看
Tag	否	否	Array of MachineTag	标签信息 示例值：查看
Uuid	否	否	String	主机安全uuid，若客户端长时间不在线将返回空字符。 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

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
Condition	是	否	String	检索语句 示例值： count is_one_of 200
DisplayData	是	否	String	展示数据 示例值： [{"id":369266774838,"patternsField":"count","selectedtype":"is"}]
Flag	是	否	String	检索方式。输入框检索：standard,过滤，检索：simple 示例值： simple
Id	否	否	Uint64	规则ID 示例值： 198
LogType	是	否	String	检索索引类型 示例值： userlog-vul
Name	是	否	String	检索名称 示例值： nOqBFVNMgONSxKmSGYZpekKdZJKFMtuGyxMcJeoMsGEIScvKeDcpSFuzHkTlEjqkGVWameNFwntVRRkEbdoDG@Uayay
Query	是	否	String	转换的检索语句内容 示例值： {"index":["userlog-vul"], "body":{"query":{},"sort":[{"create_time":"desc"}]}
TimeRange	是	否	String	时间范围 示例值： 2021-11-11 00:00:00 至 2021-02-01 12:00:00

FileTamperRuleCount

主机关联核心文件规则数量信息

被如下接口引用：DescribeFileTamperRuleCount

名称	必选	允许NULL	类型	描述
Count	是	否	Uint64	关联规则的数量 示例值： 1
Name	是	是	String	关联规则的名称（仅展示其中一条） 示例值： redis_node_check
Uuid	是	否	String	主机uuid 示例值： 935e27b1-d675-4509-80bf-96fbf0764237

TopInfo

被如下接口引用：DescribeAttackTop

名称	必选	允许NULL	类型	描述
Count	否	是	Uint64	top统计计数 示例值： 10
Value	否	是	String	top统计数据，如ip、漏洞名等 示例值： DstPort

VulFixStatusHostInfo

查看漏洞修复详情 每台主机每个漏洞修复状态

被如下接口引用：DescribeVulFixStatus

名称	必选	允许NULL	类型	描述
FailReason	是	是	String	修复失败原因 示例值： 修复超时
HostIp	是	否	String	主机ip 示例值： 10.13.45.12
HostName	是	否	String	主机名称 示例值： redis_node_cvm
ModifyTime	是	否	String	修复时间 示例值： 2021-03-30 19:17:28
Quuid	是	否	String	主机的quuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
Status	是	否	Uint64	状态：0-初始状态；1-已下发任务（修复中）2-完成（成功）；3-修复失败（失败）4-快照创建失败 导致修复失败（未修复）； 示例值： 1

AssetWebAppPluginInfo

资产管理Web应用插件详情

被如下接口引用：DescribeAssetWebAppPluginList

名称	必选	允许NULL	类型	描述
Desc	是	否	String	描述信息 示例值： memo
Link	是	否	String	链接 示例值： /usr/bin/name
Name	是	否	String	名称 示例值： any-app
Version	是	否	String	版本 示例值： 10.0.1

BanWhiteListDetail

阻断白名单展示列表，包含了机器的信息

被如下接口引用：DescribeBanWhiteList

名称	必选	允许NULL	类型	描述
CreateTime	是	否	Datetime	创建白名单时间 示例值： 2021-03-03 16:05:00
Id	是	否	String	白名单ID 示例值： 1
IsGlobal	是	否	Bool	白名单是否全局 示例值： false
MachineIp	是	否	String	机器IP 示例值： 10.0.0.2
MachineName	是	否	String	机器名称 示例值： machineName
ModifyTime	是	否	Datetime	修改白名单时间 示例值： 2021-03-03 16:05:00
Quuid	是	否	String	机器的UUID 示例值： 059cb8b1-98c7-4e44-8345-ba9d87d722e2
Remark	是	否	String	白名单别名 示例值： remarkName
SrcIp	是	否	String	阻断来源IP 示例值： 10.0.0.1
Uuid	是	否	String	主机安全程序的UUID 示例值： 059cb8b1-98c7-4e44-8345-ba9d87d722e2

MonthInspectionReport

专家服务-月巡检报告

被如下接口引用：DescribeMonthInspectionReport

名称	必选	允许NULL	类型	描述
ModifyTime	是	否	String	巡检报告更新时间 示例值： 2021-03-11 09:50:33
ReportName	是	否	String	巡检报告名称 示例值： report-2021-03.pdf
ReportPath	是	否	String	巡检报告下载地址 示例值： https://www.domain.xom/report-2021-03.pdf

ReverseShell

反弹Shell数据

被如下接口引用：DescribeReverseShellEvents

名称	必选	允许NULL	类型	描述
CmdLine	否	否	String	命令详情 示例值： dadad
CmdLineQuote	否	否	String	命令详情的转义后内容，供正则加白全字符串匹配使用 示例值： c2ggcmVkaXMuc2g=
CreateTime	否	否	String	产生时间 示例值： 2021-05-20 17:00:33
DetectBy	否	否	Uint64	检测方法: 0行为分析; 1命令特征检测 示例值： 1
DstIp	否	否	String	目标IP 示例值： 127.0.0.1
DstPort	否	否	Uint64	目标端口 示例值： 12
FullPath	否	否	String	进程路径 示例值： /home
Hostip	否	否	String	主机内网IP 示例值： 127.0.0.1
Id	否	否	Uint64	ID 主键 示例值： 11
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
MachineName	否	否	String	主机名 示例值： redis_node_cvm
ParentProcGroup	否	否	String	父进程用户组 示例值： root
ParentProcName	否	否	String	父进程名 示例值： check_reverse
ParentProcPath	否	否	String	父进程路径 示例值： /home
ParentProcUser	否	否	String	父进程用户 示例值： root

名称	必选	允许NULL	类型	描述
Pid	否	是	Int64	进程id 示例值： 1
ProcTree	否	否	String	进程树 示例值： bash(25605),python3.7(25604),bash(25603),bash(25579),bash(25578),bash(3477),login(1307)
ProcessName	否	否	String	进程名 示例值： 1.exe
Quuid	否	否	String	主机ID 示例值： check_reverse
RiskLevel	否	是	Uint64	威胁等级：0中危，1高危 示例值： 1
Status	否	否	Uint64	处理状态：0-待处理 2-白名单 3-已处理 4-已忽略 6-已拦截 示例值： 2
UserGroup	否	否	String	执行用户组 示例值： root
UserName	否	否	String	执行用户 示例值： root
Uuid	否	否	String	主机安全UUID 示例值： 5a540076-d38a-4078-aa98-q45rt371d322

Filters

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：DescribeBaselineEffectHostList、DescribeBaselineList、DescribeCanNotSeparateMachine、DescribeEmergencyResponseList、DescribeEmergencyVulList、DescribeFileTamperEvents、DescribeFileTamperRules、DescribeGeneralStat、DescribeIgnoreRuleEffectHostList、DescribeImportMachineInfo、DescribeJavaMemShellList、DescribeJavaMemShellPluginInfo、DescribeJavaMemShellPluginList、DescribeLicenseBindList、DescribeLicenseList、DescribeMaPodList、DescribeMachineClearHistory、DescribeMaliciousRequestWhiteList、DescribeOrderList、DescribeRansomDefenseBackupList、DescribeRansomDefenseEventsList、DescribeRansomDefenseMachineList、DescribeRansomDefenseRollBackTaskList、DescribeRansomDefenseStrategyList、DescribeRansomDefenseStrategyMachines、DescribeScanState、DescribeScanTaskDetails、DescribeShellPolicyList、DescribeTags、DescribeVulList、ExportAttackEvents、ExportAttackLogs、ExportBaselineEffectHostList、ExportBaselineList、ExportBashEvents、ExportBashEventsNew、ExportBashPolicies、ExportBruteAttacks、ExportFileTamperEvents、ExportIgnoreRuleEffectHostList、ExportLicenseDetail、ExportMaliciousRequests、ExportMalwares、ExportPrivilegeEvents、ExportRansomDefenseBackupList、ExportRansomDefenseEventsList、ExportRansomDefenseMachineList、ExportRansomDefenseStrategyList、ExportRansomDefenseStrategyMachines、ExportReverseShellEvents、ExportScanTaskDetails、ExportVulDetectionReport、ModifyEventAttackStatus、ModifyRiskEventsStatus、OpenProVersionActivity

名称	必选	允许NULL	类型	描述
ExactMatch	否	否	Bool	是否模糊匹配，前端框架会带上，可以不管 示例值： false
Name	是	否	String	过滤键的名称。 示例值： Name
Values	是	否	Array of String	一个或者多个过滤值。 示例值： ["value"]

RegionInfo

地域信息

被如下接口引用：DescribeMachineList、DescribeMachineRegionList、DescribeMachineRegions、DescribeMachines、DescribeMachinesSimple、DescribeRansomDefenseMachineList、DescribeRansomDefenseRollBackTaskList、DescribeRansomDefenseStrategyMachines

名称	必选	允许NULL	类型	描述
Region	是	否	String	地域 示例值： region1
RegionCode	是	否	String	地域代码，如 gz，sh，bj 示例值： gz
RegionId	是	否	Uint64	地域ID 示例值： 1
RegionName	是	否	String	地域名字 示例值： region1
RegionNameEn	是	否	String	地域英文名 示例值： ap-region1

BaselineHostDetect

基线主机检测

被如下接口引用：DescribeBaselineHostDetectList

名称	必选	允许NULL	类型	描述
DetectStatus	否	否	Int64	0:未通过 1:忽略 3:通过 5:检测中 示例值： 0
FirstTime	否	否	String	首次检测时间 示例值： 2021-02-01 12:00:00
HostId	否	否	String	主机Id 示例值： 7b2effb9-d1d9-4bb7-9b5d-d80c88ddayay
HostIp	否	否	String	内网Ip 示例值： 192.168.0.204
HostName	否	否	String	主机名称 示例值： redis_node_cvm
ItemCount	否	否	Int64	关联检测项数 示例值： 1
LastTime	否	否	String	最后检测时间 示例值： 2021-02-01 12:00:00
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
NotPassedItemCount	否	否	Int64	检测未通过数 示例值： 1
PassedItemCount	否	否	Int64	检测通过数 示例值： 0
Uuid	否	是	String	主机安全UUID 示例值： 1bc7422a-2366-11e9-a4c5-525400f7ayay
WanIp	否	否	String	外网Ip 示例值： 192.168.0.204

AssetWebServiceBaseInfo

资源管理Web服务列表信息

被如下接口引用：DescribeAssetWebServiceInfoList

名称	必选	允许NULL	类型	描述
BinPath	否	否	String	二进制路径 示例值： /usr/bin
ConfigPath	否	否	String	配置路径 示例值： /root
Desc	否	否	String	描述信息 示例值： 1
FirstTime	否	否	String	首次采集时间 示例值： 2022-07-15 11:27:01
Id	否	否	String	Web服务ID 示例值： 1001
InstallPath	否	否	String	安装路径 示例值： /root
IsNew	否	否	Int64	是否新增[0:否
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	否	String	主机内网IP 示例值： 10.0.0.11
MachineName	否	否	String	主机名称 示例值： agentinstance
MachineWanIp	否	否	String	主机外网IP 示例值： 1.1.1.1
Name	否	否	String	服务名 示例值： Nginx
OsInfo	否	否	String	操作系统信息 示例值： Centos 64Bit
ProcessCount	否	否	Uint64	关联进程数 示例值： 1
ProjectId	否	否	Uint64	主机业务组ID 示例值： 1
Quuid	否	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Tag	否	是	Array of MachineTag	主机标签 示例值：查看
UpdateTime	否	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
User	否	否	String	启动用户 示例值： root
Uuid	否	否	String	主机Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Version	否	否	String	版本 示例值： 1.0.1

NetAttackWhiteRule

被如下接口引用：DescribeNetAttackWhiteList

名称	必选	允许NULL	类型	描述
CreateTime	否	是	String	创建时间 示例值： 2024-10-30 02:18:51
DealOldEvents	否	是	Uint64	是否处理之前的事件 0: 不处理 1:处理 示例值： 1
Description	否	是	String	规则描述 示例值： add for redis cvm
Id	否	是	Uint64	规则id 示例值： 1
ModifyTime	否	是	String	修改时间 示例值： 2024-10-30 02:18:51
Quuids	否	是	String	主机quuid 多个用;隔开 示例值： ea71992a-b484-4d9c-882a-419fb6d0a5b0
Scope	否	是	Uint64	0: 一组quuid 1: 所有主机 示例值： 1
SrcIP	否	是	String	来源IP 单IP:1.1.1.1 IP范围:1.1.1.1-1.1.2.1 IP范围：1.1.1.0/24 多个用;隔开 示例值： 127.0.0.1

BillingDefineParams

计费下单自定义参数

被如下接口引用：CreateLicenseOrder

名称	必选	允许NULL	类型	描述
AutoBindSwitch	否	否	Bool	自动绑定开关 示例值： false
AutoRepurchaseRenewSwitch	否	否	Bool	自动加购订单是否自动续费 示例值： false
AutoRepurchaseSwitch	否	否	Bool	自动加购开关 示例值： false
ProtectType	否	否	String	防护版本 示例值： "PRO_VERSION"

RansomDefenseStrategyMachineInfo

防勒索机器硬盘配置

被如下接口引用：CreateRansomDefenseStrategy

名称	必选	允许NULL	类型	描述
DiskInfo	否	是	String	指定硬盘列表，为空时表示所有硬盘：disk_id1
Uuid	是	否	String	主机uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

NetAttackTopInfo

被如下接口引用：DescribeAttackTop

名称	必选	允许NULL	类型	描述
Agent	否	是	Array of TopInfo	网络攻击主机维度top统计数据 示例值：查看
DstPort	否	是	Array of TopInfo	网络攻击目标端口维度top统计数据 示例值：查看
SrcIp	否	是	Array of TopInfo	网络攻击ip来源维度top统计数据 示例值：查看
Vul	否	是	Array of TopInfo	网络攻击漏洞维度top统计数据 示例值：查看

ScreenMachine

大屏主机列表数据

被如下接口引用：DescribeScreenMachines

名称	必选	允许NULL	类型	描述
BaselineNum	否	否	Int64	基线风险数。 示例值： 2
CoreVersion	否	否	String	内核版本 示例值： 3.10.0-1127.19.1.el7.x86_64
CpuLoad	否	否	String	cpu 负载状态 示例值： 低
CpuSize	否	否	Float	cpu 核数 示例值： 1
CyberAttackNum	否	否	Int64	网络风险数。 示例值： 2
DiskLoad	否	否	String	硬盘使用率 % 示例值： 10.60
DiskSize	否	否	Float	硬盘容量GB 示例值： 40
InvasionNum	否	否	Int64	入侵事件数 示例值： 1
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	否	String	主机IP。 示例值： 10.0.0.2
MachineName	否	否	String	主机名称。 示例值： redis_node_cvm
MachineOs	否	否	String	主机系统。 示例值： centos
MachineStatus	否	否	Uint64	大屏主机状态 0：未安装agent，1：离线状态，2:离线-风险，3：离线-严重 4：安装设备-正常，5：安装设备-正常 且是专业版或旗舰版，6：安装设备-风险（网络攻击事件>0）， 7：安装设备-风险（网络攻击事件>0 且是专业版或旗舰版，8：安装设备-严重（入侵检测事件>0）， 9：安装设备-严重（入侵检测事件>0）且是专业版或旗舰版 示例值： 1
MachineType	否	否	String	机器所属专区类型 CVM 云服务器, BM 黑石, ECM 边缘计算, LH 轻量应用服务器 ,Other 混合云专区 示例值： CVM
MachineWanIp	否	否	String	主机外网IP。 示例值： 114.11.12.13
MemLoad	否	否	String	内存负载率% 示例值： 18.66
MemSize	否	否	Float	内存容量 GB 示例值： 2
Quuid	否	否	String	CVM或BM机器唯一Uuid。 示例值： d99a1b46-cc2d-4633-a11f-4a7663d2523e
SecurityStatus	否	否	String	风险状态。 • SAFE：安全 • RISK：风险 • UNKNOWN：未知 示例值： RISK
Uuid	否	否	String	主机安全Uuid，若客户端长时间不在线将返回空字符。 示例值： d99a1b46-cc2d-4633-a11f-4a7663d2523e
VulNum	否	否	Int64	漏洞数。 示例值： 2

DefendAttackLog

网络攻击日志

被如下接口引用：DescribeAttackLogs

名称	必选	允许NULL	类型	描述
CreatedAt	否	否	String	攻击时间 示例值： 2020-01-01 00:00:00
DstIp	否	否	String	目标IP 示例值： 1.1.1.1
DstPort	否	否	Uint64	目标端口 示例值： 8080
HttpCgi	否	否	String	攻击描述 示例值： any attack msg

名称	必选	允许NULL	类型	描述
HttpContent	否	否	String	攻击内容 示例值： content
HttpMethod	否	否	String	攻击方式 示例值： POST
HttpParam	否	否	String	攻击参数 示例值： POST /demo3-1/baseServlet HTTP/1.1
Id	否	否	Uint64	日志ID 示例值： 10001
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
MachineIp	否	否	String	目标服务器IP 示例值： 1.1.1.1
MachineName	否	否	String	目标服务器名称 示例值： 1.1.1.1
SrcIp	否	否	String	来源IP 示例值： 1.1.1.1
SrcPort	否	否	Uint64	来源端口 示例值： 32456
Uuid	否	否	String	客户端ID 示例值： 93b5fa8f-f5bc-4cf9-8253-d2739e5aa484
VulType	否	否	String	威胁类型 示例值： tcp

PushTaskResult

快捷防护-下发检测，扫描结果

被如下接口引用：CreateQuickProtectSetting

名称	必选	允许NULL	类型	描述
FailureReason	是	否	String	下发失败原因 示例值： 正在检测中
IsSuccess	是	否	Bool	是否下发成功 示例值： true
TaskId	是	否	Uint64	对应任务Id 示例值： 1
TaskType	是	否	String	任务种类：Vul-检测漏洞，Malware-文件查杀，Baseline-基线检测，AutoBan-自动阻断 示例值： Vul

RiskDnsList

恶意请求列表

被如下接口引用：DescribeRiskDnsInfo、DescribeRiskDnsList

名称	必选	允许NULL	类型	描述
AccessCount	是	否	Uint64	访问次数 示例值： 22
Alias	是	否	String	别名 示例值： by_nginx
CmdLine	是	否	String	命令行 示例值： cmd
CreateTime	是	否	String	首次访问时间 示例值： 2021-04-26 15:19:04
Description	是	否	String	描述信息 示例值： desc of this risk
GlobalRuleId	是	否	Uint64	是否为全局规则，0否，1是 示例值： 22
HostIp	是	否	String	主机ip 示例值： 13.22.3.1
Id	是	否	Uint64	唯一ID 示例值： 153
MachineStatus	是	是	String	主机在线状态[OFFLINE:离线
MachineWanIp	是	是	String	外网ip 示例值： 13.22.3.1
MergeTime	是	否	String	最近访问时间 示例值： 2021-04-26 15:19:04
Pid	是	否	Uint64	进程号 示例值： 33
ProcessMd5	是	否	String	进程MD5 示例值： e10adc3949ba59abbe56e057f20f883e
ProcessName	是	否	String	进程名 示例值： nginx
Quuid	是	否	String	唯一 Quuid 示例值： 5a540076-d38a-4078-aa98-q45rt371d322
Reference	是	否	String	参考 示例值： http://www.vxjump.net/files/virus_analysis/virut%20botnet%20anal
Status	是	否	Uint64	状态；0-待处理，2-已加白，3-非信任状态，4-已处理，5-已忽略 示例值： 0
SuggestScheme	是	否	String	建议方案 示例值： 1、检查恶意进程及非法端口，删除可疑的启动项和定时任务； 2、隔离或者删除相关的木马文件；
Tags	是	否	Array of String	标签特性 示例值： ["vueir","mle"]
Url	是	否	String	对外访问域名 示例值： re.r3r3.org
UserRuleId	是	否	Uint64	用户规则id 示例值： 12

名称	必选	允许NULL	类型	描述
Uuid	是	否	String	唯一UUID 示例值： 5a540076-d38a-4078-aa98-q45rt371d322

ScreenDefendAttackLog

大屏网络攻击日志

被如下接口引用：DescribeScreenHostInvasion

名称	必选	允许NULL	类型	描述
CreatedTime	是	否	String	攻击时间 示例值： 2021-03-30 19:17:28
DstIp	是	否	String	目标IP 示例值： 120.22.1.22
DstPort	是	否	Uint64	目标端口 示例值： 2343
HttpMethod	是	否	String	攻击方式 示例值： POST
Id	是	否	Uint64	日志ID 示例值： 1
Quuid	是	否	String	主机 quuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
SrcIp	是	否	String	来源IP 示例值： 120.22.1.22
SrcPort	是	否	Uint64	来源端口 示例值： 546
Uuid	是	否	String	客户端ID 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
VulType	是	否	String	威胁类型 示例值： CMD-EXEC

VulInfoHostInfo

批量修复漏洞二次弹窗

被如下接口引用：DescribeCanFixVulMachine

名称	必选	允许NULL	类型	描述
HostIp	是	是	String	主机ip 示例值： 10.13.45.12
HostName	是	是	String	主机名 示例值： redis_node_cvm
InstanceId	是	是	String	主机InstanceId 示例值： ins-dhuahsd
IsSupportAutoFix	是	是	Uint64	0 :漏洞不可自动修复， 1：可自动修复， 2：客户端已离线， 3：主机不是旗舰版只能手动修复， 4：机型不允许 ，5：修复中 ，6：已修复， 7：检测中, 9:修复失败, 10:已忽略 ,11:漏洞只支持linux不支持Windows, 12：漏洞只支持Windows不支持linux 示例值： 1
Quuid	是	是	String	主机quuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
Tags	是	是	Array of String	主机标签 示例值： ["tag1","tag2"]
Uuid	是	是	String	主机uuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0

BaselineBasicInfo

基线基础信息

被如下接口引用：DescribeBaselineBasicInfo

名称	必选	允许NULL	类型	描述
BaselineId	是	是	Uint64	基线id 示例值： 1
Name	是	是	String	基线名称 示例值： 弱密码
ParentId	是	是	Uint64	父级id 示例值： 0

BroadcastInfo

安全播报文章详情

被如下接口引用：DescribeSecurityBroadcastInfo

名称	必选	允许NULL	类型	描述
Content	是	否	String	富文本内容信息 示例值： 漏洞详情信息
CreateTime	是	否	String	发布时间 示例值： 2021-03-30 19:17:28
GotoType	是	是	Uint64	跳转位置：0=不跳转，1=文件查杀，2=漏洞扫描，3=安全基线 示例值： 1
Id	是	否	Uint64	文章唯一Id 示例值： 12
Subtitle	是	否	String	副标题 示例值： 新版本支持漏洞修复
Title	是	是	String	文章名字 示例值： 漏洞爆发
Type	是	否	Uint64	类型：0=紧急通知，1=功能更新，2=行业荣誉，3=版本发布 示例值： 1

OrderModifyConfig

订单变配对象

被如下接口引用：ModifyOrder

名称	必选	允许NULL	类型	描述
InquireKey	是	是	String	计费项 sv 示例值： sv_yunjing_ue_x
InquireNum	是	是	Uint64	购买量 示例值： 10
SubProductCode	是	是	String	子产品 sp_ 示例值： sp_yunjing_0014

ScreenNameValue

【云安全预警】大屏可视化数据Name Value 数据

被如下接口引用：DescribeScreenEventsCnt、DescribeScreenGeneralStat、DescribeScreenRiskAssetsTop

名称	必选	允许NULL	类型	描述
Name	是	否	String	统计类型 不同接口对应不同的内容 示例值： 离线/关机
Value	是	否	Uint64	统计数量 示例值： 12

StandardModeConfig

标准模式阻断配置

被如下接口引用：DescribeBanMode

名称	必选	允许NULL	类型	描述
Ttl	是	否	Uint64	阻断时长，单位：秒 示例值： 300

ScreenBroadcasts

大屏可视化安全播报内容

被如下接口引用：DescribeScreenBroadcasts

名称	必选	允许NULL	类型	描述
Id	是	否	Uint64	文章ID 示例值： 10003
Level	是	否	Uint64	播报文章危险程度 0：无， 1：严重， 2: 高危， 3:中危， 4: 低危 示例值： 1
Time	是	否	String	发布时间 示例值： 2021-03-30 19:17:28
Title	是	否	String	播报文章标题 示例值： 发现 Apache HTTP/2 协议拒绝服务漏洞(CVE-2023-44487) 漏洞

AssetPortBaseInfo

资源管理账号基本信息

被如下接口引用：DescribeAssetPortInfoList

名称	必选	允许NULL	类型	描述
BindIp	否	否	String	绑定IP 示例值： 192.168.0.1
FirstTime	否	否	String	首次采集时间 示例值： 2022-07-15 11:27:01
GroupName	否	否	String	所属用户组 示例值： staffs
IsNew	否	否	Int64	是否新增[0:否
MachineExtraInfo	否	是	MachineExtraInfo	主机信息 示例值：查看
MachineIp	否	否	String	主机内网IP 示例值： 10.33.0.155
MachineName	否	否	String	主机名称 示例值： 1
MachineWanIp	否	否	String	主机外网IP 示例值： 112.44.64.99
Md5	否	否	String	进程MD5 示例值： c2caaa18e873ddae87c6167791ff97a8
OsInfo	否	否	String	操作系统信息 示例值： Centos 64Bit
Param	否	否	String	启动参数 示例值： /usr/sbin/cupsd -l
ParentProcessName	否	否	String	父进程名称 示例值： root
Pid	否	否	String	进程ID 示例值： 1024
Port	否	否	String	端口 示例值： 22
Ppid	否	否	String	父进程ID 示例值： 1
ProcessName	否	否	String	进程名称 示例值： a.out
ProcessPath	否	否	String	进程路径 示例值： /root
ProcessVersion	否	否	String	进程版本 示例值： 1.1.1

名称	必选	允许NULL	类型	描述
ProjectId	否	否	Uint64	主机业务组ID 示例值： 1
Proto	否	否	String	端口协议： udp、tcp 示例值： tcp
Quuid	否	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
StartTime	否	否	String	启动时间 示例值： 2024-10-23 14:12:54
Tag	否	是	Array of MachineTag	主机标签 示例值：查看
Teletype	否	否	String	进程TTY 示例值： ?
UpdateTime	否	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
User	否	否	String	运行用户 示例值： root
Uuid	否	否	String	主机Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

MachineFileTamperRule

查询主机相关核心文件监控规则详情

被如下接口引用：DescribeMachineFileTamperRules

名称	必选	允许NULL	类型	描述
Id	是	否	Uint64	唯一id 示例值： 11
Name	是	是	String	规则名称 示例值： 禁止访问
Rule	是	否	Array of FileTamperRule	规则 示例值：查看
RuleCategory	是	否	Uint64	规则类型 0 ：系统规则 1：用户规则 示例值： 1

AssetUserKeyInfo

资产管理账号key详情

被如下接口引用：DescribeAssetUserInfo、DescribeAssetUserKeyList

名称	必选	允许NULL	类型	描述
Comment	是	否	String	公钥备注 示例值： comment
EncryptType	是	否	String	加密方式 示例值： aes
Value	是	否	String	公钥值 示例值： value1

UpdateHostLoginWhiteObj

编辑白名单实体

被如下接口引用：ModifyLoginWhiteInfo

名称	必选	允许NULL	类型	描述
EndTime	否	否	String	结束时间 示例值： 2024-01-01 23:59:59
Id	是	否	Uint64	要更新的数据id 示例值： 128
Places	是	否	Array of Place	地域信息数组 示例值：查看
Remark	是	否	String	备注信息 示例值： updateRemark1
SrcIp	是	否	String	来源ip 示例值： 1.2.3.4
StartTime	否	否	String	开始时间 示例值： 2024-01-01 00:00:00
UserName	是	否	String	用户名 示例值： username

BaselineRuleDetect

基线规则检测

被如下接口引用：DescribeBaselineRuleDetectList

名称	必选	允许NULL	类型	描述
DetectStatus	是	否	Int64	0:未通过 1:忽略 3:通过 5:检测中 示例值： 0
FirstTime	是	否	String	首次检测时间 示例值： 2021-02-01 12:00:00
HostCount	是	否	Int64	关联主机数 示例值： 9
ItemCount	是	否	Int64	关联项数 示例值： 32
ItemIds	是	是	Array of Int64	ItemID集合 示例值： [3855]
LastTime	是	否	String	string 示例值： 2021-02-01 12:00:00

名称	必选	允许NULL	类型	描述
RuleDesc	是	否	String	规则描述 示例值： 国际标准-CentOS 6安全基线检查
RuleId	是	否	Int64	规则Id 示例值： 30
RuleName	是	否	String	规则名称 示例值： 国际标准-CentOS 6安全基线检查

KeyValueInfo

键值索引配置

被如下接口引用：DescribeLogIndex

名称	必选	允许NULL	类型	描述
CaseSensitive	是	否	Bool	是否大小写敏感 示例值： false
KeyValues	是	是	Array of KeyValueArrayInfo	需要建立索引的键值对信息 示例值：查看

VulEffectModuleInfo

漏洞影响组件详情

被如下接口引用：DescribeVulEffectModules

名称	必选	允许NULL	类型	描述
FixCmd	是	否	String	修复命令 示例值： sudo yum update openssl
Name	是	否	String	组件名 示例值： net-wsion
Path	是	否	String	组件路径 示例值： /root/
Quuids	是	否	Array of String	影响的主机quuid 示例值： ["e5b4724c-49af-46ab-bd84-cdbae897e7e0"]
Rule	是	否	String	组件影响版本 示例值： npt version less than 2.0.0
Uuids	是	否	Array of String	影响的主机uuid 示例值： ["e5b4724c-49af-46ab-bd84-cdbae897e7e0"]
Version	是	否	String	组件版本 示例值： 1.1.1

RansomDefenseStrategyMachineDetail

防勒索主机列表

被如下接口引用：DescribeRansomDefenseStrategyMachines

名称	必选	允许NULL	类型	描述
CloudTags	是	是	Array of Tag	云标签 示例值：查看
DiskInfo	是	是	String	硬盘信息，为空时所有硬盘生效： ;分割 diskId1
HostVersion	是	是	Uint64	版本信息：0-基础版 1-专业版 2-旗舰版 3-普惠版 示例值： 0
InstanceId	是	否	String	主机实例id 示例值： cvm-asasa
MachineIp	是	否	String	内网ip 示例值： 10.0.0.22
MachineName	是	否	String	主机名称 示例值： redis_node_cvm
MachineWanIp	是	是	String	外网ip 示例值： 112.11.33.22
Quuid	是	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
RegionInfo	是	是	RegionInfo	可用区信息 示例值：查看
Status	是	是	Uint64	防护状态：0关闭，1开启 示例值： 0
StrategyId	是	是	Uint64	策略id，为0时未绑定策略 示例值： 0
StrategyName	是	是	String	策略名称 示例值： tt1
Tag	是	是	Array of MachineTag	主机安全标签 示例值：查看
Uuid	是	否	String	主机Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

MachineLicenseDetail

机器绑定授权信息

被如下接口引用：DescribeMachineLicenseDetail

名称	必选	允许NULL	类型	描述
InquireKey	是	否	String	废弃字段, 示例值： sv_yunjing_ue_x
PayMode	是	否	Uint64	计费模式, 0 按量计费，1 预付费 示例值： 1
Quuid	是	否	String	主机quuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0

名称	必选	允许NULL	类型	描述
ResourceId	是	否	String	资源ID 示例值： anyid
SourceType	是	否	Uint64	订单类型,0 默认计费订单 1 试用订单, 2 赠送 3 体验 示例值： 1

LoginWhiteCombinedInfo

异地登录合并后白名单

被如下接口引用：DescribeLoginWhiteCombinedList

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	创建时间 示例值： 2024-11-04 09:57:28
Desc	是	否	String	白名单描述：IsLocal=1时固定为：全部服务器；单台机器时为机器ip，多台服务器时为服务器quuid 示例值： 192.168.0.2
EndTime	是	否	String	结束时间 示例值： 2024-11-04 09:57:28
Id	是	否	Uint64	白名单ID 示例值： 1001
IsGlobal	是	否	Uint64	是否对全局生效, 1：全局有效 0: 对指定主机列表生效' 示例值： 1
Locale	是	否	String	地域字符串 示例值： locale1
Locations	是	否	String	登陆地 示例值： location1
ModifyTime	是	否	String	最近修改时间 示例值： 2024-11-04 09:57:28
Name	是	否	String	白名单名字：IsLocal=1时固定为：全部服务器；单台机器时为机器名字，多台服务器时为服务器quuid 示例值： redis_node_cvm
Places	是	是	Array of Place	白名单地域 示例值：查看
Remark	是	否	String	备注 示例值： add redis cvm ip
SrcIp	是	否	String	白名单IP（多个IP逗号隔开） 示例值： 192.168.0.204
StartTime	是	否	String	开始时间 示例值： 2024-11-04 09:57:28
UserName	是	否	String	白名单用户（多个用户逗号隔开） 示例值： uname
Uuid	是	否	String	服务器Uuid 示例值： df131b24-8528-4809-9d07-a9e4d58ad566

ReverseShellEventInfo

反弹Shell数据详情

被如下接口引用：DescribeReverseShellEventInfo

名称	必选	允许NULL	类型	描述
CmdLine	是	否	String	命令详情 示例值： ./reverse_out
CmdLineQuote	否	否	String	命令详情的转义后内容，供正则加白全字符串匹配使用 示例值： ./reverse_out
CreateTime	是	否	String	产生时间 示例值： 2021-05-20 17:00:33
DetectBy	是	否	Uint64	检测方法 示例值： 1
DstIp	是	否	String	目标IP 示例值： 127.0.0.1
DstPort	是	否	Uint64	目标端口 示例值： 12
FullPath	是	否	String	进程路径 示例值： /home
HarmDescribe	是	否	String	描述信息 示例值： 黑客在入侵服务器后，为了进行下一步的恶意操作，会执行恶意文件下载、连接矿池、添加公钥、查看敏感文件等操作。
HostIp	是	否	String	主机内网IP 示例值： 127.0.0.1
Id	是	否	Uint64	ID 主键 示例值： 11
MachineName	是	否	String	主机名 示例值： redis_node_cvm
MachineStatus	是	否	String	主机在线状态 OFFLINE ONLINE 示例值： OFFLINE
MachineWanIp	是	否	String	主机外网ip 示例值： 124.2.4.55
ModifyTime	是	否	String	处理时间 示例值： 2021-03-30 19:17:28
ParentProcGroup	是	否	String	父进程用户组 示例值： root
ParentProcName	是	否	String	父进程名 示例值： 2.exe
ParentProcPath	是	否	String	父进程路径 示例值： /home
ParentProcUser	是	否	String	父进程用户 示例值： root
ProcessName	是	否	String	进程名 示例值： reverse_out

名称	必选	允许NULL	类型	描述
PsTree	是	是	String	进程树 json pid:进程id，exe:文件路径 ，account:进程所属用组和用户 ,cmdline:执行命令，ssh_service: SSH服务ip, ssh_soure:登录源 示例值： [{"pid":"1"}]
Quuid	是	否	String	主机uuid 示例值： e8fc6e04-5b3d-405d-ab61-da7cc8be2583
References	是	否	Array of String	参考链接 示例值： ["http://www.domain.com"]
Status	是	否	Uint64	处理状态：0-待处理 2-白名单 3-已处理 4-已忽略 示例值： 2
SuggestScheme	是	否	String	建议方案 示例值： 1.检查恶意进程及非法端口，删除可疑的启动项和定时任务； 2.隔离或者删除相关的木马文件；
Tags	是	否	Array of String	标签 示例值： ["标签1","标签2"]
UserGroup	是	否	String	执行用户组 示例值： root
UserName	是	否	String	执行用户 示例值： root
Uuid	是	否	String	主机安全uuid 示例值： e8fc6e04-5b3d-405d-ab61-da7cc8be2583

CreateVulFixTaskQuuids

创建修复任务的quuids

被如下接口引用：CreateVulFix

名称	必选	允许NULL	类型	描述
FixMethod	否	是	Uint64	修复方式 0组件更新或者安装补丁,1禁用服务 示例值： 0
Quuids	是	否	Array of String	需要修复漏洞的主机，所有主机必须有VulId的这个漏洞且是待修复状态。 示例值： ["e5b4724c-49af-46ab-bd84-cdbae897e7e0"]
VulId	是	否	Uint64	漏洞id 示例值： 1089

AssetAppProcessInfo

软件应用关联进程信息

被如下接口引用：DescribeAssetAppProcessList、DescribeAssetJarInfo、DescribeAssetWebServiceProcessList

名称	必选	允许NULL	类型	描述
Name	是	否	String	名称 示例值： sshd
Path	是	否	String	路径 示例值： /usr/bin/sshd
StartTime	是	否	String	启动时间 示例值： 2024-10-23 14:17:00
Status	是	否	String	进程状态：R 可执行、S 可中断、D 不可中断、T 暂停状态或跟踪状态、Z 僵尸状态、X 将被销毁 示例值： R
User	是	否	String	用户 示例值： root
Version	是	否	String	进程版本 示例值： 1.1.1

CanNotSeparateInfo

不可隔离木马的机器信息

被如下接口引用：DescribeCanNotSeparateMachine

名称	必选	允许NULL	类型	描述
Alias	是	否	String	主机名 示例值： redis_node_cvm
PrivateIp	是	否	String	内网ip 示例值： 127.12.1.1
PublicIp	是	否	String	外网ip 示例值： 192.2.23.1
Quuid	是	否	String	主机quuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
Reason	是	否	Uint64	隔离失败原因 1:agent离线 示例值： 1
Uuid	是	否	String	主机uuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0

LicenseExtraParam

授权额外参数

被如下接口引用：DescribeLicenseList

名称	必选	允许NULL	类型	描述
IsUnBind	否	是	Bool	是否允许解绑/换绑 示例值： false
UnionBuyDetail	否	是	Array of UnionProtectDetail	容器&主机联合购买信息 示例值：查看

ProcessStatistics

进程数据统计数据。

被如下接口引用：DescribeProcessStatistics

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
MachineNum	是	否	Uint64	主机数量。 示例值： 0
ProcessName	是	否	String	进程名。 示例值： nginx

BaselineCategory

基线规则或项的分类

被如下接口引用：DescribeBaselineItemInfo、DescribeBaselineRuleCategoryList

名称	必选	允许NULL	类型	描述
CategoryId	是	否	Int64	分类Id 示例值： 1
CategoryName	是	否	String	分类名称 示例值： 弱密码
ItemCount	否	是	Uint64	子分类下检测项总数 示例值： 100
ParentCategoryId	是	否	Int64	父分类ID,如果为0则没有父分类 示例值： 1

BaselineEventLevelInfo

服务器风险Top的主机信息

被如下接口引用：DescribeBaselineHostTop

名称	必选	允许NULL	类型	描述
EventCount	是	是	Uint64	漏洞数量 示例值： 10
EventLevel	是	是	Uint64	危害等级：1-低危；2-中危；3-高危；4-严重 示例值： 2

CKafkaRouteInfo

CKafka域名信息

被如下接口引用：DescribeLogDeliveryKafkaOptions

名称	必选	允许NULL	类型	描述
AccessType	是	否	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） 示例值： 1
Domain	是	否	String	域名 示例值： www.a.com
DomainPort	是	否	Uint64	域名端口 示例值： 80
RouteID	是	否	Int64	路由ID 示例值： 1
Vip	是	否	String	虚拟ip 示例值： 1.1.1.1
VipType	是	否	Int64	虚拟ip类型1:外网TGW 2:基础网络 3:VPC网络 4:支撑网络(标准版) 5:SSL外网访问方式访问 6:黑石环境vpc 7:支撑网络(专业版) 示例值： 1

MachineClearHistory

机器清理记录对象

被如下接口引用：DescribeMachineClearHistory

名称	必选	允许NULL	类型	描述
AgentLastOfflineTime	是	否	String	客户端最后离线时间 示例值： 2020-03-28 17:33:04
CreateTime	是	否	String	创建时间 示例值： 2019-03-28 17:33:04
Id	是	否	Uint64	ID值 示例值： 1
InstanceId	是	否	String	实例ID 示例值： ins-vdfy7df
InstanceName	是	否	String	实例名称 示例值： redis_node_cvm
PrivateIp	是	否	String	内网IP 示例值： 10.0.0.1
PublicIp	是	否	String	公网IP 示例值： 8.8.8.8

BaselineDetail

基线详情

被如下接口引用：DescribeBaselineDetail

名称	必选	允许NULL	类型	描述
Description	是	是	String	基线描述 示例值： MySQL 采用弱口令容易被黑客猜解从而获取数据权限，导致数据被黑客偷窃、删除等；同时，黑客可能再基于数据库进一步获取系统权限。
Level	是	是	Uint64	危害等级 示例值： 3
Name	是	是	String	基线名 示例值： 弱密码
PackageName	是	是	String	package名 示例值： 21.dat

名称	必选	允许NULL	类型	描述
ParentId	是	是	Uint64	父级id 示例值： 1

OrderExtraParam

订单额外参数

被如下接口引用：DescribeOrderList

名称	必选	允许NULL	类型	描述
DisposableStatus	否	是	Bool	一次性服务交付状态,仅一次性资源订单才有该值 false 未验收 true 已验收 示例值： true
Mode	否	是	String	PrePay 包年包月 PostPay 按量计费 Disposable 一次性交付 示例值： PrePay

LicenseDetail

授权订单列表对象

被如下接口引用：DescribeLicenseList

名称	必选	允许NULL	类型	描述
Alias	是	否	String	资源别名 示例值： redis_node_cvm
AutoRenewFlag	是	否	Uint64	0 初始化,1 自动续费,2 不自动续费 示例值： 0
BuyTime	是	否	String	购买时间 示例值： 2018-02-28 00:00:00
Deadline	是	否	String	截止日期 示例值： 2018-02-28 00:00:00
ExtraParam	否	是	LicenseExtraParam	额外参数 示例值：查看
FreezeNum	否	是	Int64	冻结数,当为0时 为未冻结,非0 则表示冻结授权数额 示例值： 0
LicenseCnt	是	否	Uint64	总授权数 示例值： 0
LicenseId	是	否	Uint64	授权ID 示例值： 1
LicenseStatus	是	是	Uint64	授权状态 0 未使用,1 部分使用, 2 已用完, 3 不可用 示例值： 0
LicenseType	是	否	Uint64	授权类型 0 专业版, 5 旗舰版 示例值： 0
OrderStatus	是	否	Uint64	订单状态 1 正常 2隔离, 3销毁 示例值： 1
ProjectId	是	否	Uint64	项目ID 示例值： 1
ResourceId	是	否	String	订单资源ID 示例值： 1c007adc2f0bb9f7c052860e2d3703fa
SourceType	是	否	Uint64	订单类型,0 默认计费订单 1 试用订单, 2 赠送 3 体验 示例值： 0
Tags	是	是	Array of Tags	平台标签 示例值：查看
TaskId	是	否	Uint64	任务ID ,默认0 ,查询绑定进度用 示例值： 1
UsedLicenseCnt	是	否	Uint64	已使用授权数 示例值： 0

VulInfoByCveId

根据cve_id查询漏洞详情

被如下接口引用：DescribeVulCveIdInfo

名称	必选	允许NULL	类型	描述
FixSwitch	是	否	Uint64	修复支持情况：0-Windows/Linux均不支持修复 ;1-Windows/Linux 均支持修复 ;2-仅Linux支持修复;3-仅Windows支持修复 示例值： 1
VulId	是	否	Uint64	漏洞id 示例值： 12

ClsLogsetInfo

cls日志集信息

被如下接口引用：DescribeClsLogsets

名称	必选	允许NULL	类型	描述
AssumerName	否	是	String	云产品标识 示例值： CWP
CreateTime	否	是	String	创建时间 示例值： 2021-04-01 08:00:00
LogsetId	否	是	String	日志集ID 示例值： 25425
LogsetName	否	是	String	日志集名称 示例值： redis_node_log
TopicCount	否	是	Uint64	日志主题总数 示例值： 10

RuleInfo

索引规则

被如下接口引用：DescribeLogIndex

名称	必选	允许NULL	类型	描述
FullText	是	否	FullTextInfo	全文索引的相关配置 示例值：查看
KeyValue	是	否	KeyValueInfo	键值索引的相关配置 示例值：查看
Tag	是	否	KeyValueInfo	元字段索引配置 示例值：查看

VulEventList

漏洞动态列表对象

被如下接口引用：DescribeEventList

名称	必选	允许NULL	类型	描述
AliasName	是	否	String	主机别名 示例值： redis_node_cvm
Descript	是	否	String	漏洞描述 示例值： 如果 Redis 以 root 权限启动且未授权访问，则会造成任意文件写入，最终导致命令执行漏洞。
HostIp	是	否	String	HostIp 示例值： 192.168.0.10
Id	是	否	Uint64	漏洞事件id 示例值： 1
IfProfession	是	否	Bool	是否为专业版防护 示例值： false
LastTime	是	否	String	最后检测时间 示例值： 2020-02-01 12:00:00
Level	是	否	Uint64	漏洞等级 1:低 2:中 3:高 4:提示 示例值： 1
Name	是	否	String	漏洞名称 示例值： Apache HTTP/2 协议拒绝服务漏洞(CVE-2023-44487)
PublishTime	是	否	String	漏洞披露时间 示例值： 2020-02-01 12:00:00
Quuid	是	否	String	主机quuid 示例值： 5a540076-d38a-4078-aa98-qwert371d322
Status	是	否	Uint64	事件状态:0: 待处理 1:忽略 3:已修复 5:检测中， 控制台仅处理0,1,3,5四种状态 示例值： 1
Uuid	是	否	String	Uuid 示例值： 5a540076-d38a-4078-aa98-qwert371d322
VulId	是	否	Uint64	漏洞id 示例值： 1

AssetType

资产指纹类型描述

被如下接口引用：DescribeAssetTypes

名称	必选	允许NULL	类型	描述
Id	是	否	Uint64	类型ID 示例值： 1
Name	是	否	String	类型名称 示例值： 账号

MaLabel

被如下接口引用：DescribeMaConnEventList、DescribeMaCustomPolicyList、DescribeMaHostList、DescribeMaLabel、DescribeMaLabelList、DescribeMaPodList、DescribeMaSelfLearnPolicyList、DescribeMaWorkloadLabel、DescribeMaWorkloadList、ModifyMaCustomPolicy、ModifyMaLabel

名称	必选	允许NULL	类型	描述
Id	否	是	Int64	标签ID 示例值： 1
Key	是	是	String	标签键 示例值： evn
Source	否	是	String	标签来源 • learn 自学习 • custom 用户自定义 • cwp 主机安全 • tcloud 云 示例值： learn
Value	是	是	String	标签值 示例值： ma
WorkloadCount	否	是	Int64	关联负载数 示例值： 10

VulDefencePluginDetail

单个进程漏洞防御插件状态

被如下接口引用：DescribeVulDefencePluginDetail

名称	必选	允许NULL	类型	描述
ErrorLog	是	否	String	错误日志 示例值： [Error] 注入失败
InjectLog	是	否	String	注入日志 示例值： [Info] 注入成功
MainClass	是	否	String	注入进程主类名 示例值： Main.class
Pid	是	否	Int64	注入进程Pid 示例值： 1

名称	必选	允许NULL	类型	描述
Status	是	否	Int64	插件状态：0: 注入中, 1: 注入成功, 2: 插件超时, 3: 插件退出, 4: 注入失败 5: 软删除 示例值： 2

HostRiskLevelCount

主机风险计数

被如下接口引用：DescribeBaselineHostRiskTop

名称	必选	允许NULL	类型	描述
HighCount	是	否	Int64	高危个数 示例值： 1
HostId	是	否	String	主机ID 示例值： 1
HostName	是	是	String	主机名 示例值： 1
LowCount	是	否	Int64	低危个数 示例值： 1
MediumCount	是	否	Int64	中危个数 示例值： 1
SeriousCount	是	否	Int64	严重个数 示例值： 1

LicenseUnBindRsp

授权解绑信息

被如下接口引用：ModifyLicenseUnBinds

名称	必选	允许NULL	类型	描述
ErrMsg	是	否	String	失败原因 示例值： 解绑次数不足
Quuid	是	否	String	服务器uuid 示例值： 93b5fa8f-f5bc-4cf9-8253-d2739e5aa484

MalwareInfo

恶意文件详情

被如下接口引用：DescribeMalwareInfo

名称	必选	允许NULL	类型	描述
Breadth	否	是	String	影响广度 // 暂时不提供 示例值： Breadth
CheckPlatform	否	是	String	木马检测平台用,分割 1云查杀引擎、2TAV、3binaryAi、4异常行为、5威胁情报 示例值： 1
CreateTime	否	否	String	首次发现时间 示例值： 2021-04-26 15:19:04
FileCreateTime	否	否	String	首次运行时间 示例值： 2021-04-26 15:19:04
FileExists	否	是	Bool	木马文件是否存在 示例值： true
FileModifierTime	否	否	String	最近一次运行时间 示例值： 2021-04-26 15:19:04
FileName	否	否	String	文件名称 示例值： FileName
FilePath	否	否	String	文件地址 示例值： /usr/local/services/tnginx_1_0_0-1.0/lib/luajit/lib
FileSize	否	否	Int64	文件大小 示例值： 1024
FirstDetectionMethod	否	是	Uint64	首次检出方式0扫描;1实时监控 示例值： 0
HarmDescribe	否	否	String	危害描述 示例值： 这是描述
Heat	否	是	String	查询热度 // 暂时不提供 示例值： Heat
HostIp	否	否	String	服务器IP 示例值： 15.2.3.442
Id	否	否	Uint64	唯一ID 示例值： 1
LatestScanTime	否	否	String	最近扫描时间 示例值： 2021-04-26 15:19:04
Level	否	是	Uint64	风险等级 0提示、1低、2中、3高、4严重 示例值： 1
MD5	否	否	String	文件MD5 示例值： e10adc3949ba59abbe56e057f20f883e
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineStatus	否	是	String	主机在线状态 OFFLINE ONLINE 示例值： OFFLINE
MachineWanIp	否	是	String	外网ip 示例值： 15.2.3.442
ModifyTime	否	是	String	最近修改时间 示例值： 2021-04-26 15:19:04
ProcessExists	否	是	Bool	木马进程是否存在 示例值： true
ProcessID	否	否	String	进程ID 示例值： 116
ProcessName	否	否	String	进程名称 示例值： nginx

名称	必选	允许NULL	类型	描述
PsTree	否	是	String	进程树 json pid:进程id，exe:文件路径 ，account:进程所属用组和用户 ,cmdline:执行命令，ssh_service: SSH服务ip, ssh_soure:登录源 示例值： [{"pid":"13"}]
Reference	否	否	String	参考链接 示例值： http://www.vxjump.net/files/virus_analysis/virut%20botnet%20anal
References	否	是	Array of String	参考链接 示例值： ["https://domain.com"]
ServersName	否	否	String	服务器名称 示例值： nginx
Status	否	是	Uint64	状态；4-待处理，5-已信任，6-已隔离 示例值： 1
StrFileAccessTime	否	是	String	最近访问时间 示例值： 2021-04-26 15:19:04
SuggestScheme	否	否	String	建议方案 示例值： 1.检查恶意进程及非法端口，删除可疑的启动项和定时任务； 2.隔离或者删除相关的木马文件；
Tags	否	否	Array of String	标签特性 示例值： ["tewt","wekk"]
Uuid	否	是	String	主机uuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
VirusName	否	否	String	病毒名称 示例值： Linux.Trojan.Downloader.Snkl

ScreenEmergentMsg

大屏可视化紧急通知

被如下接口引用：DescribeScreenEmergentMsg

名称	必选	允许NULL	类型	描述
Text	是	否	String	通知内容 示例值： 发现漏洞
Title	是	否	String	通知标签/标题 示例值： 紧急通知
Type	是	否	Uint64	跳转类型：0=漏洞管理 示例值： 0

BaselineWeakPassword

基线弱口令

被如下接口引用：DescribeBaselineWeakPasswordList、ModifyBaselineWeakPassword

名称	必选	允许NULL	类型	描述
CreateTime	否	否	String	创建时间 示例值： 2006-01-02 15:04:05
ModifyTime	否	否	String	修改时间 示例值： 2006-01-02 15:04:05
PasswordId	是	否	Int64	密码Id 示例值： 1002
WeakPassword	是	否	String	密码 示例值： passwd-01

OrderList

订单列表对象成员

被如下接口引用：DescribeOrderList

名称	必选	允许NULL	类型	描述
Alias	否	是	String	资源别名 示例值： redis_node_cvm
AutoRenewFlag	否	是	Uint64	自动续费标签 0 默认不自动续费(大客户特权会自动续费的) 1 自动续费 2 手动设置不自动续费(大客户特权不会自动续费) 示例值： 0
BeginTime	否	是	String	订单的开始时间 示例值： 0000-00-00 00:00:00
DealName	否	是	String	当前子订单号 示例值： name-anyone
EndTime	否	是	String	订单的结束时间 示例值： 0000-00-00 00:00:00
ExtraParam	否	是	OrderExtraParam	订单额外参数 示例值：查看
InquireKey	否	是	String	计费项四层 sv_ 示例值： sv_yunjing_ue_x
InquireNum	否	是	Uint64	资源购买量 示例值： 1
PayMode	否	是	Uint64	计费模式 0 后付费 1 预付费(包年包月) 示例值： 0
ProductCode	否	是	String	所属产品 p_ 示例值： p_azaz
ProjectID	否	是	Uint64	项目ID 示例值： 0
RegionID	否	是	Uint64	地域ID 示例值： 1
ResourceId	否	是	String	资源ID 示例值： any data
SourceType	否	是	Uint64	订单类型,0 默认计费订单 1 试用订单, 2 赠送 3 体验 示例值： 0
Status	否	是	Uint64	订单状态 1 正常 2隔离 3销毁 示例值： 1

名称	必选	允许NULL	类型	描述
SubProductCode	否	是	String	子产品 sp_ 示例值： sp_yunjing_0014
TagList	否	是	Array of Tags	云标签 示例值：查看
UsedNum	否	是	Uint64	资源用量 示例值： 0
ZoneID	否	是	Uint64	可用区ID 示例值： 100001

VulInfoList

主机安全-漏洞管理-漏洞列表

被如下接口引用：DescribeVulList

名称	必选	允许NULL	类型	描述
AttackLevel	否	是	Uint64	攻击热度级别，大于等于3为热点攻击 示例值： 1
CveId	是	是	String	cve编号 示例值： CVE-2021-3156
CvssScore	是	是	Float	CVSS评分 示例值： 9
DefenseAttackCount	是	是	Uint64	已防御的攻击次数 示例值： 12
Descript	是	是	String	描述信息 示例值： 漏洞描述
DescriptWisteria	是	是	String	废弃字段 示例值： 废弃字段
FirstAppearTime	是	是	String	首次出现时间 示例值： 2021-03-30 19:17:28
FixNoNeedRestart	否	是	Bool	漏洞修复后是否需要重启 示例值： true
FixSwitch	是	是	Uint64	是否能自动修复且包含能自动修复的主机， 0=否 1=是 示例值： 1
From	是	是	Uint64	废弃字段 示例值： 0
HostCount	是	否	Uint64	影响主机数 示例值： 2
Ids	是	否	String	漏洞包含的事件id串，多个用","分割 示例值： 1
IsSupportDefense	是	是	Uint64	是否支持防御， 0:不支持 1:支持 示例值： 1
Labels	是	是	String	漏洞标签 多个逗号分割 存在EXP:EXP 在野攻击:KNOWN_EXPLOITED 本地利用:LOCAL 必修漏洞:NEED_FIX 远程利用:NETWORK 存在POC:POC 系统重启:RESTART 示例值： LOCAL,NETWORK
LastTime	是	否	String	最后检测时间 示例值： 2021-03-16 16:21:51
Level	是	否	Uint64	漏洞等级 1:低 2:中 3:高 4:严重 示例值： 1
Method	否	是	Uint64	检测方式0 - 版本比对, 1 - POC验证 示例值： 1
Name	是	否	String	漏洞名 示例值： Apache HTTP/2 协议拒绝服务漏洞(CVE-2023-44487)
NameWisteria	是	是	String	废弃字段 示例值： 废弃字段
PublishTime	是	否	String	漏洞披露事件 示例值： 2021-03-16 16:21:51
PublishTimeWisteria	是	是	String	废弃字段 示例值： 废弃字段
Status	是	否	Uint64	0: 待处理 1:忽略 3:已修复 5:检测中 6:修复中 8:修复失败 示例值： 1
StatusStr	是	是	String	聚合后事件状态串 示例值： 1,2
TaskId	是	是	Uint64	最后扫描任务的id 示例值： 12
VulCategory	是	是	Uint64	漏洞类别 1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 示例值： 1
VulFixSwitch	否	是	Uint64	漏洞是否支持修复 0不支持，1支持 示例值： 1
VulId	是	否	Uint64	漏洞id 示例值： 1

ScreenTrendsChart

大屏攻防趋势图

被如下接口引用：DescribeScreenDefenseTrends

名称	必选	允许NULL	类型	描述
Type	是	否	String	统计分类类型 值：防御次数，攻击次数 示例值： 防御次数
X	是	否	String	X轴 时间 示例值： 2021-03-30 19:17:28

名称	必选	允许NULL	类型	描述
Y	是	否	Uint64	Y轴 数值 示例值： 12

SecurityEventInfo

安全事件统计列表

被如下接口引用：DescribeSecurityEventsCnt

名称	必选	允许NULL	类型	描述
EventCnt	是	否	Uint64	安全事件数 示例值： 37
UuidCnt	是	否	Uint64	受影响机器数 示例值： 6

RansomDefenseEvent

防勒索诱饵篡改事件

被如下接口引用：DescribeRansomDefenseEventsList

名称	必选	允许NULL	类型	描述
BaitFilePath	是	否	String	被篡改文件路径 示例值： /var/www/index.html
CreateTime	是	否	String	事件发送时间 示例值： 2024-10-30 09:12:21
FileMd5	是	否	String	恶意文件md5 示例值： 708cae4cf814c3deda4208da228fad4e
FilePath	是	否	String	恶意文件路径 示例值： /tmp/any
FileSize	是	否	Uint64	恶意文件大小 示例值： 1
HostIp	是	否	String	主机外网ip 示例值： 10.0.0.1
HostName	是	否	String	主机名称 示例值： redis_node_cvm
Id	是	否	Uint64	事件id 示例值： 1
InstanceId	是	否	String	cvm 实例id 示例值： ins-eubxdt5
ModifyTime	是	否	String	事件修改事件 示例值： 2024-10-30 09:12:21
Pid	是	否	Uint64	恶意进程id 示例值： 1
PidParam	是	否	String	恶意进程参数 示例值： bash -c echo "Csip data any" >> /home/.yjfile/121hcXh.doc ayay
ProcessStartTime	是	否	String	进程启动时间 示例值： 2024-10-30 09:12:21
PsTree	是	否	String	进程树 base64 json 示例值： W3sicGlkIjozMjI1NCwiZXhlIjoiL3Vzci9iaW*
Quuid	是	否	String	cvm uuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
SnapshotNum	是	否	Uint64	主机拥有快照备份数 示例值： 1
Status	是	否	Uint64	事件状态 0待处理，1已处理，2已信任，3处理中，4已恢复备份 示例值： 1
StrategyId	是	否	Uint64	策略id 示例值： 1
StrategyName	是	否	String	策略名称 示例值： anyname
Type	是	否	Uint64	事件类型：0加密勒索，1文件篡改 示例值： 0
Uuid	是	否	String	主机uuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
WanIp	是	否	String	主机内网ip 示例值： 10.0.0.1

Strategy

基线安全用户策略信息

被如下接口引用：DescribeBaselineStrategyList

名称	必选	允许NULL	类型	描述
CategoryIds	是	是	String	基线id 示例值： 1
Enabled	是	是	Uint64	是否可用 示例值： 1
HostCount	是	是	Uint64	主机数量 示例值： 42
IsDefault	是	是	Uint64	是否默认策略 示例值： 0
PassRate	是	是	Uint64	通过率 示例值： 100
RuleCount	是	是	Uint64	基线检测项总数 示例值： 9
ScanAt	是	是	String	扫描时间 示例值： 01:35:30
ScanCycle	是	是	Uint64	扫描周期 示例值： 7

名称	必选	允许NULL	类型	描述
StrategyId	是	是	Uint64	策略id 示例值： 1089429
StrategyName	是	是	String	策略名 示例值： check_redis_node

MalwareWhiteListAffectEvent

木马白名单影响事件信息

被如下接口引用：DescribeMalwareWhiteListAffectList

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	添加时间 示例值： 2024-10-30 09:12:21
FilePath	是	否	String	文件路径 示例值： /tmp/any
HostIp	是	否	String	主机ip 示例值： 10.0.0.1
Id	是	否	Uint64	唯一ID。 示例值： 1
Md5	是	否	String	影响的md5 示例值： 708cae4cf814c3deda4208da228fad4e

AssetWebLocationBaseInfo

资产管理Web站点列表信息

被如下接口引用：DescribeAssetWebLocationList

名称	必选	允许NULL	类型	描述
FirstTime	否	否	String	首次采集时间 示例值： 2022-07-15 11:27:01
Id	否	否	String	Web站点Id 示例值： 1
IsNew	否	是	Int64	是否新增[0:否
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	否	String	内网IP 示例值： 10.0.11
MachineName	否	否	String	主机名称 示例值： any-ins
MachineWanIp	否	否	String	外网IP 示例值： 112.54.121.11
MainPath	否	否	String	主目录 示例值： /root
MainPathOwner	否	否	String	主目录所有者 示例值： 1
Name	否	否	String	域名 示例值： any.com
OsInfo	否	否	String	操作系统 示例值： centos 64bit
PathCount	否	否	Uint64	站点路经数 示例值： 1
Permission	否	否	String	拥有者权限 示例值： 1
Port	否	否	String	站点端口 示例值： 22
ProjectId	否	否	Uint64	主机业务组ID 示例值： 1
Proto	否	否	String	站点协议 示例值： http
Quuid	否	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
ServiceType	否	否	String	服务类型（Tomcat/Apache/Nginx/WebLogic/Websphere/JBoss/Jetty/IHS/Tengine） 示例值： Tomcat
Tag	否	否	Array of MachineTag	主机标签 示例值：查看
UpdateTime	否	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
User	否	否	String	运行用户 示例值： root
Uuid	否	否	String	主机Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

BaselinePolicyDetect

基线检测策略

被如下接口引用：DescribeBaselineDetectList

名称	必选	允许NULL	类型	描述
FailedCount	是	否	Int64	失败主机数 示例值： 1
FinishTime	是	否	String	结束时间 示例值： 2021-02-01 12:00:00
HostCount	是	否	Int64	关联主机数 示例值： 52
PolicyDetectStatus	是	是	Int64	1:检测中 2:检测完成 示例值： 1

名称	必选	允许NULL	类型	描述
PolicyId	是	否	Int64	策略Id 示例值： 1523
PolicyName	是	否	String	策略名称 示例值： 未授权访问
StartTime	是	否	String	开始时间 示例值： 2021-02-01 12:00:00
SuccessCount	是	否	Int64	成功主机数 示例值： 1
TaskId	是	否	Int64	检测任务Id 示例值： 38644956
TimeoutCount	是	否	Int64	失败主机数 示例值： 1

BaselineRuleTopInfo

基线检测项TOP信息

被如下接口引用：DescribeBaselineTop

名称	必选	允许NULL	类型	描述
EventCount	是	是	Uint64	事件总数 示例值： 0
Level	是	是	Uint64	基线风险等级：0低危 1中危 2高危 3严重 示例值： 1
RuleId	是	是	Uint64	检测项id 示例值： 20
RuleName	是	是	String	基线检测项名 示例值： 弱口令

ScreenVulInfo

大屏漏洞列表

被如下接口引用：DescribeScreenHostInvasion

名称	必选	允许NULL	类型	描述
Category	是	是	Uint64	漏洞类型 1: web-cms漏洞, 2:应用漏洞, 4: Linux软件漏洞, 5: Windows系统漏洞 示例值： 1
Id	是	否	Uint64	漏洞事件id 示例值： 1
LastTime	是	否	String	最后检测时间 示例值： 2021-03-16 16:21:51
Level	是	否	Uint64	漏洞等级 1:低 2:中 3:高 4:提示 示例值： 1
Name	是	否	String	漏洞名 示例值： git注入
Uuid	是	是	String	主机UUID 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
VulId	是	否	Uint64	漏洞id 示例值： 1

AssetJarBaseInfo

资产管理jar包列表

被如下接口引用：DescribeAssetJarList

名称	必选	允许NULL	类型	描述
FirstTime	否	否	String	首次采集时间 示例值： 2022-07-15 11:27:01
Id	否	否	String	Jar包ID 示例值： 1024
IsNew	否	否	Int64	是否新增[0:否
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	否	String	服务器IP 示例值： 10.0.0.11
MachineName	否	否	String	服务器名称 示例值： any-instance
MachineWanIp	否	否	String	服务器外网IP 示例值： 1.1.1.1
Md5	否	否	String	Jar包Md5 示例值： fc702c8398071ea3697d449c2b894dae
Name	否	否	String	名称 示例值： com.apple.util
OsInfo	否	否	String	操作系统 示例值： centos 64bit
Path	否	否	String	路径 示例值： /root
Quuid	否	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Status	否	否	Uint64	是否可执行：0未知，1是，2否 示例值： 1
Type	否	否	Int64	类型：1应用程序，2系统类库，3Web服务自带库，8:其他， 示例值： 1
UpdateTime	否	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
Uuid	否	否	String	主机uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

名称	必选	允许NULL	类型	描述
Version	否	否	String	版本 示例值： 1.0.1

LicenseOrder

授权订单对象内容

被如下接口引用：DescribeImportMachineInfo、DescribeMachinesSimple

名称	必选	允许NULL	类型	描述
LicenseId	是	否	Uint64	授权ID 示例值： 667445
LicenseType	是	否	Uint64	授权类型 0 专业版, 5 旗舰版 示例值： 1
ResourceId	是	否	String	资源ID 示例值： resource_id
SourceType	是	否	Uint64	订单类型,0 默认计费订单 1 试用订单, 2 赠送 3 体验 示例值： 0
Status	是	否	Uint64	授权订单资源状态 1 正常、2 隔离、3 销毁 示例值： 1

AssetScanTaskHostDetail

描述资产扫描任务中各个主机的任务状态

被如下接口引用：DescribeAssetScanTaskDetail

名称	必选	允许NULL	类型	描述
ErrorMessage	是	否	String	异常信息 示例值： some message
MachineIp	是	否	String	主机IP 示例值： 192.168.0.1
MachineName	是	否	String	主机名称 示例值： redis_node_cvm
Quuid	是	否	String	主机Quuid 示例值： 5a540076-d38a-4078-aa98-qwert371d322
Status	是	否	Uint64	任务状态：0进行中，1成功，2失败 示例值： 1

ExportInfo

日志下载任务列表

被如下接口引用：DescribeLogExports

名称	必选	允许NULL	类型	描述
CosPath	是	否	String	日志导出路径 示例值： /tmp/data/
Count	是	否	Int64	日志导出数量 示例值： 12
CreateTime	是	否	String	日志导出创建时间 示例值： 2021-02-01 12:00:00
EndTime	是	否	Int64	日志导出结束时间，uinx毫秒时间戳 示例值： 0
ExportId	是	否	String	日志导出任务ID 示例值： export-d0ef1b2c-64f6-4193-b251-e583a810ayay
FileName	是	否	String	日志导出文件名 示例值： fielaName.txt
FileSize	是	否	Int64	日志文件大小 示例值： 0
Format	是	否	String	日志导出格式 示例值： json
Order	是	否	String	日志导出时间排序 示例值： desc
Query	是	否	String	日志导出查询语句 示例值： dev
StartTime	是	否	Int64	日志导出起始时间，uinx毫秒时间戳 示例值： 0
Status	是	否	String	日志下载状态。Processing:导出正在进行中，Complete:导出完成，Failed:导出失败，Expired:日志导出已过期（三天有效期）。 示例值： Complete

IgnoreRuleEffectHostInfo

忽略检测项影响主机信息

被如下接口引用：DescribeIgnoreRuleEffectHostList

名称	必选	允许NULL	类型	描述
EventId	是	是	Uint64	事件id 示例值： 1
HostName	是	是	String	主机名称 示例值： redis_node_cvm
LastScanTime	是	是	String	最后检测时间 示例值： 2021-11-10 00:00:00
Level	是	是	Uint64	危害等级：1-低位，2-中危，3-高危，4-严重 示例值： 1
Quuid	是	是	String	主机quuid 示例值： 935e27b1-d675-4509-80bf-96fbf0764237
Status	是	是	Uint64	状态：0-未通过，1-忽略，3-已通过，5-检测中 示例值： 0

名称	必选	允许NULL	类型	描述
TagList	是	是	Array of String	主机标签数组 示例值： ["tag-01"]

VulTopInfo

漏洞top统计实体

被如下接口引用：DescribeVulTop

名称	必选	允许NULL	类型	描述
VulCategory	否	是	Uint64	1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 0= 应急漏洞 示例值： 2
VulCount	是	是	Uint64	漏洞数量 示例值： 82
VulId	是	是	Uint64	漏洞id 示例值： 104994
VulLevel	是	是	Uint64	危害等级：1-低危；2-中危；3-高危；4-严重 示例值： 3
VulName	是	是	String	漏洞 名 示例值： Apache HTTP/2 协议拒绝服务漏洞(CVE-2023-44487)

RiskDnsEvent

恶意请求事件

被如下接口引用：DescribeRiskDnsEventInfo、DescribeRiskDnsEventList

名称	必选	允许NULL	类型	描述
AccessCount	否	否	Int64	访问次数 示例值： 10
AgentId	否	否	String	客户端ID 示例值： a1f53e38-3f03-4a72-bf16-afa78dd698f3
CmdLine	否	否	String	命令行 示例值： cmd
Domain	否	否	String	访问域名 示例值： re.r3r3.org
FirstTime	否	否	String	首次访问时间 示例值： 2021-04-26 15:19:04
HandleStatus	否	否	Int64	处理状态；[0:待处理
HostId	否	否	String	主机ID 示例值： d1f53e38-3f03-4a72-bf16-afa78ed698f2
HostIp	否	否	String	主机IP 示例值： 10.0.0.1
HostName	否	否	String	主机名称 示例值： security-data-seayay
HostStatus	否	否	String	主机在线状态[OFFLINE:离线
Id	否	否	Int64	事件Id 示例值： 153
LastTime	否	否	String	最近访问时间 示例值： 2022-07-15 11:27:01
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
OsType	否	是	Int64	[1:CentOS
Pid	否	否	Int64	进程ID 示例值： 1
PolicyId	否	否	Int64	策略ID 示例值： 10000
PolicyName	否	否	String	命中策略名称 示例值： 系统规则(标准)
PolicyType	否	否	Int64	命中策略类型[-1:未知
ProcessMd5	否	否	String	进程MD5 示例值： 3c59dc048e8850243be8079a5c74d079
ProcessName	否	否	String	进程名 示例值： bash
ProtectLevel	否	否	Int64	保护级别[0:基础版
ReferenceLink	否	否	String	参考链接 示例值： http://www.vxjump.net/files/virus_analysis/virut%20botnet%20anal
SuggestSolution	否	否	String	修复方案 示例值： 1.检查恶意进程及非法端口，删除可疑的启动项和定时任务； 2.隔离或者删除相关的木马文件；
Tags	否	否	Array of String	标签特性 示例值： ["vueir","mle"]
ThreatDesc	否	否	String	威胁描述 示例值： 发现主机存在访问恶意IP/域名的行为，您的主机可能已经失陷。\n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。
WanIp	否	否	String	外网IP 示例值： 13.22.3.1

RansomDefenseRollbackTask

防勒索回滚任务

被如下接口引用：DescribeRansomDefenseRollBackTaskList

名称	必选	允许NULL	类型	描述
BackupTime	是	否	String	快照时间 示例值： 2022-11-11 11:00:00
CreateTime	是	否	String	操作时间 示例值： 2022-11-11 11:00:00

名称	必选	允许NULL	类型	描述
Disks	是	否	String	硬盘id列表，;分隔 示例值： dsk-dsdsds;dsk-dssds
Id	是	否	Uint64	任务ID 示例值： 1
MachineName	是	否	String	主机名称 示例值： redis_node_cvm
ModifyTime	是	否	String	Status!=0时为完成时间 示例值： 2022-11-11 11:00:00
Quuid	是	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
RegionInfo	是	否	RegionInfo	可用区信息 示例值：查看
Status	是	否	Uint64	回滚任务状态：0进行中，1成功，2失败 示例值： 1
Uuid	是	否	String	主机Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

VulEmergentMsgInfo

紧急通知实体

被如下接口引用：DescribeVulEmergentMsg

名称	必选	允许NULL	类型	描述
Name	是	否	String	漏洞名 示例值： Apache HTTP/2 协议拒绝服务漏洞(CVE-2023-44487)
NameEn	否	否	String	英文漏洞名 示例值： Apache HTTP/2 DoS vulnerability (CVE-2023-44487)
PublishTime	是	否	String	漏洞纰漏时间 示例值： 2021-02-01 12:00:00
VulId	是	否	Uint64	漏洞id 示例值： 105375

HostLoginWhiteObj

新增登录审计白名单实体

被如下接口引用：AddLoginWhiteLists

名称	必选	允许NULL	类型	描述
EndTime	否	否	String	结束时间 示例值： 2024-11-03 18:37:03
HostInfos	是	否	Array of HostInfo	白名单生效的机器信息列表 示例值：查看
IsGlobal	是	否	Uint64	是否对全局生效, 1：全局有效 0: 仅针对单台主机' 示例值： False
Places	否	否	Array of Place	加白地域 示例值：查看
Remark	否	否	String	备注 示例值： 内部使用
SrcIp	是	否	String	加白源IP，支持网段，多个IP以逗号隔开 示例值： 10.0.1.11
StartTime	否	否	String	开始时间 示例值： 2024-11-03 18:37:03
UserName	是	否	String	加白用户名，多个用户名以逗号隔开 示例值： root

VulLevelCountInfo

漏洞等级数量实体

被如下接口引用：DescribeVulHostTop

名称	必选	允许NULL	类型	描述
VulCount	是	否	Uint64	漏洞数量 示例值： 10
VulLevel	是	否	Uint64	漏洞等级 1:低 2:中 3:高 4:严重 示例值： 3

BashRule

高危命令规则

被如下接口引用：DescribeBashRules

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	创建时间 示例值： 2021-03-30 19:17:28
DealOldEvents	是	是	Uint64	是否处理之前的事件 0: 不处理 1:处理 示例值： 0
Decription	是	否	String	规则描述 示例值： 192.168.0.1
Description	否	是	String	规则描述 示例值： desc of rule
Hostip	是	否	String	主机IP 示例值： 172.27.16.14
Id	是	否	Uint64	规则ID 示例值： 10003
IsGlobal	是	否	Uint64	是否全局规则 示例值： 0

名称	必选	允许NULL	类型	描述
Level	是	否	Uint64	危险等级(0 ：无 1: 高危 2:中危 3: 低危) 示例值： 1
ModifyTime	是	否	String	修改时间 示例值： 2021-03-30 19:17:28
Name	是	否	String	规则名称 示例值： redis_node_use
Operator	是	否	String	操作人 示例值： admin
Rule	是	否	String	正则表达式 示例值： vim
Status	是	否	Uint64	状态 (0: 有效 1: 无效) 示例值： 0
Uuid	是	否	String	客户端ID 示例值： 451f36cf-ac23-4635-bb96-23cd721b4b25
Uuids	是	是	Array of String	生效服务器的uuid数组 示例值： ["451f36cf-ac23-4635-bb96-23cd721b4b25"]
White	是	是	Uint64	0=黑名单 1=白名单 示例值： 1

OsName

操作系统名称

被如下接口引用：DescribeMachineOsList

名称	必选	允许NULL	类型	描述
MachineOSType	是	否	Uint64	操作系统类型： 1 CentOS、2 Debian、3 Gentoo、4 Redhat、5 Ubantu、6 WindowsServer、7 TOS、8 CoreOS、9 FreeBSD、10 SUSE、11 AliYunLinux、12 OpenCloud 示例值： 1
Name	是	否	String	系统名称 示例值： Linux

VersionWhiteConfig

授权版本白名单配置信息

被如下接口引用：DescribeLicenseWhiteConfig

名称	必选	允许NULL	类型	描述
Deadline	是	否	Uint64	到期天数 示例值： 7
IsApplyFor	是	否	Bool	是否可申请 示例值： false
LicenseNum	是	否	Uint64	授权数量 示例值： 10
SourceType	是	否	Uint64	订单类型,0 默认计费订单 1 试用订单, 2 赠送 3 体验 示例值： 0

ReverseShellRuleAggregation

反弹Shell规则-聚合版本

被如下接口引用：DescribeReverseShellRulesAggregation

名称	必选	允许NULL	类型	描述
CreateTime	否	是	String	创建时间 示例值： 2020-10-01 00:00:00
DestIp	否	是	String	目标IP 示例值： 1.2.3.4
DestPort	否	是	String	目标端口 示例值： 80
GroupID	否	是	String	批次id 示例值： 1
HandleHistory	否	是	Uint64	处理历史事件， 0:不处理 1:处理 示例值： 0
Id	否	是	Uint64	规则ID 示例值： 1
IsGlobal	否	是	Uint64	是否全局规则 示例值： 1
MachinesNums	否	是	String	应用资产，描述服务器数量，全局时候为：全部服务器 示例值： 12
ModifyTime	否	是	String	修改时间 示例值： 2020-10-01 00:00:00
Operator	否	是	String	操作人 示例值： opt1
ProcessName	否	是	String	进程名称 示例值： /etc/sshd
RuleRegexp	否	是	String	正则表达式(base64编码) 示例值： c2ggcmVkaXMuc2g=
Status	否	是	Uint64	状态 (0: 有效 1: 无效) 示例值： 0
UuidHostips	否	是	Array of UuidHostip	客户端ID 示例值：查看
WhiteType	否	是	Uint64	加白方式， 0:常规加白 1:正则加白 示例值： 1

CommandLine

命令行内容

被如下接口引用：CheckBashPolicyParams、DescribeBashPolicies、ModifyBashPolicy

名称	必选	允许NULL	类型	描述
Cmdline	否	是	String	命令行,需要base64加密 示例值： c2ggcmVkaXMuc2g=
Exe	否	是	String	路径,需要base64加密 示例值： L2RhdGEvZGlybmFtZS8=

DuplicateHosts

批量添加白名单：重复情况重复列表实体

被如下接口引用：AddLoginWhiteLists、CreateBanWhiteList

名称	必选	允许NULL	类型	描述
Id	是	否	Uint64	Id 示例值： 1
Quuid	是	是	String	Quuid 示例值： 05f0bcab-726c-4ea4-8109-bcd03d5598f7
Uuid	是	是	String	Uuid 示例值： 05f0bcab-726c-4ea4-8109-bcd03d5598f7

BruteAttackInfo

密码破解列表实体

被如下接口引用：DescribeBruteAttackList

名称	必选	允许NULL	类型	描述
AttackStatusDesc	否	是	String	破解状态说明 示例值： fail
BanExpiredTime	否	是	String	阻断过期时间（仅阻断中事件有效） 示例值： 2024-10-30 15:58:43
BanStatus	否	是	Uint64	0 -不阻断(客户端版本不支持) 1 -已阻断 2 -阻断失败(程序异常) 3 -不阻断(内网不阻断) 4 -可用区不支持阻断 10-阻断中 81-不阻断(未开启阻断) 82-不阻断(非专业版) 83-不阻断(已加白名单) 86-不阻断(系统白名单) 87-不阻断(客户端离线) 88-不阻断(来源Ip归属相同客户) 89-不阻断(ipv6不支持阻断) 示例值： 0
City	否	是	Uint64	城市id 示例值： 1
Count	否	是	Uint64	发生次数 示例值： 2
Country	否	是	Uint64	国家id 示例值： 1
CreateTime	否	是	String	创建时间 示例值： 2021-05-25 12:01:50
DataFrom	否	是	Int64	事件来源：0--阻断规则，1--威胁情报 示例值： 0
DataStatus	否	是	Uint64	0：待处理，1：忽略，5：已处理，6：加入白名单 示例值： 1
EventType	否	是	Uint64	事件类型：200-暴力破解事件，300-暴力破解成功事件（页面展示），400-暴力破解不存在的账号事件 示例值： 1
Id	否	否	Uint64	唯一Id 示例值： 1001
InstanceId	否	是	String	实例ID 示例值： ins-fsfsaw
IsProVersion	否	是	Bool	是否为专业版（true/false） 示例值： false
Location	否	是	String	地理位置名字 示例值： location1:location2:location3
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	是	String	主机ip 示例值： 127.0.0.1
MachineName	否	是	String	主机名 示例值： redis_node_cvm
ModifyTime	否	是	String	最近攻击时间 示例值： 2021-05-25 12:01:50
Port	否	是	Uint64	端口 示例值： 22
Protocol	否	是	String	被攻击的服务的用户名 示例值： ssh/rdp
Province	否	是	Uint64	省份id 示例值： 1
Quuid	否	是	String	机器UUID 示例值： 380add75-bb06-4cc4-84c5-cf806d102fba
RiskLevel	否	是	Uint64	威胁等级：0低危，1中危，2高危 示例值： 1
SrcIp	否	是	String	来源ip 示例值： 66.12.2.14
Status	否	是	String	SUCCESS：破解成功；FAILED：破解失败 示例值： FAILED
UserName	否	是	String	用户名 示例值： root
Uuid	否	是	String	主机安全客户端唯一标识UUID 示例值： 380add75-bb06-4cc4-84c5-cf806d102fba

BaselineCustomRuleIdName

基线自定规则ID和名字

被如下接口引用：DescribeBaselineItemIgnoreList、DescribeBaselineItemInfo、DescribeIgnoreHostAndItemConfig

名称	必选	允许NULL	类型	描述
RuleId	是	是	Int64	自定义规则ID 示例值： 1
RuleName	是	是	String	自定义规则名字 示例值： 自定义

BashEventNew

高危命令数据(新)

被如下接口引用：DescribeBashEventsNew

名称	必选	允许NULL	类型	描述
BashCmd	否	否	String	执行命令 示例值： rm
CreateTime	否	否	String	发生时间 示例值： 2021-03-30 19:17:28
DetectBy	否	是	Uint64	0: bash日志 1: 实时监控(雷霆版) 示例值： 1
Exe	否	是	String	进程名称 示例值： 1.exe
HostIp	否	否	String	主机内网IP 示例值： 127.0.0.1
Id	否	否	Uint64	数据ID 示例值： 1
MachineExtraInfo	否	是	MachineExtraInfo	机器额外信息 示例值：查看
MachineName	否	否	String	主机名 示例值： redis_node_cvm
MachineType	否	是	Int64	0:普通 1:专业版 2:旗舰版 示例值： 1
ModifyTime	否	是	String	处理时间 示例值： 2021-03-30 19:17:28
Pid	否	是	String	进程id 示例值： 1
Platform	否	否	Uint64	平台类型 示例值： 1
Quuid	否	否	String	主机ID 示例值： dadasda
RegexBashCmd	否	是	String	转义后的正则表达式 示例值： rm -rf /tmp/t*
RuleCategory	否	是	Uint64	规则类别 0=系统规则，1=用户规则 示例值： 0
RuleId	否	否	Uint64	规则ID 示例值： 1
RuleLevel	否	否	Uint64	规则等级：1-高 2-中 3-低 示例值： 1
RuleName	否	否	String	规则名称 示例值： 1
Status	否	否	Uint64	处理状态： 0 = 待处理 1= 已处理, 2 = 已加白， 3 = 已忽略 示例值： 1
User	否	否	String	执行用户名 示例值： root
Uuid	否	否	String	主机安全ID 示例值： 5a540076-d38a-4078-aa98-q45rt371d322

PriceDetail

询价参数

被如下接口引用：DescribePrice

名称	必选	允许NULL	类型	描述
GoodsCategoryId	是	否	Uint64	订单分类 示例值： 1
GoodsDetail	是	否	String	订单详情参数 示例值： {"pid":1004928,"license":1,"productCode":"p_yunjing","subProductCode":"sp_yunjing_vip","sv_yunjing_protection_vip":"3","timeSpan":1,"timeUnit":"d","yunjing_pro":1}
GoodsNum	是	否	Uint64	订单数 示例值： 1
PayMode	是	否	Uint64	费用模式 0 后付费,1 预付费 示例值： 1
RegionId	是	否	Uint64	地域 示例值： 1
ZoneId	是	否	Uint64	可用区 示例值： 1

ScreenAttackHotspot

大屏全网攻击热点

被如下接口引用：DescribeScreenAttackHotspot

名称	必选	允许NULL	类型	描述
CreatedTime	是	否	String	时间 示例值： 2021-03-30
DstIp	是	否	String	受害者IP 示例值： 12.23.212.2

名称	必选	允许NULL	类型	描述
EventName	是	否	String	事件名 示例值： 命令注入攻击
Region	是	否	String	地域 示例值： region1
SrcIp	是	否	String	攻击者IP 示例值： 12.23.212.2

HistoryAccount

账号变更历史数据。

被如下接口引用：DescribeHistoryAccounts

名称	必选	允许NULL	类型	描述
Id	是	否	Uint64	唯一ID。 示例值： 1
MachineIp	是	否	String	主机内网IP。 示例值： 1.2.3.4
MachineName	是	否	String	主机名。 示例值： stone
ModifyTime	是	否	Datetime	变更时间。 示例值： 2020-01-01 01:01:01
ModifyType	是	否	String	账号变更类型。 • CREATE：表示新增账号 • MODIFY：表示修改账号 • DELETE：表示删除账号 示例值： CREATE
Username	是	否	String	账号名。 示例值： user1
Uuid	是	否	String	主机安全客户端唯一Uuid。 示例值： 8c09e1b1-5611-45b3-9c02-737996011b81

RiskDnsPolicy

恶意请求策略

被如下接口引用：DescribeRiskDnsPolicyList、ModifyRiskDnsPolicy

名称	必选	允许NULL	类型	描述
Domains	是	否	Array of String	域名,作为入参时需要进行base64 encode 示例值： [domainName1,domainName2]
EventId	否	否	Int64	事件ID 示例值： 1
HostIds	是	否	Array of String	主机ID 示例值： [a7c573cb-c228-4211-85e3-64e000f159a5]
HostScope	是	否	Int64	主机范围[1: 所有专业版+旗舰版
IsDealOldEvent	否	否	Int64	是否处理之前的事件[0:不处理
IsEnabled	是	否	Int64	是否生效[0:生效,1:不生效] 示例值： 1
PolicyAction	是	否	Int64	策略动作[0:告警,1:放行,2:拦截+告警] 示例值： 1
PolicyDesc	否	否	String	策略描述 示例值： add for nginx web cvm
PolicyId	否	否	Int64	策略ID 示例值： 1
PolicyName	是	否	String	策略名称 示例值： for_nginx_web
PolicyType	是	否	Int64	策略类型[0:系统,1:用户] 示例值： 1
UpdateTime	否	否	String	更新时间 示例值： 2022-07-15 11:27:01

VulFixStatusSnapshotInfo

机器快照信息

被如下接口引用：DescribeVulFixStatus

名称	必选	允许NULL	类型	描述
FailReason	是	是	String	快照创建失败原因 示例值： 获取授权失败
HostIp	是	是	String	主机ip 示例值： 145.12.3.12
HostName	是	是	String	主机名称 示例值： redis_node_cvm
Id	是	否	Uint64	记录唯一id 示例值： 12
ModifyTime	是	是	String	快照创建时间 示例值： 2021-03-11 18:15:17
Quuid	是	否	String	cvm id 示例值： 380add75-bb06-4cc4-84c5-cf806d102fba
SnapshotId	是	是	String	快照id 示例值： snp-dhusaay
SnapshotName	是	是	String	快照名称 示例值： 2021-03-01备份
Status	是	否	Uint64	快照状态 0-初始状态1-快照创建成功；2-快照创建失败； 示例值： 1

AssetUserBaseInfo

资源管理账号基本信息

被如下接口引用：DescribeAssetUserList

名称	必选	允许NULL	类型	描述
FirstTime	否	否	String	首次采集时间 示例值： 2011-11-11 12:12:12
Gid	否	否	String	账号GID 示例值： 16
HomePath	否	否	String	Home目录 示例值： /var/lib/oprofile
IsDomain	否	否	Uint64	是否域账号：0否， 1是，2否, 999为空 仅Windows 示例值： 1
IsNew	否	否	Int64	是否新增[0:否
IsRoot	否	否	Uint64	是否有root权限：0-否；1是，999为空: 仅linux 示例值： 1
IsSshLogin	否	否	Uint64	是否允许ssh登录，1是，0否, 999为空, 仅linux 示例值： 1
IsSudo	否	否	Uint64	是否有sudo权限，1是，0否, 999为空, 仅linux 示例值： 1
LastLoginTime	否	否	String	上次登录时间 示例值： 1
LoginType	否	否	Uint64	登录方式：0-不可登录；1-只允许key登录；2只允许密码登录；3-允许key和密码，999为空，仅linux 示例值： 1
MachineExtraInfo	否	是	MachineExtraInfo	主机信息 示例值：查看
MachineIp	否	否	String	主机内网IP 示例值： 10.0.0.11
MachineName	否	否	String	主机名称 示例值： redis_node_cvm
MachineWanIp	否	否	String	主机外网IP 示例值： 112.65.22.19
Name	否	否	String	账号名称 示例值： admin
OsInfo	否	否	String	操作系统信息 示例值： Centos 64bit
PasswordChangeTime	否	否	String	密码修改时间 示例值： 2024-10-22 19:40:38
PasswordDueTime	否	否	String	密码过期时间 仅linux 示例值： 2024-10-22 19:40:38
PasswordLockDays	否	否	Int64	密码锁定时间：单位天, -1为永不锁定 999为空，仅linux 示例值： 1
PasswordStatus	否	否	Int64	密码状态：1正常 2即将过期 3已过期 4已锁定 999为空 仅linux 示例值： 1
ProjectId	否	否	Uint64	主机业务组ID 示例值： 1
Quuid	否	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Shell	否	否	String	Shell路径 仅linux 示例值： /bin/bash
ShellLoginStatus	否	否	Uint64	是否shell登录性，0不是；1是 仅linux 示例值： 1
Status	否	否	Uint64	账号状态：0-禁用；1-启用 示例值： 1
Uid	否	否	String	账号UID 示例值： 16
UpdateTime	否	是	String	更新时间 示例值： 2011-11-11 12:12:12
UserType	否	否	Uint64	账号类型：0访客用户，1标准用户，2管理员用户 ,999为空,仅Windows 示例值： 1
Uuid	否	否	String	主机Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

ScreenBaselineInfo

大屏基线信息

被如下接口引用：DescribeScreenHostInvasion

名称	必选	允许NULL	类型	描述
BaselineFailCount	是	是	Uint64	基线风险项 示例值： 23
CategoryId	是	是	Uint64	基线id 示例值： 12
LastScanTime	是	是	String	最后检测时间 示例值： 2021-03-30 19:17:28
Level	是	是	Uint64	危害等级：1-低危；2-中危；3-高危；4-严重 示例值： 1
Name	是	是	String	基线名 示例值： 国际标准
Uuid	是	是	String	主机uuid 示例值： 1c26308c-5493-4eaf-a817-112ec25f499e

MalwareRiskOverview

文件查杀概览信息

被如下接口引用：DescribeMalwareRiskOverview

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
FileCount	是	否	Int64	恶意文件数 示例值： 1
HostCount	是	否	Int64	影响主机数 示例值： 1
IsFirstScan	是	否	Bool	是否首次扫描[false:否
ProcessCount	是	否	Int64	异常进程数 示例值： 1
ScanTime	是	否	String	最后扫描时间 示例值： 2022-09-23 15:11:46

FullMachine

主机信息

被如下接口引用：DescribeAllMachines

名称	必选	允许NULL	类型	描述
IsProVersion	是	否	Bool	是否是专业版 *true：是* false：否 示例值： true
MachineIp	是	否	String	主机IP。 示例值： 192.168.0.1
MachineName	是	否	String	主机名称。 示例值： redis_node_cvm
MachineWanIp	是	否	String	主机外网IP。 示例值： 35.168.0.1
Quuid	是	否	String	主机唯一标识Uuid。 示例值： 5a540076-d38a-4078-aa98-qwert371d322

BaselineDownload

基线导出结果下载

被如下接口引用：DescribeBaselineDownloadList

名称	必选	允许NULL	类型	描述
DownloadUrl	是	否	String	下载地址 示例值： https://cwp-1258344699.cos.ap-region1.mydomain.com/baseline-rule-view-result-20220823-095a9c44-7cc5-49c0-a02b-9a3e3442d5d6.csv?q-sign-algorithm=sha1
EndTime	是	否	String	完成时间 示例值： 2021-02-01 12:00:00
StartTime	是	否	String	开始时间 示例值： 2021-02-01 12:00:00
Status	是	否	Int64	状态0:未完成 1:完成 示例值： [0:未完成
TaskId	是	否	Int64	任务Id 示例值： 1661258891
TaskName	是	否	String	任务名称 示例值： baseline_rule_view_result_2021-02-01 12:00:00

ValueInfo

索引的value描述

被如下接口引用：DescribeLogIndex

名称	必选	允许NULL	类型	描述
ContainZH	是	否	Bool	Whether to contain zh characters 示例值： false
SqlFlag	是	否	Bool	字段是否开启分析功能 示例值： false
Tokenizer	是	否	String	字段的分词符 示例值： \n\t\r
Type	是	否	String	目前支持的类型有：long、text、double 示例值： text

DefaultStrategyInfo

默认策略基础信息

被如下接口引用：DescribeBaselineDefaultStrategyList

名称	必选	允许NULL	类型	描述
StrategyId	是	否	Uint64	策略id 示例值： 1
StrategyName	是	否	String	策略名 示例值： 国际标准基线

BaselineItemsCategory

基线检测项分类树状结构

被如下接口引用：DescribeBaselineItemInfo

名称	必选	允许NULL	类型	描述
CategoryCount	否	是	Int64	基线检测项子分类数目 示例值： 53
CategoryLists	否	是	Array of BaselineCategory	基线检测项子分类列表 示例值：查看
ParentCategoryId	否	是	Int64	基线检测项父分类id 示例值： 1
ParentCategoryName	否	是	String	基线检测项父分类名称 示例值： 弱密码

LoginWhiteLists

异地登录白名单

被如下接口引用：DescribeLoginWhiteList

名称	必选	允许NULL	类型	描述
CreateTime	是	否	Datetime	创建白名单时间 示例值： 2020-10-01 00:00:01
EndTime	是	否	String	结束时间 示例值： 2020-10-01 00:00:02
HostIp	是	否	String	机器IP 示例值： 10.20.30.40
Id	是	否	Uint64	记录ID 示例值： 1
IsGlobal	是	否	Bool	是否为全局规则 示例值： false
MachineName	是	否	String	机器名 示例值： stone
ModifyTime	是	否	Datetime	修改白名单时间 示例值： 2020-10-01 00:00:02
Places	是	否	Array of Place	白名单地域 示例值：查看
SrcIp	是	否	String	白名单IP（多个IP逗号隔开） 示例值： 1.2.2.3
StartTime	是	否	String	起始时间 示例值： 2020-10-01 00:00:01
UserName	是	否	String	白名单用户（多个用户逗号隔开） 示例值： user
Uuid	是	否	String	主机安全uuid 示例值： 8c09e1b1-5611-45b3-9c02-737996011b81

AssetEnvBaseInfo

资产管理环境变量列表

被如下接口引用：DescribeAssetEnvList

名称	必选	允许NULL	类型	描述
FirstTime	否	否	String	首次采集时间 示例值： 2022-07-15 11:27:01
IsNew	否	否	Int64	是否新增[0:否
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	否	String	服务器IP 示例值： 1.1.1.1
MachineName	否	否	String	服务器名称 示例值： hname
MachineWanIp	否	否	String	服务器外网IP 示例值： 1.1.1.1
Name	否	否	String	名称 示例值： BASHOPTS
OsInfo	否	否	String	操作系统 示例值： Linux
Quuid	否	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Type	否	否	Uint64	类型： 0:用户变量 1:系统变量 示例值： 1
UpdateTime	否	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
User	否	否	String	启动用户 示例值： root
Uuid	否	否	String	主机uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Value	否	否	String	环境变量值 示例值： checkwinsize:cmdhist:complete_fullquote:extquote:force_fignore:globasciiranges:hostcomplete:interactive_comments:login_shell:progcomp:promptvars:sourcepath

Vul

漏洞列表数据

被如下接口引用：DescribeVuls

名称	必选	允许NULL	类型	描述
ImpactedHostNum	是	否	Uint64	受影响机器数量 示例值： 1
LastScanTime	是	否	Datetime	最后扫描时间 示例值： 2020-02-01 12:00:00
VulId	是	否	Uint64	漏洞种类ID 示例值： 1
VulLevel	是	否	String	漏洞危害等级: HIGH：高危 MIDDLE：中危 LOW：低危 NOTICE：提示 示例值： LOW
VulName	是	否	String	漏洞名称 示例值： Apache
VulStatus	是	否	String	漏洞状态 *UN_OPERATED：待处理* FIXED：已修复

名称	必选	允许NULL	类型	描述
				示例值： UN_OPERATED

AssetKeyVal

key-val类型的通用数据结构

被如下接口引用：DescribeAssetAppCount、DescribeAssetDatabaseCount、DescribeAssetHostTotalCount、DescribeAssetMachineTagTop、DescribeAssetPortCount、DescribeAssetProcessCount、DescribeAssetRecentMachineInfo、DescribeAssetTotalCount、DescribeAssetTypeTop、DescribeAssetUserCount、DescribeAssetWebAppCount、DescribeAssetWebFrameCount、DescribeAssetWebLocationCount、DescribeAssetWebServiceCount

名称	必选	允许NULL	类型	描述
Desc	是	是	String	描述信息 示例值： none
Key	是	否	String	标签 示例值： app
NewCount	是	是	Int64	今日新增数量 示例值： 10
Value	是	否	Int64	数量 示例值： 21

LoginWhiteListsNew

异地登录白名单

被如下接口引用：DescribeLoginWhiteListNew

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	创建白名单时间 示例值： 2020-02-01 12:00:00
EndTime	是	是	String	结束时间 示例值： 2020-02-01 12:00:00
HostIp	是	否	String	机器IP 示例值： 192.168.0.10
Id	是	否	Uint64	记录ID 示例值： 1
IsGlobal	是	否	Uint64	是否为全局规则,1： 全局有效 0: 仅针对单台主机 示例值： 1
Locale	是	否	String	地域字符串 示例值： locale1
MachineName	是	否	String	机器名 示例值： redis_node_cvm
ModifyTime	是	否	String	修改白名单时间 示例值： 2020-02-01 12:00:00
Places	是	是	Array of Place	白名单地域 示例值：查看
Quuid	是	否	String	主机Quuid 示例值： 5a540076-d38a-4078-aa98-qwert371d322
Remark	是	是	String	备注 示例值： add redis cvm ip
SrcIp	是	否	String	白名单IP（多个IP逗号隔开） 示例值： 192.168.0.1
StartTime	是	是	String	开始时间 示例值： 2020-02-01 12:00:00
UserName	是	否	String	白名单用户（多个用户逗号隔开） 示例值： Alice
Uuid	是	否	String	云镜客户端ID 示例值： 5a540076-d38a-4078-aa98-qwert371d322

MaWorkload

被如下接口引用：DescribeMaWorkloadList

名称	必选	允许NULL	类型	描述
HostIp	否	是	String	主机/POD内网IP 示例值： 10.0.0.0.1
Id	否	是	Int64	ID 示例值： 1
IsSupportMa	否	是	Int64	是否支持微告警[1:是
Labels	否	是	Array of MaLabel	标签 示例值：查看
Name	否	是	String	主机/POD名称 示例值： redis_node_cvm
NotSupportMaCode	否	是	Int64	不支持微告警的原因[0:支持
PublicIp	否	是	String	主机公网IP 示例值： 35.168.0.1
Type	否	是	Int64	类型[0:主机

PrivilegeEscalationProcess

本地提权数据

被如下接口引用：DescribePrivilegeEvents

名称	必选	允许NULL	类型	描述
CmdLine	否	否	String	执行命令 示例值： ./a
CreateTime	否	否	String	发生时间 示例值： 2024-10-30 02:19:08
FullPath	否	否	String	进程路径 示例值： /tmp/any

名称	必选	允许NULL	类型	描述
Hostip	否	否	String	主机内网IP 示例值： 10.0.0.1
Id	否	否	Uint64	数据ID 示例值： 1
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineName	否	否	String	机器名 示例值： 2024-10-30 02:19:08
ParentProcGroup	否	否	String	父进程用户组 示例值： root
ParentProcName	否	否	String	父进程名 示例值： bash
ParentProcPath	否	否	String	父进程路径 示例值： /bin/bash
ParentProcUser	否	否	String	父进程用户名 示例值： root
Pid	否	是	Int64	进程id 示例值： 1
ProcFilePrivilege	否	否	String	进程文件权限 示例值： rwx
ProcTree	否	否	String	进程树 示例值： a(root),bash(ubuntu),sshd(ubuntu),sshd(root),sshd(root),init(root)
ProcessName	否	否	String	进程名 示例值： /etc/sshd
Quuid	否	否	String	主机ID 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
Status	否	否	Uint64	处理状态：0-待处理 2-白名单 3-已处理 4-已忽略 示例值： 0
UserGroup	否	否	String	用户组 示例值： root
UserName	否	否	String	用户名 示例值： root
Uuid	否	否	String	主机安全ID 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0

BaselineRiskItem

基线检测项top5

被如下接口引用：DescribeBaselineItemRiskTop

名称	必选	允许NULL	类型	描述
HostCount	是	否	Int64	影响服务器数 示例值： 1
ItemId	是	是	Int64	检测项Id 示例值： 1
ItemName	是	否	String	检测项名字 示例值： 弱口令
Level	是	否	Int64	基线风险等级：0低危 1中危 2高危 3严重 示例值： 1

EffectiveMachineInfo

批量导入机器信息.

被如下接口引用：DescribeImportMachineInfo

名称	必选	允许NULL	类型	描述
CloudFrom	否	是	Int64	云服务器来源 示例值： 0
CloudTags	否	是	Array of Tags	云标签信息 示例值：查看
InstanceID	否	是	String	机器instance ID 示例值： ins-sdsds
KernelVersion	否	是	String	内核版本号 示例值： 3.5
LicenseOrder	否	是	LicenseOrder	授权订单对象 示例值：查看
MachineName	否	是	String	机器名称 示例值： redis_node_cvm
MachinePrivateIp	否	是	String	机器内网ip 示例值： 1.2.3.4
MachinePublicIp	否	是	String	机器公网ip 示例值： 1.2.3.4
MachineStatus	否	是	String	在线状态 OFFLINE，ONLINE 示例值： OFFLINE
MachineTag	否	是	Array of MachineTag	机器标签 示例值：查看
Quuid	否	是	String	机器Quuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
Uuid	否	是	String	主机Uuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
VulNum	否	是	Uint64	漏洞数量 示例值： 1

AccountStatistics

帐号统计数据。

被如下接口引用：DescribeAccountStatistics

名称	必选	允许NULL	类型	描述
MachineNum	是	否	Uint64	主机数量。 示例值： 100
Username	是	否	String	用户名。 示例值： root

AssetUserDetail

资源管理账号基本信息

被如下接口引用：DescribeAssetUserInfo

名称	必选	允许NULL	类型	描述
DisableTime	是	否	String	账号到期时间 示例值： 2024-10-22 19:44:42
Gid	是	否	String	账号GID 示例值： 16
GroupName	是	否	String	用户组名 示例值： root
HomePath	是	否	String	Home目录 示例值： 1
IsDomain	是	否	Uint64	是否域账号：0否， 1是, 999为空 仅Windows 示例值： 1
IsRoot	是	否	Uint64	是否有root权限：0-否；1是，999为空: 仅linux 示例值： 1
IsSshLogin	是	否	Uint64	是否允许ssh登录，1是，0否, 999为空, 仅linux 示例值： 1
Keys	是	是	Array of AssetUserKeyInfo	用户公钥列表 示例值：查看
LastLoginIp	是	否	String	最近登录IP 示例值： 1.1.1.1
LastLoginLoc	是	否	String	最近登录位置 示例值： usa
LastLoginTerminal	是	否	String	最近登录终端 示例值： 1
LastLoginTime	是	否	String	上次登录时间 示例值： 2024-10-22 19:44:19
MachineIp	是	否	String	主机内网IP 示例值： 10.0.0.11
MachineName	是	否	String	主机名称 示例值： redis_node_cvm
Name	是	否	String	账号名称 示例值： root
PasswordChangeTime	是	否	String	密码修改时间 示例值： 2024-10-22 19:44:42
PasswordChangeType	是	否	Uint64	密码修改设置：0-不可修改，1-可修改 示例值： 1
PasswordDueTime	是	否	String	密码过期时间 仅linux 示例值： 2024-10-22 19:44:42
PasswordLockDays	是	否	Int64	密码锁定时间：单位天, -1为永不锁定 999为空，仅linux 示例值： 1
PasswordWarnDays	是	否	Uint64	密码过期提醒：单位天 示例值： 10
Quuid	是	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Remark	是	否	String	备注 示例值： no login
Shell	是	否	String	Shell路径 仅linux 示例值： /root
ShellLoginStatus	是	否	Uint64	是否shell登录性，0不是；1是 仅linux 示例值： 1
Status	是	否	Uint64	账号状态：0-禁用；1-启用 示例值： 1
Uid	是	否	String	账号UID 示例值： 134393481
UpdateTime	是	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
UserType	是	否	Uint64	账号类型：0访客用户，1标准用户，2管理员用户,999为空,仅Windows 示例值： 1
Uuid	是	否	String	主机Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

AttackSourceEvent

攻击溯源事件

被如下接口引用：DescribeAttackSourceEvents

名称	必选	允许NULL	类型	描述
Content	是	否	String	【文件查杀】病毒名 VirusName、文件名 FileName、文件路径 FilePath、文件大小 FileSize、文件MD5 MD5、首次发现时间 CreateTime、最近检测时间LatestScanTime、危害描述 HarmDescribe、修复建议SuggestScheme 【异常登录】来源IP SrcIp、来源地 Location、登录用户名 UserName、登录时间 LoginTime 【密码破解】来源IP SrcIp、来源地 City,Country 、协议 Protocol、登录用户名UserName 、端口 Port、尝试次数 Count、首次攻击时间 CreateTime、最近攻击时间 ModifyTime 【恶意请求】恶意请求域名 Url、进程ProcessName 、MD5 ProcessMd5、PID Pid、请求次数 AccessCount、最近请求时间 MergeTime、危害描述 HarmDescribe、修复建议SuggestScheme 【高危命令】命中规则名 RuleName、规则类别 RuleCategory、命令内容 BashCmd、数据来源 DetectBy、登录用户 User、PID Pid、发生时间 CreateTime 、危害描述 HarmDescribe、修复建议SuggestScheme 示例值： VirusName
CreatedTime	是	否	String	入侵时间 示例值： 2021-03-30 19:17:28
EventType	是	否	Uint64	事件类型：0：文件查杀，1：异常登录， 2：密码破解，3：恶意请求，4：高危命令 示例值： 1
Id	是	否	Uint64	事件id 示例值： 12

名称	必选	允许NULL	类型	描述
Level	是	否	Uint64	等级 事件统一等级 0：提示，1：低危，2：中危，3：高危，4：严重 示例值： 1
LevelZh	是	否	String	等级名字 示例值： 严重
Uuid	是	否	String	主机uuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0

RecordInfo

客户端异常信息结构

被如下接口引用：DescribeClientException

名称	必选	允许NULL	类型	描述
HostIP	是	否	String	主机ip 示例值： 10.10.10.10
InstanceID	是	否	String	主机实例id 示例值： ins-gdsgdsd
OfflineTime	是	否	String	客户端离线时间 示例值： 2022-11-14 00:00:00
UninstallCmd	是	否	String	客户端卸载调用链 示例值： sh uninstall.sh
UninstallTime	是	否	String	客户端卸载时间 示例值： 2022-11-14 00:00:00
Uuid	是	否	String	客户端uuid 示例值： c6bf7a9e-95cf-4048-a6cc-97e85d02e6ee

KeyValueArrayInfo

索引键值信息

被如下接口引用：DescribeLogIndex

名称	必选	允许NULL	类型	描述
Key	是	否	String	需要配置键值或者元字段索引的字段 示例值： key1
Value	是	否	ValueInfo	字段的索引描述信息 示例值：查看

OpenPortStatistics

端口统计列表

被如下接口引用：DescribeOpenPortStatistics

名称	必选	允许NULL	类型	描述
MachineNum	是	否	Uint64	主机数量 示例值： 100
Port	是	否	Uint64	端口号 示例值： 8080

CKafkaTopicInfo

Ckafka主题名称

被如下接口引用：DescribeLogDeliveryKafkaOptions

名称	必选	允许NULL	类型	描述
TopicID	是	否	String	主题ID 示例值： topic_gsyds
TopicName	是	否	String	主题名称 示例值： topic_dsyg

MaWhitelist

被如下接口引用：DescribeMaWhitelist、ModifyMaWhitelist

名称	必选	允许NULL	类型	描述
CreateTime	否	是	String	创建时间 示例值： 2023-10-10 00:00:00
Dest	是	是	String	访问目标，支持IP/P段/IP范围，多个之间使用英文分号隔开;默认all 示例值： 1.1.1.1-1.1.1.2
DestPort	否	是	String	目标端口，多个之间使用英文分号隔开，不填写则表示all 示例值： 80;8080
Enable	是	是	Uint64	是否生效 • 0：不生效 • 1：生效 示例值： 1
From	是	是	Uint64	白名单配置来源 • 1：租户端 • 0：运营端，租户端不可以删除和关闭运营端来源的全局配置白名单 示例值： 1
Id	否	是	Uint64	白名单配置项ID 示例值： 1
ModifyTime	否	是	String	更新时间 示例值： 2023-10-10 00:00:00
Name	是	是	String	白名单名称 示例值： 白名单1
Source	是	是	String	访问源，支持IP/P段/IP范围，多个之间使用英文分号隔开;默认all 示例值： 1.1.1.1/24

名称	必选	允许NULL	类型	描述
Updater	是	是	String	白名单创建人/更新人 示例值： Alice

RansomDefenseStrategyMachineBackupInfo

防勒索策略绑定主机备份详情

被如下接口引用：DescribeRansomDefenseMachineList

名称	必选	允许NULL	类型	描述
BackupCount	是	是	Uint64	备份数量 示例值： 1
BackupSuccessCount	是	是	Uint64	备份成功次数 示例值： 1
CloudTags	是	是	Array of Tag	云标签 示例值：查看
DiskInfo	是	是	String	硬盘信息，为空时所有硬盘生效： ;分割 diskId1
InstanceId	是	否	String	主机实例id 示例值： cvm-dwcs
LastBackupMessage	是	是	String	最近一次备份失败原因 示例值： fail
LastBackupStatus	是	是	Uint64	最近一次备份状态：0备份中，1正常，2失败，9暂无备份 示例值： 1
LastBackupTime	是	是	String	最近一次备份时间 示例值： 2022-11-11 11:11:11
MachineIp	是	否	String	内网ip 示例值： 10.0.0.22
MachineName	是	否	String	主机名称 示例值： redis_node_cvm
MachineWanIp	是	是	String	外网ip 示例值： 112.11.33.22
Quuid	是	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
RegionInfo	是	是	RegionInfo	可用区信息 示例值：查看
RollBackPercent	是	是	Uint64	最近一次回滚进度百分比 示例值： 1
RollBackStatus	是	是	Uint64	最近一次回滚状态：0进行中，1成功，2失败 示例值： 1
Status	是	是	Uint64	防护状态：0关闭，1开启 示例值： 0
StrategyId	是	是	Uint64	策略id，为0时未绑定策略 示例值： 0
StrategyName	是	是	String	策略名称 示例值： any1
Tag	是	是	Array of MachineTag	主机安全标签 示例值：查看
Uuid	是	否	String	主机Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

BaselineItem

基线项

被如下接口引用：DescribeBaselineItemList

名称	必选	允许NULL	类型	描述
CanBeFixed	否	是	Int64	是否可以修复 示例值： 1
CategoryId	否	否	Int64	检测项分类 示例值： 50
DetectResultDesc	否	是	String	检测结果描述 示例值： 如果 Redis 以 root 权限启动且未授权访问，则会造成任意文件写入，最终导致命令执行漏洞。
DetectStatus	否	是	Int64	检测状态：0 未通过，1：忽略，3：通过，5：检测中 示例值： 1
FirstTime	否	是	String	第一次出现时间 示例值： 1
FixMethod	否	否	String	修复方法 示例值： 1. 以低权限用户权限启动 Redis；
HostId	否	是	String	主机ID 示例值： 1
HostIp	否	是	String	主机IP 示例值： 192.168.0.1
HostName	否	是	String	主机名 示例值： redis_node_cvm
ItemDesc	否	否	String	项描述 示例值： 如果 Redis 以 root 权限启动且未授权访问，则会造成任意文件写入，最终导致命令执行漏洞。
ItemId	否	否	Int64	项Id 示例值： 1100
ItemName	否	否	String	项名称 示例值： Redis 基线合规检测
LastTime	否	是	String	最近出现时间 示例值： 2025-01-01 12:00:00
Level	否	是	Int64	基线风险等级：0低危 1中危 2高危 3严重 示例值： 1
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看

名称	必选	允许NULL	类型	描述
RuleName	否	否	String	所属规则 示例值： Linux系统弱口令检测
Uuid	否	是	String	主机安全uuid 示例值： 5a540076-d38a-4078-aa98-q45rt371d322
WanIp	否	是	String	外网IP 示例值： 35.236.25.11

VulDefencePluginStatus

主机漏洞防御插件信息

被如下接口引用：DescribeVulDefencePluginStatus

名称	必选	允许NULL	类型	描述
Alias	是	否	String	主机别名 示例值： redis_node_cvm
CreateTime	是	否	String	创建时间 示例值： 2021-01-20 16:17:11
Exception	是	否	Int64	插件状态：0 正常，1 异常 示例值： 1
ModifyTime	是	否	String	最后跟新时间 示例值： 2021-01-20 16:17:11
PrivateIp	是	否	String	内网ip 示例值： 10.1.1.2
PublicIp	是	否	String	公网ip 示例值： 112.23.2.1
Quuid	是	否	String	主机quuid 示例值： d92d723e-4aac-4f4a-bbf9-e5430e29d289

ProtectDirInfo

防护目录列表集

被如下接口引用：DescribeProtectDirList

名称	必选	允许NULL	类型	描述
AutoRestoreSwitchStatus	是	否	Uint64	自动恢复开关 (Filters 过滤Quuid 时 返回) 默认0 示例值： 0
DirName	是	否	String	网站名称 示例值： nginx web
DirPath	是	否	String	网站防护目录地址 示例值： /opt/nginx
FirstProtectTime	否	是	String	首次开启防护时间 示例值： 2021-02-01 12:00:00
Id	是	否	String	唯一ID 示例值： 2
LatestProtectTime	否	是	String	最近开启防护时间 示例值： 2021-02-01 12:00:00
NoProtectServerNum	是	否	Uint64	未防护服务器数 示例值： 0
ProtectException	是	否	Uint64	防护异常 示例值： 0
ProtectFileType	否	是	String	防护文件类型 示例值： .php;.js
ProtectFilesCount	否	是	Int64	防护文件总数 示例值： 0
ProtectServerNum	是	否	Uint64	防护服务器数 示例值： 0
ProtectStatus	是	否	Uint64	防护状态 示例值： 0
RelatedServerNum	是	否	Uint64	关联服务器数 示例值： 0

NetAttackEventInfo

被如下接口引用：DescribeAttackEventInfo

名称	必选	允许NULL	类型	描述
AbnormalAction	否	是	String	异常行为 示例值： dnslog:v5igcrlnyt94ka7f.k2qb16y0.ser.dnslogayay
AttackLevel	否	是	Uint64	攻击热度级别，大于等于3为热点攻击 示例值： 3
CVEId	否	是	String	漏洞CVE编号 示例值： CVE-2023-44487
Count	否	是	Uint64	攻击次数 示例值： 1
DstPort	否	是	Uint64	目标端口 示例值： 80
HostOpProcessTree	否	是	String	进程树,需要用base64 解码 示例值： W3sicGlkIjoyODc0MCwiZXhlIjoiL3Vzci9iaW4vY3VybCIsImFjY291bnQiOiIwOjAiLCJjbWRsaW5lIjoiY3VybCAtcyAtTCBodHRwczovL2Rvd25sb2FkLmMzcG9v
HostOpType	否	是	Uint64	0:无失陷行为 1: rce(命令执行) 2: dnslog 3: writefile 示例值： 1
Id	否	是	Uint64	事件id 示例值： 49754647
Location	否	是	String	攻击源地 示例值： location1-location2
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看

名称	必选	允许NULL	类型	描述
MergeTime	否	是	String	攻击发生时间 示例值： 2021-02-01 12:00:00
NetPayload	否	是	String	攻击数据包 示例值： POST /wls-wsat/CoordinatorPortType HTTP/1.1 X-Stgw-Time: 1730212752.801 Host: h2.lghd111.com X-Client-Proto: https X-Forwarded-Proto: https X-Client-Proto-Ver: HTTP/1.1
PayVersion	否	是	Uint64	机器付费版本，0 基础版，1专业版，2旗舰版，3普惠版 示例值： 1
Quuid	否	是	String	cvm uuid 示例值： 3ddf6cc1-9389-4b9a-a10b-85f30491ayay
SrcIP	否	是	String	攻击源ip 示例值： 192.168.0.204
Status	否	是	Uint64	处理状态，0 待处理 1 已处理 2 已加白 3 已忽略 4 已删除 5: 已开启防御 示例值： 1
SvcPs	否	是	String	服务进程 base64 示例值： eyJhY2NvdW50IjoiMDowIiwiYXJndil6Im5naW54OiBtYXN0ZXIgcHJvY2VzcyAvdXNyL3NiaW4vbmdpbngiLCJleGUiOiIvdXNyL2xvY2FsL25naW54L25naW54IiwibGlzdGVuIjoiMC4wLjAuMDo4MCIsInBpZCI6MTI0ayay
Type	否	是	Uint64	0: 尝试攻击 1:攻击成功 示例值： 1
Uuid	否	是	String	主机uuid 示例值： 3ddf6cc1-9389-4b9a-a10b-85f30491ayay
VulDefenceStatus	否	是	Uint64	漏洞防御状态，0关闭，1开启 示例值： 1
VulId	否	是	Uint64	漏洞id 示例值： 100386
VulName	否	是	String	漏洞名称 示例值： Weblogic 反序列化远程代码执行漏洞 (CVE-2019-2ayay
VulSupportDefense	否	是	Uint64	漏洞是否支持防御，0:不支持 1:支持 示例值： 1

AssetProcessBaseInfo

资源管理进程基本信息

被如下接口引用：DescribeAssetProcessInfoList

名称	必选	允许NULL	类型	描述
Desc	否	否	String	进程说明 示例值： user any
FirstTime	否	否	String	首次采集时间 示例值： 2022-07-15 11:27:01
GroupName	否	否	String	进程用户组 示例值： root
HasSign	否	否	Uint64	数字签名:0无，1有， 999 空，仅Windows 示例值： 1
InstallByPackage	否	否	Uint64	是否通过安装包安装：:0否，1是， 999 空，仅linux 示例值： 1
IsNew	否	否	Int64	是否新增[0:否
MachineExtraInfo	否	是	MachineExtraInfo	主机信息 示例值：查看
MachineIp	否	否	String	主机内网IP 示例值： 10.0.0.11
MachineName	否	否	String	主机名称 示例值： 1
MachineWanIp	否	否	String	主机外网IP 示例值： 112.42.66.11
Md5	否	否	String	进程MD5 示例值： e10adc3949ba59abbe56e057f20f883e
Name	否	否	String	进程名称 示例值： rsyslogd
OsInfo	否	否	String	操作系统信息 示例值： Centos 64bit
PackageName	否	否	String	软件包名 示例值： rsyslog
Param	否	否	String	启动参数 示例值： /usr/sbin/rsyslogd -n
ParentProcessName	否	否	String	父进程名称 示例值： systemd
Path	否	否	String	进程路径 示例值： /usr/sbin/rsyslogd
Pid	否	否	String	进程ID 示例值： 10021
Ppid	否	否	String	父进程ID 示例值： 1
ProjectId	否	否	Uint64	主机业务组ID 示例值： 1
Quuid	否	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
StartTime	否	否	String	启动时间 示例值： 2024-10-23 14:17:00
Status	否	否	String	进程状态：R 可执行、S 可中断、D 不可中断、T 暂停状态或跟踪状态、Z 僵尸状态、X 将被销毁 示例值： R
Tag	否	是	Array of MachineTag	主机标签 示例值：查看
Tty	否	否	String	进程TTY 示例值： ?

名称	必选	允许NULL	类型	描述
UpdateTime	否	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
User	否	否	String	运行用户 示例值： root
Uuid	否	否	String	主机Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Version	否	否	String	进程版本 示例值： 1

VulDefenceOverview

漏洞防御趋势页，包括插件状态及攻防趋势，趋势由三个长度相同，元素一一对应的数组保存，如果某天没有数据将会缺失

被如下接口引用：DescribeVulDefenceOverview

名称	必选	允许NULL	类型	描述
AttackCounts	是	是	Array of Int64	每日攻击趋势 示例值： [0,0,20,0,0,0,0,17,11,2,33,49,105,80]
Date	是	是	Array of String	日期 示例值： ["2024-10-21","2024-10-22","2024-10-23","2024-10-24","2024-10-25","2024-10-26","2024-10-27","2024-10-28","2024-10-29","2024-10-30","2024-10-31","2024-11-01","2024-11-02","2024-11-03"]
DefendCounts	是	是	Array of Int64	每日防御趋势 示例值： [0,0,20,0,0,0,0,17,11,2,33,49,105,80]
DefendHostCount	是	否	Int64	已开启防御主机数 示例值： 12
Enable	是	否	Int64	防御开关：0 关闭 1 开启 示例值： 1
ExceptionCount	是	否	Int64	插件异常数 示例值： 2

VulLevelInfo

漏洞数量按等级分布统计结果实体

被如下接口引用：DescribeVulLevelCount

名称	必选	允许NULL	类型	描述
Count	是	否	Uint64	数量 示例值： 100
VulLevel	是	否	Uint64	// 危害等级：1-低危；2-中危；3-高危；4-严重 示例值： 1

ScreenProtection

大屏可视化攻防状态

被如下接口引用：DescribeScreenProtectionStat

名称	必选	允许NULL	类型	描述
Name	是	否	String	类型值：文件查杀，暴力破解，漏洞扫描，基线检测 示例值： 文件查杀
Status	是	否	Uint64	文件查杀: 0:从未检测过，或0资产付费情况, 1:已检测，存在恶意文件, 2:已检测，未开启隔离防护, 3:已检测且已开启防护且无风险； 暴力破解: 0:未开启防护（0付费资产情况）1:已开启自动阻断； 漏洞扫描: 0:从未检测过，或0资产付费情况, 1:存在漏洞风险, 2:无风险； 基线检测: 0:从未检测过，或0资产付费情况, 1:存在基线风险,2:无风险； 示例值： 1

UnionProtectDetail

联合购买容器防护计费项信息

被如下接口引用：DescribeLicenseList

名称	必选	允许NULL	类型	描述
Deadline	否	是	String	到期时间 示例值： 2024-07-30 15:02:19
InquireKey	否	是	String	计费项 示例值： sv_yunjing_ue_x
Number	否	是	Int64	数量 示例值： 10
ResourceId	否	是	String	资源ID 示例值： resource_gdskh12h

VulStoreListInfo

被如下接口引用：DescribeHotVulTop、DescribeVulStoreList

名称	必选	允许NULL	类型	描述
AttackLevel	否	是	Uint64	攻击热度级别，大于等于3为热点攻击 示例值： 1
CveId	否	是	String	cve编号 示例值： CVE-2023-44487
FixSwitch	否	是	Uint64	漏洞是否支持自动修复 0-Windows/Linux均关闭; 1-Windows/Linux均打开; 2-仅Linux; 3-仅Windows 示例值： 1
Level	否	是	Uint64	漏洞等级 1:低 2:中 3:高 4:严重 示例值： 1
Method	否	是	Uint64	漏洞检测方法 0 - 版本比对, 1 - POC验证 示例值： 0
Name	否	是	String	漏洞名称 示例值： Apache HTTP/2 协议拒绝服务漏洞(CVE-2023-44487)
PublishDate	否	是	String	发布时间 示例值： 2012-10-10 07:55:00

名称	必选	允许NULL	类型	描述
SupportDefense	否	是	Uint64	漏洞是否支持防御 0:不支持 1:支持 示例值： 1
VulCategory	否	是	Uint64	1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 0= 应急漏洞 示例值： 1
VulId	否	是	Uint64	漏洞ID 示例值： 1

VulEffectHostList

漏洞影响主机列表

被如下接口引用：DescribeVulEffectHostList

名称	必选	允许NULL	类型	描述
AliasName	否	是	String	主机别名 示例值： redis_node_cvm
CloudTags	否	是	Array of Tags	云标签信息 示例值：查看
Description	否	是	String	说明 示例值： 如果 Redis 以 root 权限启动且未授权访问，则会造成任意文件写入，最终导致命令执行漏洞。
DescriptionEn	否	是	String	说明 示例值： 说明英文
EventId	否	是	Uint64	事件id 示例值： 1
FirstDiscoveryTime	否	是	String	首次发现时间 示例值： 2021-03-24 16:37:57
FixStatusMsg	否	是	String	失败原因 示例值： 修复超时
HostIp	否	是	String	主机HostIp 示例值： 10.12.78.56
HostVersion	否	是	Uint64	版本信息：0-基础版 1-专业版 2-旗舰版 3-普惠版 示例值： 1
InstanceState	否	是	String	实例状态："PENDING"-创建中 "LAUNCH_FAILED"-创建失败 "RUNNING"-运行中 "STOPPED"-关机 "STARTING"-表示开机中 "STOPPING"-表示关机中 "REBOOTING"-重启中 "SHUTDOWN"-表示停止待销毁 "TERMINATING"-表示销毁中 " 示例值： RUNNING
IsSupportAutoFix	否	是	Uint64	是否能自动修复 0 :漏洞不可自动修复， 1：可自动修复， 2：客户端已离线， 3：主机不是旗舰版只能手动修复， 4：机型不允许 ，5：修复中 ，6：已修复， 7：检测中 9:修复失败，10:已忽略 11:漏洞只支持linux不支持Windows 12：漏洞只支持Windows不支持linux，13:修复失败但此时主机已离线，14:修复失败但此时主机不是旗舰版， 15:已手动修复 示例值： 2
LastTime	否	是	String	最后检测时间 示例值： 2021-03-24 16:37:57
Level	否	是	Uint64	危害等级：1-低危；2-中危；3-高危；4-严重 示例值： 1
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
PublicIpAddresses	否	是	String	外网ip 示例值： 120.12.78.73
Quuid	否	是	String	主机Quuid 示例值： 5a540076-d38a-4078-aa98-q45rt371d322
Status	否	是	Uint64	状态：0: 待处理 1:忽略 3:已修复 5:检测中 6:修复中 7: 回滚中 8:修复失败 示例值： 0
Tags	否	是	Array of String	主机标签 示例值： ["tag-01"]
Uuid	否	是	String	主机Uuid 示例值： 5a540076-d38a-4078-aa98-q45rt371d322

MaConnPodInfo

被如下接口引用：DescribeMaConnEventList

名称	必选	允许NULL	类型	描述
ClusterId	否	是	String	pod的集群Id 示例值： cls-dfdayayay
Namespace	否	是	String	pod命名空间 示例值： tcss
PodName	否	是	String	pod名字 示例值： redis-job-sdfa-9885-sd23

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：DescribeAssetAppList、DescribeAssetCoreModuleList、DescribeAssetDatabaseList、DescribeAssetEnvList、DescribeAssetInitServiceList、DescribeAssetJarList、DescribeAssetPlanTaskList、DescribeAssetWebServiceInfoList、DescribeLoginWhiteHostList、DescribeMachineList、DescribeProtectDirList、DescribeWebPageEventList、ExportAssetAppList、ExportAssetCoreModuleList、ExportAssetDatabaseList、ExportAssetEnvList、ExportAssetInitServiceList、ExportAssetJarList、ExportAssetPlanTaskList、ExportAssetWebServiceInfoList、ExportProtectDirList、ExportWebPageEventList

名称	必选	允许NULL	类型	描述
ExactMatch	否	否	Bool	是否模糊查询 示例值： true
Name	是	否	String	过滤键的名称。 示例值： Ip
Values	是	否	Array of String	一个或者多个过滤值。 示例值： ["192.168.0.1"]

BashEventsInfo

高危命令数据详情

被如下接口引用：DescribeBashEventsInfo

名称	必选	允许NULL	类型	描述
BashCmd	是	否	String	执行命令 示例值： rm
CreateTime	是	否	String	发生时间 示例值： 2021-03-30 19:17:28
DetectBy	否	是	Int64	数据来源 示例值： agent
Exe	是	是	String	进程名称 示例值： 1.exe
HarmDescribe	是	是	String	描述信息 示例值： desc of event
HostIp	是	否	String	主机内网IP 示例值： 127.0.0.1
Id	是	否	Uint64	数据ID 示例值： 1001
MachineName	是	否	String	主机名 示例值： redis_node_cvm
MachineStatus	是	是	String	主机在线状态 OFFLINE ONLINE 示例值： ONLINE
MachineWanIp	是	是	String	主机外网ip 示例值： 124.2.4.55
ModifyTime	是	是	String	处理时间 示例值： 2021-03-30 19:17:28
Pid	是	是	String	进程号 示例值： 1
Platform	是	否	Uint64	系统类型： 2 windows、4 linux 示例值： 1
PsTree	是	是	String	进程树 json pid:进程id，exe:文件路径 ，account:进程所属用组和用户 ,cmdline:执行命令，ssh_service: SSH服务ip, ssh_soure:登录源 示例值： "[{"pid":134,"exe":"/usr/bin/bash","account":"root:root","cmdl"
Quuid	是	否	String	主机ID 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
References	是	是	Array of String	参考链接 示例值： ["http://www.domain.com"]
RegexBashCmd	是	是	String	自动生成的正则表达式 示例值： rm -rf /tmp/t*
RuleCategory	是	是	Uint64	规则类别 0=系统规则，1=用户规则 示例值： 0
RuleId	是	否	Uint64	规则ID,等于0表示已规则已被删除或生效范围已修改 示例值： 1
RuleLevel	是	否	Uint64	规则等级：1-高 2-中 3-低 示例值： 1
RuleName	是	否	String	规则名称 示例值： redis_node_use
Status	是	否	Uint64	处理状态： 0 = 待处理 1= 已处理, 2 = 已加白， 3= 已忽略 示例值： 1
SuggestScheme	是	是	String	建议方案 示例值： attempt to repair
Tags	是	是	Array of String	标签 示例值： ["tag-redis","tag-nginx"]
User	是	是	String	登录用户 示例值： root
Uuid	是	否	String	主机uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

WarningInfoObj

告警设置列表

被如下接口引用：DescribeWarningList

名称	必选	允许NULL	类型	描述
BeginTime	是	否	String	开始时间，格式: HH:mm 示例值： 00:00
ControlBit	是	否	Uint64	漏洞等级控制位（对应DB的十进制存储） 示例值： 0
ControlBits	是	否	String	漏洞等级控制位二进制，每一位对应页面漏洞等级的开启关闭：低中高（0:关闭；1：开启），例如：101 → 同时勾选低+高 示例值： 0
Count	是	是	Int64	配置的告警范围主机个数，前端用此判断展示提示信息 示例值： 0
DisablePhoneWarning	是	否	Uint64	1: 关闭告警 0: 开启告警 示例值： 1
EndTime	是	否	String	结束时间，格式: HH:mm 示例值： 00:00
HostRange	否	是	Int64	告警主机范围类型，0:全部主机，1:按所属项目选，2:按云标签选，3:按主机安全标签选，4:自选主机 示例值： 0
OfflineInterval	是	是	Int64	离线类型判断时间 单位秒 示例值： 1432524532
TimeZone	是	否	String	时区信息 示例值： Europe/London
Type	是	否	Uint64	事件告警类型；1：离线，2：木马，3：异常登录，4：爆破，5：漏洞（已拆分为9-12四种类型）6：高危命令，7：反弹sell，8：本地提权，9：应用漏洞，10：web-cms漏洞，11：应急漏洞，12：安全基线,13: 防篡改，14：恶意请求，15: 网络攻击，16：Windows系统漏洞，17：Linux软件漏洞，18：核心文件监控告警，19：客户端卸载告警。20：客户端离线告警 示例值： 1

AssetLoadDetail

资产管理负载信息

被如下接口引用：DescribeAssetLoadInfo

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
Desc	是	否	String	描述信息 示例值： 4G
MachineName	是	否	String	主机名称 示例值： redis_node_cvm
Quuid	是	否	String	主机Quuid 示例值： d99a1b46-cc2d-4633-a11f-4a7663d2523e
Uuid	是	否	String	主机Uuid 示例值： d99a1b46-cc2d-4633-a11f-4a7663d2523e
Value	是	否	Float	负载 示例值： 0.4

AssetWebLocationInfo

资产管理Web站点列表信息

被如下接口引用：DescribeAssetWebLocationInfo

名称	必选	允许NULL	类型	描述
Command	是	否	String	启动命令 示例值： true
Ip	是	否	String	绑定IP 示例值： 0.0.0.0
MainPath	是	否	String	主目录 示例值： /data
Name	是	否	String	域名 示例值： domain.com
Port	是	否	String	站点端口 示例值： 22
Proto	是	否	String	站点协议 示例值： tcp
SafeStatus	是	否	Uint64	安全模块状态：0未启用，1启用，999空，仅nginx 示例值： 1
ServiceType	是	否	String	服务类型 示例值： web
UpdateTime	是	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
User	是	否	String	运行用户 示例值： root

FileTamperRuleInfo

核心文件监控规则列表

被如下接口引用：DescribeFileTamperRules

名称	必选	允许NULL	类型	描述
AddWhiteType	否	是	String	加白处理类型 • cur 仅对当前加白 • all 所有符合条件加白 示例值： cur
CreateTime	是	否	String	创建时间 示例值： 2021-03-30 19:17:28
FileAction	是	是	String	监控行为 • read 读取文件 • write 修改文件 • read-write 读取修改文件 示例值： read
HostCount	是	是	Uint64	影响主机数 示例值： 12
Id	是	否	Uint64	规则id，系统的规则时为0。 示例值： 12
IsGlobal	是	否	Uint64	是否是全局的 0：否 ，1：是 示例值： 1
Level	是	否	Uint64	风险等级 0：无， 1: 高危， 2:中危， 3: 低危 示例值： 3
ModifyTime	是	否	String	更新时间 示例值： 2021-03-30 19:17:28
Name	是	是	String	规则名称 示例值： 禁止访问
ReadRuleCount	是	否	Uint64	子规则读条目数 示例值： 1
ReadWriteRuleCount	是	否	Uint64	子规则读写条目数 示例值： 1
RuleCategory	是	否	Uint64	规则类型 0 ：系统规则 1：用户规则 示例值： 1
Status	是	否	Uint64	状态 0: 启用 1: 已关闭 示例值： 1
WriteRuleCount	是	否	Uint64	子规则写条目数 示例值： 1

RansomDefenseBackup

主机快照备份列表

被如下接口引用：DescribeRansomDefenseBackupList

名称	必选	允许NULL	类型	描述
BackupStatus	是	否	Uint64	备份状态：0备份中，1正常，2、3失败，4快照已过期，9快照已删除 示例值： 1

名称	必选	允许NULL	类型	描述
BackupTime	是	否	String	备份时间 示例值： 2022-11-11 11:00:00
DiskCount	是	否	Uint64	备份磁盘数量 示例值： 1
Disks	是	否	String	硬盘信息，；分隔 示例值： id1
EventStatus	是	否	Uint64	勒索状态：0无告警, 1有告警 示例值： 1
SnapshotIds	是	否	String	快照列表，；分隔 示例值： id1;id2
StrategyId	是	否	Uint64	策略id 示例值： 1
StrategyName	是	否	String	策略名称 示例值： tt1
StrategyStatus	是	否	Uint64	策略状态:0关闭，1开启，9已删除 示例值： 1

VulDetailInfo

漏洞详细信息

被如下接口引用：DescribeScanTaskDetails

名称	必选	允许NULL	类型	描述
CveId	是	否	String	cve编号 示例值： cve_ay
Cvss	是	否	String	CVSS详情 示例值： dadad
CvssScore	是	否	Float	CVSS评分 示例值： 1.1
Descript	是	否	String	漏洞描述 示例值： desc of this vul
Fix	是	否	String	修复建议 示例值： 修复
Level	是	否	Uint64	漏洞级别 示例值： 1
Name	是	否	String	漏洞名称 示例值： 漏洞
PublishTime	是	否	String	发布时间 示例值： 11
Reference	是	否	String	参考链接 示例值： http://www.domain.com/any/any
VulCategory	是	否	Uint64	1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 0= 应急漏洞 示例值： 1
VulId	是	否	Uint64	漏洞ID 示例值： 1

VulHostTopInfo

服务器风险top5实体

被如下接口引用：DescribeVulHostTop

名称	必选	允许NULL	类型	描述
HostName	是	是	String	主机名 示例值： redis_node_cvm
Quuid	是	是	String	主机Quuid 示例值： 8efa1586-c390-4131-ad90-19c1ff64ayay
Score	是	是	Uint64	top评分 示例值： 511
VulLevelList	是	是	Array of VulLevelCountInfo	漏洞等级与数量统计列表 示例值：查看

BashEventsInfoNew

高危命令数据详情(新)

被如下接口引用：DescribeBashEventsInfoNew

名称	必选	允许NULL	类型	描述
BashCmd	是	否	String	执行命令 示例值： rm
CreateTime	是	否	String	发生时间 示例值： 2021-03-30 19:17:28
DetectBy	是	是	Int64	检测来源 0:bash日志 1:实时监控 示例值： 0
Exe	是	是	String	进程名称 示例值： 1.exe
HarmDescribe	是	是	String	描述信息 示例值： desc of event
HostIp	是	否	String	主机内网IP 示例值： 127.0.0.1
Id	是	否	Uint64	数据ID 示例值： 1
MachineName	是	否	String	主机名 示例值： redis_node_cvm
MachineStatus	是	是	String	主机在线状态 OFFLINE ONLINE 示例值： ONLINE
MachineType	是	是	Int64	0:普通 1:专业版 2:旗舰版 示例值： 1

名称	必选	允许NULL	类型	描述
MachineWanIp	是	是	String	主机外网ip 示例值： 124.2.4.55
ModifyTime	是	是	String	处理时间 示例值： 2021-03-30 19:17:28
Pid	是	是	String	进程号 示例值： 1
Platform	是	否	Uint64	系统类型： 2 windows、4 linux 示例值： 1
PsTree	是	是	String	进程树 json pid:进程id，exe:文件路径 ，account:进程所属用组和用户 ,cmdline:执行命令，ssh_service: SSH服务ip, ssh_soure:登录源 示例值： "[{"pid":134,"exe":"/usr/bin/bash","account":"root:root","cmdl"
Quuid	是	否	String	主机ID 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
References	是	是	Array of String	参考链接 示例值： ["http://www.domain.com"]
RegexBashCmd	是	是	String	自动生成的正则表达式 示例值： rm -rf /tmp/t*
RuleCategory	是	是	Uint64	规则类别 0=系统规则，1=用户规则 示例值： 0
RuleId	是	否	Uint64	规则ID,等于0表示已规则已被删除或生效范围已修改 示例值： 1
RuleLevel	是	否	Uint64	规则等级：1-高 2-中 3-低 示例值： 1
RuleName	是	否	String	规则名称 示例值： redis_node_use
Status	是	否	Uint64	处理状态： 0 = 待处理 1= 已处理, 2 = 已加白， 3= 已忽略 示例值： 1
SuggestScheme	是	是	String	建议方案 示例值： attempt to repair
Tags	是	是	Array of String	标签 示例值： ["tag-redis","tag-nginx"]
User	是	是	String	登录用户 示例值： user1
Uuid	是	否	String	主机安全ID 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

MaHost

被如下接口引用：DescribeMaHostList

名称	必选	允许NULL	类型	描述
AlarmCount	否	是	Int64	异常访问数量 示例值： 10
HostIp	否	是	String	内网IP 示例值： 10.0.0.1
Id	否	是	Int64	ID 示例值： 1
InstanceId	否	是	String	实例ID 示例值： ins-hnwf3y81
IsEnabled	否	是	Int64	监控开关[1:开
IsNew	否	是	Int64	15日新增[1:是
IsSupportMa	否	是	Int64	是否支持微告警[1:是
Labels	否	是	Array of MaLabel	关联标签 示例值：查看
LearnEndTime	否	是	String	单个负载结束学习时间 示例值： 2024-01-01 00:00:00
LearnStartTime	否	是	String	单个负载开始学习时间 示例值： 2024-01-01 00:00:00
Name	否	是	String	主机名称 示例值： redis_node_cvm
NotSupportMaCode	否	是	Int64	不支持微告警的原因[0:支持
OsName	否	是	String	操作系统 示例值： CentOS Linux release 7.8.2003 (Core)
PublicIp	否	是	String	公网IP 示例值： 8.8.8.8
Region	否	是	String	地域 示例值： ap-region1
Uuid	否	是	String	主机UUID 示例值： b538f4cc-e666-408a-aa94-fc5280b5d629
VpcId	否	是	String	所属网络 示例值： vpc-82h54yji

FileTamperRule

核心文件监控规则

被如下接口引用：DescribeFileTamperEventRuleInfo、DescribeFileTamperRuleInfo、DescribeMachineFileTamperRules、ModifyFileTamperRule

名称	必选	允许NULL	类型	描述
Action	是	否	String	执行动作 跳过：skip，告警：alert 示例值： alert
FileAction	是	否	String	监控行为 • read 读取文件 • write 修改文件 • read;write 读取或修改文件 示例值： read
ProcessPath	是	否	String	进程路径 示例值： /tmp/*

名称	必选	允许NULL	类型	描述
Target	是	否	String	被访问文件路径 示例值： /etc/shadow

AgentInstallResult

主机agent安装结果

被如下接口引用：DescribeAgentInstallResult、DescribeAgentInstallTaskResult、ModifyAssetsProtectionStatus

名称	必选	允许NULL	类型	描述
AppId	否	是	Uint64	appid信息 示例值： 1255080011
AssetId	否	是	String	资产ID 示例值： ins-fsguhjbf
Code	否	是	String	错误码： 空：成功 ErrLicenseNotEnough：授权不足 ErrStrTatNotOnline：tat客户端不在线 ErrStrAgentInstallTimeout：任务超时 ErrStrLicenseLocked: 授权操作中 示例值： ErrStrLicenseLocked
MemberId	否	是	String	member-id 示例值： member-jdkaghdjag
Message	否	是	String	错误信息 示例值： PayResourceChangingQuota
Region	否	是	String	地域 示例值： ap-region1

MaliciousRequestWhiteListInfo

恶意请求白名单列表信息

被如下接口引用：DescribeMaliciousRequestWhiteList

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	创建时间 示例值： 2021-02-08 14:46:25
Domain	是	否	String	域名 示例值： www.domain.com
Id	是	否	Uint64	白名单id 示例值： 1
Mark	是	否	String	备注 示例值： add redis cvm
ModifyTime	是	否	String	更新时间 示例值： 2021-02-08 14:46:25

ZoneInfo

可用区信息

被如下接口引用：DescribeBanRegions

名称	必选	允许NULL	类型	描述
ZoneName	是	否	String	可用区名称 示例值： zone1

JavaMemShellPluginSetting

Java内存马插件配置

被如下接口引用：DescribeJavaMemShellPluginList

名称	必选	允许NULL	类型	描述
Alias	是	否	String	服务器名 示例值： redis_node_cvm
CreateTime	是	否	String	创建时间 示例值： 2021-01-20 16:17:11
Exception	是	否	Uint64	插件是否存在异常 0: 正常 1: 异常 示例值： 0
HostIp	是	否	String	服务器ip 示例值： 192.168.255.10
JavaShellStatus	是	否	Uint64	javashell插件开关 0: 关闭 1: 开启 示例值： 1
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
ModifyTime	是	否	String	修改时间 示例值： 2021-01-20 16:17:1
Quuid	是	否	String	容器quuid 示例值： e1f081aa-7777-4fdf-a2f7-88f3faa3d302
Uuid	否	是	String	服务器uuid 示例值： e1f081aa-7777-4fdf-a2f7-88f3faa3d302

BashPolicy

高位命令策略

被如下接口引用：DescribeBashPolicies、ModifyBashPolicy

名称	必选	允许NULL	类型	描述
BashAction	是	否	Int64	0:告警 1:白名单 2:拦截 示例值： 1
Category	否	否	Int64	策略类型，0:系统 1:用户 示例值： 1

名称	必选	允许NULL	类型	描述
CreateTime	否	否	String	创建时间 示例值： 2020-12-12 00:00:00
DealOldEvents	否	是	Int64	是否处理旧事件为白名单 0=不处理 1=处理 示例值： 1
Descript	否	是	String	策略描述 示例值： 系统规则(标准)
Enable	是	否	Int64	1:有效 0:无效 示例值： 0
EventId	否	是	Int64	事件列表点击"加入白名单"时,需要传EventId 事件的id 示例值： 1
Id	否	否	Int64	策略ID 示例值： 1
Level	是	否	Int64	危险等级(0:无，1: 高危 2:中危 3: 低危) 示例值： 1
ModifyTime	否	否	String	修改时间 示例值： 2020-12-12 00:00:00
Name	是	否	String	策略名称 示例值： policy
Quuids	否	是	Array of String	生效主机的QUUID集合 示例值： ["d99a1b46-cc2d-4633-a11f-4a7663d25ay*"]
Rule	是	否	String	正则表达式 base64 加密,该字段废弃,如果写入则自动替换为Rules.Process.CmdLine 示例值： L2RhdGEvZGlybmFtZS8=
Rules	否	是	PolicyRules	规则表达式 示例值：查看
Scope	是	否	Int64	生效范围（0:一组quuid 1:所有专业版(包含旗舰版) 2:所有旗舰版 3:所有主机） 示例值： 1
Uuids	否	否	Array of String	老版本兼容可能会用到 示例值： ["d99a1b46-cc2d-4633-a11f-4a7663d25ay*"]
White	是	否	Int64	0:黑名单 1:白名单 示例值： 1

TagMachine

标签相关服务器信息

被如下接口引用：DescribeTagMachines

名称	必选	允许NULL	类型	描述
Id	是	否	String	ID 示例值： 100
MachineIp	是	否	String	主机内网IP 示例值： 192.168.0.204
MachineName	是	否	String	主机名称 示例值： tcs-dev3
MachineRegion	是	否	String	主机区域 示例值： None
MachineType	是	否	String	主机区域类型 示例值： CVM
MachineWanIp	是	否	String	主机外网IP 示例值： 192.168.0.204
Quuid	是	否	String	主机ID 示例值： 0096440e-9a9f-4e80-a82d-0b018637ayay

JavaMemShellInfo

java内存马事件信息

被如下接口引用：DescribeJavaMemShellList

名称	必选	允许NULL	类型	描述
Alias	否	是	String	服务器名称 示例值： dev-centos8
Annotations	否	是	String	注释 示例值： @Override
ClassName	否	是	String	类名 示例值： org.apache.catalina.startup.Bootstrap
CreateTime	否	否	String	首次发现时间 示例值： 2021-01-20 16:17:11
Description	否	否	String	说明 示例值： 检测到java进程pid为1128220的org.apache.catalina.startup.Bootstrap类中存在木马
HostIp	否	是	String	服务器IP 示例值： 192.168.255.10
Id	否	否	Uint64	事件ID 示例值： 142
Interfaces	否	是	String	继承的接口 示例值： org.apache.catalina.startup.Bootstrap
LoaderClassName	否	是	String	所属的类加载器 示例值： org.apache.catalina.startup.Bootstrap
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
Quuid	否	否	String	服务器quuid 示例值： e1f081aa-7777-4fdf-a2f7-88f3faa3d302
RecentFoundTime	否	否	String	最近检测时间 示例值： 2021-01-20 16:17:11
Status	否	否	Uint64	处理状态 0 -- 待处理 1 -- 已加白 2 -- 已删除 3 - 已忽略 4 - 已手动处理 示例值： 0
SuperClassName	否	是	String	父类名 示例值： org.apache.catalina.startup.Bootstrap

名称	必选	允许NULL	类型	描述
Type	否	否	Uint64	内存马类型 0:Filter型 1:Listener型 2:Servlet型 3:Interceptors型 4:Agent型 5:其他 示例值： 1
Uuid	否	是	String	服务器uuid 示例值： e1f081aa-7777-4fdf-a2f7-88f3faa3d302

LicenseBindTaskDetail

授权绑定任务详情

被如下接口引用：DescribeLicenseBindSchedule

名称	必选	允许NULL	类型	描述
ErrMsg	是	否	String	错误信息 示例值： 未查询到机器
FixMessage	否	是	String	修复建议 示例值： 资产管理-主机列表 点击同步资产
MachineExtraInfo	否	是	MachineExtraInfo	机器额外信息 示例值：查看
Quuid	是	否	String	云服务器UUID 示例值： 93b5fa8f-f5bc-4cf9-8253-d2739e5aa484
Status	是	否	Uint64	0 执行中, 1 成功,2失败 示例值： 2

BruteAttackRule

标准阻断模式规则

被如下接口引用：ModifyBruteAttackRules

名称	必选	允许NULL	类型	描述
LoginFailTimes	是	否	Uint64	爆破事件失败次数 示例值： 6
TimeRange	是	否	Uint64	爆破事件发生的时间范围，单位：秒 示例值： 1

MaCustomPolicyWorkload

被如下接口引用：DescribeMaCustomPolicyList、ModifyMaCustomPolicy

名称	必选	允许NULL	类型	描述
Id	是	是	Uint64	工作负载ID 示例值： 1
Name	是	是	String	工作负载名字 示例值： workload1
Type	是	是	Uint64	负载类型 • 0 主机负载 • 1 POD负载 示例值： 1

MalWareList

木马列表集合

被如下接口引用：DescribeMalWareList

名称	必选	允许NULL	类型	描述
Alias	否	否	String	主机别名 示例值： redis_node_cvm
CheckPlatform	否	否	String	'木马检测平台用,分割 1云查杀引擎、2TAV、3binaryAi、4异常行为、5威胁情报 示例值： 1
CreateTime	否	否	String	创建时间 示例值： 2024-10-30 09:12:22
FileCreateTime	否	是	String	首次运行时间 示例值： 2024-10-30 09:12:22
FileExists	否	否	Uint64	木马文件是否存在 0:不存在，1:存在 示例值： 1
FileModifierTime	否	是	String	最近运行时间 示例值： 2024-10-30 09:12:22
FilePath	否	否	String	路径 示例值： /tmp/any
HostIp	否	否	String	服务器ip 示例值： 10.0.0.1
Id	否	是	Uint64	唯一ID 示例值： 1
LatestScanTime	否	否	String	最近扫描时间 示例值： 2024-10-30 09:12:22
Level	否	否	Uint64	风险等级 0未知、1低、2中、3高、4严重 示例值： 1
MD5	否	否	String	木马样本md5 示例值： 708cae4cf814c3deda4208da228fad4e
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
ProcessExists	否	否	Uint64	木马进程是否存在 0:不存在，1:存在 示例值： 1
Quuid	否	否	String	cvm quuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
Status	否	否	Uint64	状态；4-待处理，5-已信任，6-已隔离，8-文件已删除, 14:已处理，13-已加白 示例值： 4
Tags	否	是	Array of String	特性标签，已废弃字段，不会再返回标签，详情中才会返回标签信息 示例值： ["tag1"]

名称	必选	允许NULL	类型	描述
Uuid	否	否	String	唯一UUID 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
VirusName	否	否	String	病毒名称 示例值： Linux.Trojan.Downloader.Snkl

AssetCoreModuleDetail

资产管理内核模块详情

被如下接口引用：DescribeAssetCoreModuleInfo

名称	必选	允许NULL	类型	描述
Desc	是	否	String	描述信息 示例值： module
Modules	是	否	String	被依赖模块 示例值： module
Name	是	否	String	名称 示例值： teat
Params	是	是	Array of AssetCoreModuleParam	参数信息 示例值：查看
Path	是	否	String	路径 示例值： /root
Processes	是	否	String	依赖进程 示例值： 10011
Size	是	否	Uint64	大小 示例值： 102
UpdateTime	是	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
Version	是	否	String	版本 示例值： 1.0.1

UsualPlace

常用登录地

被如下接口引用：DescribeUsualLoginPlaces

名称	必选	允许NULL	类型	描述
CityId	是	否	Uint64	城市 ID。 示例值： 101
CountryId	是	否	Uint64	国家 ID。 示例值： 2
Id	是	否	Uint64	ID。 示例值： 13267
ProvinceId	是	否	Uint64	省份 ID。 示例值： 21
Uuid	是	否	String	主机安全客户端唯一标识UUID。 示例值： 69E78F7F-FFC7-47D1-B406-13C9852ayayay

UuidHostip

过检机器和对应的hostip

被如下接口引用：DescribeMemShellRules、DescribeReverseShellRulesAggregation

名称	必选	允许NULL	类型	描述
Hostip	否	是	String	服务器ip 示例值： 172.16.0.9
Uuid	否	是	String	服务器id 示例值： 82727b6e-3676-4660-ac4e-c281dba1b23f

SecurityDynamic

安全事件消息数据。

被如下接口引用：DescribeSecurityDynamics

名称	必选	允许NULL	类型	描述
EventTime	是	否	Datetime	安全事件发生时间。 示例值： 2018-01-01 00:00:00
EventType	是	否	String	安全事件类型。 • MALWARE：木马事件 • NON_LOCAL_LOGIN：异地登录 • BRUTEATTACK_SUCCESS：密码破解成功 • VUL：漏洞 • BASELINE：安全基线 示例值： BASELINE
Message	是	否	String	安全事件消息。 示例值： 事件消息
SecurityLevel	是	否	String	安全事件等级。 • RISK: 严重 • HIGH: 高危 • NORMAL: 中危 • LOW: 低危 • UNKNOWNED: 可疑 示例值： High
Uuid	是	否	String	主机安全客户端UUID。 示例值： 5a540076-d38a-4078-aa98-q45rt371d322

VulFixStatusInfo

查看漏洞修复详情

被如下接口引用：DescribeVulFixStatus

名称	必选	允许NULL	类型	描述
FailCnt	是	是	Uint64	漏洞修复失败主机数量 示例值： 1
FixMethod	否	是	Uint64	修复方式 0组件更新或者安装补丁,1禁用服务 示例值： 0
FixSuccessCnt	是	是	Uint64	修复成功的数量 示例值： 0
HostList	是	是	Array of VulFixStatusHostInfo	漏洞对应主机修复状态 示例值：查看
Progress	是	否	Uint64	漏洞修复进度 1-100； 示例值： 80
VulId	是	是	Uint64	漏洞id 示例值： 12
VulName	是	是	String	漏洞名称 示例值： Apache HTTP/2 协议拒绝服务漏洞(CVE-2023-44487)

BaselinePolicy

基线策略信息

被如下接口引用：DescribeBaselinePolicyList、ModifyBaselinePolicy

名称	必选	允许NULL	类型	描述
AssetType	是	否	Int64	资产类型[0:所有专业版旗舰版
DetectInterval	是	否	Int64	检测间隔[1:1天
DetectTime	是	否	String	检测时间 示例值： 09:00:00
HostCount	否	否	Int64	关联基线主机数目 示例值： 0
HostIds	否	否	Array of String	主机Id 示例值： ["116d84e9-22d3-4fa3-a31b-a1e58f2bayay"]
HostIps	否	否	Array of String	主机Ip 示例值： ["1.1.1.1"]
IsDefault	否	否	Int64	是否是系统默认 示例值： 0
IsEnabled	是	否	Int64	是否开启[0:未开启
ItemCount	否	否	Int64	关联基线项数目 示例值： 1419
PolicyId	否	否	Int64	策略Id 示例值： 902471
PolicyName	是	否	String	策略名称,长度不超过128英文字符 示例值： 国际标准基线
RuleCount	否	否	Int64	关联基线项数目 示例值： 12
RuleIds	否	否	Array of Int64	规则Id 示例值： [11]

HostTagInfo

主机与主机标签信息

被如下接口引用：DescribeHostInfo

名称	必选	允许NULL	类型	描述
AliasName	否	是	String	主机名 示例值： redis_node_cvm
CloudTags	否	是	Array of Tags	云标签信息 示例值：查看
HostIp	否	是	String	主机内网Ip 示例值： 1.2.3.4
InstanceID	否	是	String	主机instance ID 示例值： ins-dada
KernelVersion	否	是	String	内核版本号 示例值： 5.1.0
MachineStatus	否	是	String	主机在线状态 ONLINE，OFFLINE 示例值： ONLINE
MachineWanIp	否	是	String	主机公网ip 示例值： 10.0.0.1
ProtectType	否	是	String	防护版本 BASIC_VERSION 基础版, PRO_VERSION 专业版 Flagship 旗舰版 示例值： BASIC_VERSION
Quuid	否	是	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
TagList	否	是	Array of String	主机标签名数组 示例值： ["dev"]
Uuid	否	是	String	主机uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
VulNum	否	是	Int64	漏洞数 示例值： 32

AssetDiskPartitionInfo

资产管理磁盘分区信息

被如下接口引用：DescribeAssetDiskList、DescribeAssetMachineDetail

名称	必选	允许NULL	类型	描述
Name	是	否	String	分区名 示例值： /dev/vda1

名称	必选	允许NULL	类型	描述
Path	是	否	String	挂载目录 示例值： /data
Percent	是	否	Float	分区使用率 示例值： 78.81294
Size	是	否	Uint64	分区大小：单位G 示例值： 50
Type	是	否	String	文件系统类型 示例值： ext4
Used	是	否	Uint64	已使用空间：单位G 示例值： 26

JavaMemShellPluginInfo

Java内存马插件信息

被如下接口引用：DescribeJavaMemShellPluginInfo

名称	必选	允许NULL	类型	描述
ErrorLog	是	否	String	错误日志 示例值： 1736132722
MainClass	是	否	String	注入进程主类 示例值： main.class
Pid	是	否	Uint64	注入进程pid 示例值： 12
Status	是	否	Uint64	注入状态：0: 注入中, 1: 注入成功, 2: 插件超时, 3: 插件退出, 4: 注入失败 5: 软删除 示例值： 1

AssetCoreModuleParam

资产管理内核模块参数

被如下接口引用：DescribeAssetCoreModuleInfo

名称	必选	允许NULL	类型	描述
Data	是	否	String	数据 示例值： 16384
Name	是	否	String	名称 示例值： hashsize

AssetMachineDetail

资产指纹中服务器列表的基本信息

被如下接口引用：DescribeAssetMachineDetail

名称	必选	允许NULL	类型	描述
AgentVersion	否	否	String	agent版本 示例值： 1.2.3.1
BootTime	否	否	String	系统启动时间 示例值： 2021-12-21
BuyTime	否	否	String	专业版开通时间 示例值： 2021-12-21
CoreVersion	否	否	String	内核版本 示例值： 3.10.0-1160.99.1.el7.x8ayay
Cpu	否	否	String	CPU信息 示例值： Intel(R) Xeon(R) Platinum 8255C CPU @ 192.168.0.204
CpuLoad	否	否	String	Cpu负载 示例值： 中
CpuLoadVul	否	是	String	CpuLoadVul 示例值： 10.1
CpuSize	否	否	Uint64	Cpu数量 示例值： 2
DeviceVersion	否	否	String	设备型号 示例值： CVM
DiskLoad	否	否	String	硬盘使用率百分比 示例值： 11
DiskSize	否	否	Uint64	硬盘容量：单位G 示例值： 11
Disks	否	否	Array of AssetDiskPartitionInfo	分区 示例值：查看
EndTime	否	否	String	专业版到期时间 示例值： 2021-12-21
FirstTime	否	是	String	时间 示例值： 2021-02-01 12:00:00
InstallTime	否	否	String	安装时间 示例值： 2021-12-21
InstanceId	否	是	String	主机ID 示例值： cvm-112234
LastLiveTime	否	否	String	最后上线时间 示例值： 2021-12-21
MachineExtraInfo	否	是	MachineExtraInfo	主机信息 示例值：查看
MachineIp	否	否	String	服务器内网IP 示例值： 11.22.33.44
MachineName	否	否	String	服务器名称 示例值： txbj-k8s-main-192.168.0.204
MachineWanIp	否	否	String	主机外网IP 示例值： 1.2.3.4
MemLoad	否	否	String	内存使用率百分比 示例值： 11

名称	必选	允许NULL	类型	描述
MemSize	否	否	Uint64	内存容量：单位G 示例值： 11
NetCards	否	否	Array of AssetNetworkCardInfo	网卡 示例值：查看
OfflineTime	否	是	String	离线时间 示例值： 2021-12-21
OsInfo	否	否	String	操作系统名称 示例值： centos
OsType	否	否	String	Linux/Windows 示例值： Linux
PartitionCount	否	否	Uint64	分区数 示例值： 1
Producer	否	否	String	生产商 示例值： Cloud Cayay
ProjectId	否	否	Uint64	业务组ID 示例值： 1241252
ProtectDays	否	否	Uint64	已防护天数 示例值： 11
ProtectLevel	否	否	Uint64	防护级别：0基础版，1专业版，2旗舰版，3普惠版 示例值： 1
Quuid	否	否	String	服务器Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
RiskStatus	否	否	String	风险状态：UNKNOW-未知，RISK-风险，SAFT-安全 示例值： RISK
SerialNumber	否	否	String	序列号 示例值： 641eb296-411e-45b5-8003-903d4f4aayay
Status	否	否	Uint64	0在线，1已离线 示例值： 1
UpdateTime	否	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
Uuid	否	否	String	服务器uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

IgnoreBaselineRule

忽略的基线检测项信息

被如下接口引用：DescribeIgnoreBaselineRule

名称	必选	允许NULL	类型	描述
EffectHostCount	是	是	Uint64	影响主机数 示例值： 10
Fix	是	是	String	修复建议 示例值： 1. 改用更复杂的密码，推荐字母、数字、特殊符号组合，长度高于 10 位；\n2. 选择使用云 CDB。\n3. 如果直接删除账户，需执行 OPTIMIZE TABLE mysql.user; 命令进ayay
ModifyTime	是	是	String	更新时间 示例值： 2021-02-01 12:00:00
RuleId	是	是	Uint64	基线检测项id 示例值： 1103
RuleName	是	是	String	基线检测项名称 示例值： Redis 基线合规检测

PrivilegeEventInfo

本地提权数据

被如下接口引用：DescribePrivilegeEventInfo

名称	必选	允许NULL	类型	描述
CmdLine	是	否	String	执行命令 示例值： /bin/nginx
CreateTime	是	否	String	发生时间 示例值： 2024-10-30 02:19:08
FullPath	是	否	String	进程路径 示例值： /bin/nginx
HarmDescribe	是	否	String	危害描述信息 示例值： 黑客在入侵服务器后，为了进行下一步的恶意操作，会执行恶意文件下载、连接矿池、添加公钥、查看敏感文件等操作。
HostIp	是	否	String	主机内网IP 示例值： 10.0.0.1
Id	是	否	Uint64	数据ID 示例值： 1
MachineName	是	否	String	机器名 示例值： ins-agent
MachineStatus	是	否	String	主机在线状态 OFFLINE ONLINE 示例值： ONLINE
MachineWanIp	是	否	String	主机外网ip 示例值： 124.2.4.55
ModifyTime	是	否	String	处理时间 示例值： 2021-03-30 19:17:28
NewCaps	是	否	String	权限列表
ParentProcGroup	是	否	String	父进程用户组 示例值： root
ParentProcName	是	否	String	父进程名 示例值： /bin/ssh
ParentProcPath	是	否	String	父进程路径 示例值： /bin/ssh
ParentProcUser	是	否	String	父进程用户名 示例值： root
ProcFilePrivilege	是	否	String	进程文件权限 示例值： rwx

名称	必选	允许NULL	类型	描述
ProcessName	是	否	String	进程名 示例值： nginx
PsTree	是	否	String	进程树 json pid:进程id，exe:文件路径 ，account:进程所属用组和用户 ,cmdline:执行命令，ssh_service: SSH服务ip, ssh_soure:登录源 示例值： {"pid":"143","account":"root","exe":"/tmp"}
Quuid	是	否	String	主机uuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
References	是	否	Array of String	参考链接 示例值： ["http://www.domain.com"]
Status	是	否	Uint64	处理状态：0-待处理 2-白名单 3-已处理 4-已忽略 示例值： 0
SuggestScheme	是	否	String	建议方案 示例值： 1.检查恶意进程及非法端口，删除可疑的启动项和定时任务； 2.隔离或者删除相关的木马文件；
Tags	是	否	Array of String	标签 示例值： ["redis_use","nginx_use"]
UserGroup	是	否	String	用户组 示例值： root
UserName	是	否	String	用户名 示例值： root
Uuid	是	否	String	主机安全uuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0

ScreenProtectionCnt

大屏可视化主机安全返回态势数据

被如下接口引用：DescribeScreenProtectionCnt

名称	必选	允许NULL	类型	描述
Count	是	否	Uint64	总数 示例值： 12
Name	是	否	String	cloud：云查杀引擎，detect：检测引擎，defend：攻击防御，threat：威胁情报，analysis：异常分析，ai：AI引擎 示例值： 威胁情报
Type	是	否	String	cloud：云查杀引擎，detect：检测引擎，defend：攻击防御，threat：威胁情报，analysis：异常分析，ai：AI引擎 示例值： cloud

Tags

平台标签

被如下接口引用：CreateLicenseOrder、DescribeHostInfo、DescribeImportMachineInfo、DescribeLicenseList、DescribeMachineList、DescribeMachines、DescribeMachinesSimple、DescribeOrderList、DescribeVulEffectHostList、ExportLicenseDetail、ModifyOrder

名称	必选	允许NULL	类型	描述
TagKey	是	否	String	标签键 示例值： business1
TagValue	是	否	String	标签值 示例值： businessValue

AssetCoreModuleBaseInfo

资产管理内核模块列表

被如下接口引用：DescribeAssetCoreModuleList

名称	必选	允许NULL	类型	描述
Desc	否	否	String	描述信息 示例值： system
FirstTime	否	否	String	首次采集时间 示例值： 2022-07-15 11:27:01
Id	否	否	String	模块ID 示例值： 10001
IsNew	否	否	Int64	是否新增[0:否
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	否	String	服务器IP 示例值： 1.1.1.1
MachineName	否	否	String	服务器名称 示例值： any-ins
MachineWanIp	否	否	String	服务器外网IP 示例值： 1.1.1.1
ModuleCount	否	否	Uint64	依赖模块数 示例值： 0
Name	否	否	String	名称 示例值： core.package
OsInfo	否	否	String	操作系统 示例值： centos-64bit
Path	否	否	String	路径 示例值： /root
ProcessCount	否	否	Uint64	依赖进程数 示例值： 0
Quuid	否	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Size	否	否	Uint64	模块大小 示例值： 10001
UpdateTime	否	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
Uuid	否	否	String	主机uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Version	否	否	String	版本 示例值： 1.0.0.1

AssetWebFrameBaseInfo

资源管理Web应用列表信息

被如下接口引用：DescribeAssetWebFrameList

名称	必选	允许NULL	类型	描述
FirstTime	否	否	String	首次采集时间 示例值： 2022-07-15 11:27:01
IsNew	否	否	Int64	是否新增[0:否
Lang	否	否	String	语言 示例值： eng
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	否	String	主机内网IP 示例值： 1.1.1.1.
MachineName	否	否	String	主机名称 示例值： redis_node_cvm
MachineWanIp	否	否	String	主机外网IP 示例值： 1.1.1.1
Name	否	否	String	Web应用名 示例值： Nginx
OsInfo	否	否	String	操作系统信息 示例值： Centos 64Bit
Path	否	是	String	应用路径 示例值： /root
ProjectId	否	否	Uint64	主机业务组ID 示例值： 1
Quuid	否	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
ServiceType	否	否	String	服务类型 示例值： tcp
Tag	否	是	Array of MachineTag	主机标签 示例值：查看
UpdateTime	否	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
Uuid	否	否	String	主机Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Version	否	否	String	版本 示例值： 1.0.1

MachineLoginType

主机登录方式

被如下接口引用：DescribeMachineLoginType

名称	必选	允许NULL	类型	描述
InstanceId	否	是	String	实例ID 示例值： inxs-36843684
LoginType	否	是	Uint64	登录方式：0-原始登录方式，1-扫码免密登录，2-开启扫码中，3-关闭扫码中 示例值： 0
Quuid	否	是	String	主机Quuid 示例值： cf706bb3-ebac-47c4-aa68-171888888888

AssetSystemPackageInfo

资源管理系统安装包列表信息

被如下接口引用：DescribeAssetSystemPackageList

名称	必选	允许NULL	类型	描述
Desc	是	否	String	描述信息 示例值： utils
FirstTime	是	否	String	首次采集时间 示例值： 2022-07-15 11:27:01
InstallTime	是	否	String	安装时间 示例值： 2024-10-23 14:17:00
IsNew	是	否	Int64	是否新增[0:否
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	是	否	String	主机IP 示例值： 1.1.1.1
MachineName	是	否	String	主机名称 示例值： redis_node_cvm
Name	是	否	String	Package名子 示例值： libevdev
OsInfo	是	否	String	操作系统 示例值： Centos
Quuid	否	是	String	主机Id 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Type	是	否	String	package type (rpm dpkg java system) 示例值： rpm
UpdateTime	是	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
Uuid	否	是	String	Agent Id 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Version	是	否	String	版本 示例值： 1.0.1

BaselineHostTopList

基线影响服务器列表数据

被如下接口引用：DescribeBaselineHostTop

名称	必选	允许NULL	类型	描述
EventLevelList	是	是	Array of BaselineEventLevelInfo	事件等级与次数列表 示例值：查看
HostName	是	是	String	主机名称 示例值： v_vxnnzhayay
Quuid	是	是	String	主机Quuid 示例值： fcf85fc9-f45e-457a-bca4-fcae074eayay
Score	是	是	Uint64	计算权重的分数 示例值： 20

FileTamperRuleDetail

核心文件监控规则详情

被如下接口引用：DescribeFileTamperEventRuleInfo、DescribeFileTamperRuleInfo

名称	必选	允许NULL	类型	描述
AddWhiteType	否	是	String	加白处理类型 • cur 仅对当前加白 • all 所有符合条件加白 示例值： cur
CreateTime	是	否	String	创建时间 示例值： 2021-10-13T11:15:06+08:00
Id	是	否	Uint64	规则id 示例值： 1
IsGlobal	是	否	Uint64	是否全局规则(默认否) 0：否 ，1：是 示例值： 1
Level	是	否	Uint64	风险等级 0：无， 1: 高危， 2:中危， 3: 低危 示例值： 1
ModifyTime	是	否	String	更新时间 示例值： 2021-10-13T11:15:06+08:00
Name	是	是	String	规则名称 示例值： 禁止访问
Rule	是	否	Array of FileTamperRule	规则 示例值：查看
Status	是	否	Uint64	状态 0: 启用 1: 已关闭 示例值： 1
UuidTotalCount	是	否	Uint64	生效主机的总数 示例值： 17
Uuids	是	是	Array of String	生效主机uuid,空表示全部主机，通过参数可控制返回的条数 示例值： ["935e27b1-d675-4509-80bf-96fbf0764237"]

RiskMainClass

内存马和rasp注入时候的风险服务

被如下接口引用：DescribeInjectRiskyServiceSwitch

名称	必选	允许NULL	类型	描述
ServiceName	否	是	String	rasp注入时候的风险服务 示例值： 1

AssetMachineBaseInfo

资产指纹中服务器列表的基本信息

被如下接口引用：DescribeAssetMachineList

名称	必选	允许NULL	类型	描述
Cpu	否	否	String	CPU信息 示例值： Intel(R) Xeon(R) Gold 6148 CPU @ 2.40GHz
CpuLoad	否	否	String	Cpu使用率百分比 示例值： 54.2
CpuLoadNum	否	是	String	cpu负载读数（仅linux系统有效） 示例值： 0
CpuSize	否	否	Uint64	Cpu数量 示例值： 1
DiskLoad	否	否	String	硬盘使用率百分比 示例值： 22.4
DiskSize	否	否	Uint64	硬盘容量：单位G 示例值： 100
FirstTime	否	否	String	首次采集时间 示例值： 2022-07-15 11:27:01
IsNew	否	否	Int64	是否新增[0:否
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	否	String	服务器内网IP 示例值： 10.0.0.11
MachineName	否	否	String	服务器名称 示例值： any-machine
MachineWanIp	否	否	String	主机外网IP 示例值： 112.22.662.11
MemLoad	否	否	String	内存使用率百分比 示例值： 22.5
MemSize	否	否	Uint64	内存容量：单位G 示例值： 1024
OsInfo	否	否	String	操作系统名称 示例值： windows

名称	必选	允许NULL	类型	描述
PartitionCount	否	否	Uint64	分区数 示例值： 1
ProjectId	否	否	Uint64	业务组ID 示例值： 1
Quuid	否	否	String	服务器Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Tag	否	是	Array of MachineTag	标签 示例值：查看
UpdateTime	否	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
Uuid	否	否	String	服务器uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

BanWhiteList

阻断白名单规则

被如下接口引用：CreateBanWhiteList、ModifyBanWhiteList

名称	必选	允许NULL	类型	描述
CreateTime	否	否	Datetime	创建白名单时间。 示例值： 2021-01-01 00:00:00
Id	否	否	String	白名单ID。 示例值： id_10001
IsGlobal	否	是	Bool	白名单是否全局 示例值： false
ModifyTime	否	否	Datetime	修改白名单时间。 示例值： 2021-01-01 00:00:00
Quuids	否	是	Array of String	白名单所属机器列表 示例值： ["1ce68339-8828-457f-b358-d5b1b34e4fe9"]
Remark	否	否	String	白名单别名。 示例值： 别名
SrcIp	否	否	String	阻断来源IP。 示例值： 1.1.1.1
Uuid	否	是	String	白名单所属机器。 示例值： 1ce68339-8828-457f-b358-d5b1b34e4fe9

ProtectDirRelatedServer

防护目录关联服务器列表信息

被如下接口引用：DescribeProtectDirRelatedServer

名称	必选	允许NULL	类型	描述
Authorization	否	否	Bool	是否已经授权 示例值： true
AutoRestoreSwitchStatus	否	否	Uint64	自动恢复开关 示例值： 0
Exception	否	否	Uint64	异常状态 示例值： 0
ExceptionMessage	否	否	String	异常信息 示例值： 启动中
HostIp	否	否	String	服务器IP 示例值： 192.168.0.204
HostName	否	否	String	服务器名称 示例值： redis_node_cvm
Id	否	否	String	唯一ID 示例值： 6961
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
MachineOs	否	否	String	服务器系统 示例值： CentOS 192.168.0.204
Progress	否	否	Uint64	过渡进度 示例值： 0
ProtectStatus	否	否	Uint64	防护状态 示例值： 6
ProtectSwitch	否	否	Uint64	防护开关 示例值： 0
Quuid	否	否	String	服务器唯一ID 示例值： 8ce366dc-624e-429c-a8da-5ab870ecayay
RelateDirNum	否	否	Uint64	关联目录数 示例值： 0

ProtectEventLists

防护事件列表信息

被如下接口引用：DescribeWebPageEventList

名称	必选	允许NULL	类型	描述
CreateTime	否	否	String	发现时间 示例值： 2020-10-01 01:01:10
EventDir	否	否	String	事件地址 示例值： event
EventStatus	否	否	Uint64	事件状态 1 已恢复 0 未恢复 示例值： 0
EventType	否	否	Uint64	事件类型 0-内容被修改恢复；1-权限被修改恢复；2-归属被修改恢复；3-被删除恢复；4-新增删除 示例值： 0
FileType	否	否	Uint64	文件类型 0-常规文件；1-目录；2-软链 示例值： 0

名称	必选	允许NULL	类型	描述
HostIp	否	否	String	服务器ip 示例值： 172.16.100.1
HostName	否	否	String	服务器名称 示例值： host1
Id	否	否	Uint64	唯一ID 示例值： 1
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
Quuid	否	是	String	机器实例uuid 示例值： 8c09e1b1-5611-45b3-9c02-737996011b81
RestoreTime	否	否	String	恢复时间 示例值： 2020-10-01 01:01:10

OrderData

订单参数

被如下接口引用：ModifyOrder

名称	必选	允许NULL	类型	描述
AutoRenewFlag	否	是	Uint64	自动续费标签 0 默认不自动续费(大客户特权会自动续费的) 1 自动续费 2 手动设置不自动续费(大客户特权不会自动续费) 示例值： 1
InquireKey	是	是	String	计费项 sv_ 示例值： sv_yunjing_ue_x
InquireNum	否	是	Uint64	购买用量,最大99999 示例值： 1
NewConfig	否	是	OrderModifyConfig	新订单配置,变配时需要传 示例值：查看
OldConfig	否	是	OrderModifyConfig	旧订单配置,变配时需要传 示例值：查看
PayMode	是	是	Uint64	计费模式 0 后付费 1预付费(包年包月) 示例值： 1
ProjectID	否	是	Uint64	项目ID 示例值： 1
RegionID	是	是	Uint64	地域ID 示例值： 1
RenewConfig	否	是	OrderRenewConfig	续费配置参数 示例值：查看
ResourceId	否	是	String	资源ID 示例值： fgtw324qerg3423221dsa231
SubProductCode	是	是	String	子产品 sp_ 示例值： sp_yunjing_0014
Tags	否	是	Array of Tags	云标签,需要同步绑定标签则传 示例值：查看
TimeSpan	否	是	Uint64	购买时长 时间长度，新购续费下单为int；变配时不用传 示例值： 1
TimeUnit	否	是	String	购买时间单位 年：y，月：m，日：d，时：h，分：M，秒：s，无计费周期：p 示例值： 2020-02-01 12:00:00
ZoneID	是	是	Uint64	可用区ID 示例值： 1

OrderRenewConfig

订单续费参数

被如下接口引用：ModifyOrder

名称	必选	允许NULL	类型	描述
SubProductCode	是	是	String	二层子产品, 续费的目标子产品 示例值： sp_yunjing_vas
TimeSpan	是	是	Uint64	时间长度，最小为1,最大36 示例值： 36
TimeUnit	是	是	String	时间单位 年：y，月：m 示例值： y

MemShellRule

内存马白名单规则

被如下接口引用：DescribeMemShellRules

名称	必选	允许NULL	类型	描述
AnnotationsRegexp	否	是	String	注释正则表达式，为空则不匹配 示例值： org.apache.catalina.startup.Bootstrap
CallStackRegexp	否	是	String	调用栈正则表达式，为空则不匹配 示例值： eval
ClassNameRegexp	否	是	String	类名正则表达式，为空则不匹配 示例值： webshell_filter
CodeSourceRegexp	否	是	String	源代码正则表达式，为空则不匹配 示例值： eval
CreateTime	否	是	String	创建时间 示例值： 2024-09-20 15:32:26
FileExist	否	是	Uint64	文件是否存在， 0:用户没选择规则时候的默认值，1：文件存在，2：文件不存在 示例值： 0
GroupID	否	是	String	批次id 示例值： ece9dcb3-e427-4ded-ac6f-727cce79130b
GroupName	否	是	String	策略名称 示例值： check_for_redis
HandleHistory	否	是	Uint64	处理历史事件， 0:不处理 1:处理 示例值： 1

名称	必选	允许NULL	类型	描述
Id	否	是	Uint64	规则ID 示例值： 12
InterfacesRegexp	否	是	String	继承的接口正则表达式，为空则不匹配 示例值： org.apache.catalina.startup.Bootstrap
IsGlobal	否	是	Uint64	是否全局规则(是否对appid下所有主机有效， 0:单台uuid 1:全局，默认否) 示例值： 0
LoaderClassNameRegexp	否	是	String	所属的类加载器正则表达式，为空则不匹配 示例值： org.apache.catalina.startup.Bootstrap
LogicalSymbol	否	是	Uint64	逻辑运算符，0: 下面5个有效的正则逻辑与 1: 逻辑或 示例值： 0
MachinesNums	否	是	String	应用资产，描述服务器数量，全局时候为：全部服务器 示例值： 2
ModifyTime	否	是	String	修改时间 示例值： 2024-11-03 15:09:33
Operator	否	是	String	操作人 示例值： Alice
Status	否	是	Uint64	状态 (0: 有效 1: 删除，2：无效（启用开关关闭）) 示例值： 0
SuperClassNameRegexp	否	是	String	父类名正则表达式，为空则不匹配 示例值： org.apache.catalina.startup.Bootstrap
UuidHostips	否	是	Array of UuidHostip	客户端ID 示例值：查看

LogHistogram

直方图周期内统计结果详情

被如下接口引用：DescribeLogHistogram

名称	必选	允许NULL	类型	描述
Count	是	否	Int64	统计周期内的日志条数 示例值： 0
TimeStamp	是	否	Int64	按 period 取整后的 unix timestamp： 单位毫秒 示例值： 0

BaselineRule

基线规则

被如下接口引用：DescribeBaselineRuleIgnoreList、DescribeBaselineRuleList、ModifyBaselineRule

名称	必选	允许NULL	类型	描述
AssetType	否	是	Int64	[0:所有专业版旗舰版
CategoryId	否	否	Int64	规则分类 示例值： 1
HostCount	否	否	Int64	主机数 示例值： 0
HostIds	否	是	Array of String	主机Id集合 示例值： ["F00A8503-6233-452E-913E-DAFEE9ayayay", "E3CB79D9-8892-408C-AE2D-A90059ayayay"]
HostIps	否	是	Array of String	主机IP 示例值： ["10.0.1.11","10.0.0.12"]
Items	否	否	Array of Item	适配项ID列表 示例值：查看
RuleDesc	否	否	String	规则描述 示例值： 国际标准-CentOS 6安全基线检查
RuleId	否	否	Int64	规则Id 示例值： 11
RuleName	是	否	String	规则名称,长度不超过128英文字符 示例值： 国际标准-CentOS 6安全基线检查
RuleType	否	否	Int64	规则类型 [0:系统

ScreenEventsCnt

统计入侵检测

被如下接口引用：DescribeScreenEventsCnt

名称	必选	允许NULL	类型	描述
Category	是	否	Array of ScreenNameValue	name 具体展示内容类型： 攻击事件, 潜在风险, 失陷资产, 潜在风险资产 Value: 事件统计数 示例值：查看
Title	是	否	String	展示内容：待处理风险总数，影响资产总数 示例值： 待处理风险总数
Total	是	否	Uint64	事件总数 示例值： 12

BruteAttackRuleList

暴力破解判定规则列表

被如下接口引用：DescribeBruteAttackRules

名称	必选	允许NULL	类型	描述
Enable	是	否	Bool	规则是否为空，为空则填充默认规则 示例值： true
LoginFailTimes	是	否	Uint64	爆破事件失败次数 示例值： 5
LoginFailTimesDefault	是	否	Uint64	爆破事件失败次数（默认规则） 示例值： 10
TimeRange	是	否	Uint64	爆破事件发生的时间范围，单位：秒 示例值： 5

名称	必选	允许NULL	类型	描述
TimeRangeDefault	是	否	Uint64	爆破事件发生的时间范围，单位：秒（默认规则） 示例值： 1

ClsTopicInfo

日志主题信息

被如下接口引用：DescribeClsTopics

名称	必选	允许NULL	类型	描述
AssumerName	否	是	String	云产品标识 示例值： CWP
CreateTime	否	是	String	创建时间 示例值： 2021-04-01 08:00:00
LogsetId	否	是	String	所属日志集ID 示例值： 34526
TopicId	否	是	String	主题ID 示例值： topic_redis_node
TopicName	否	是	String	主题名称 示例值： topic_redis_node

NetAttackEvent

被如下接口引用：DescribeAttackEvents

名称	必选	允许NULL	类型	描述
Count	否	是	Uint64	攻击次数 示例值： 1
DstPort	否	是	Uint64	目标端口 示例值： 443
Id	否	是	Uint64	日志ID 示例值： 49992719
Location	否	是	String	来源地 示例值： location1-location2
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
MergeTime	否	是	String	攻击时间 示例值： 2021-02-01 12:00:00
New	否	是	Bool	是否今日新增主机 示例值： false
PayVersion	否	是	Uint64	机器付费版本，0 基础版，1专业版，2旗舰版，3普惠版 示例值： 1
Quuid	否	是	String	cvm uuid 示例值： ebc62d3a-a4de-46ad-a0d5-b94cb8fdayay
SrcIP	否	是	String	来源IP 示例值： 192.168.0.204
Status	否	是	Uint64	处理状态，0 待处理 1 已处理 2 已加白 3 已忽略 4 已删除 5: 已开启防御 示例值： 0
Type	否	是	Uint64	攻击状态，0: 尝试攻击 1: 实锤攻击(攻击成功) 示例值： 0
Uuid	否	是	String	客户端ID 示例值： ebc62d3a-a4de-46ad-a0d5-b94cb8fdayay
VulDefenceStatus	否	是	Uint64	是否开启漏洞防御，0关1开 示例值： 0
VulId	否	是	Uint64	漏洞id 示例值： 100377
VulName	否	是	String	漏洞名称 示例值： Apache HTTP/2 协议拒绝服务漏洞(CVE-2023-44487)
VulSupportDefense	否	是	Uint64	漏洞是否支持防御，0:不支持 1:支持 示例值： 0

ScreenInvasion

大屏入侵事件详情

被如下接口引用：DescribeScreenHostInvasion

名称	必选	允许NULL	类型	描述
Content	是	否	String	事件数据的json, 每种事件不同， 【文件查杀】病毒名 VirusName、文件名 FileName、文件路径 FilePath、文件大小 FileSize、文件MD5 MD5、首次发现时间 CreateTime、最近检测时间LatestScanTime、危害描述 HarmDescribe、修复建议SuggestScheme 【异常登录】来源IP SrcIp、来源地 Location、登录用户名 UserName、登录时间 LoginTime 【密码破解】来源IP SrcIp、来源地 City,Country、协议 Protocol、登录用户名UserName 、端口 Port、尝试次数 Count、首次攻击时间 CreateTime、最近攻击时间 ModifyTime 【恶意请求】恶意请求域名 Url、进程ProcessName 、MD5 ProcessMd5、PID Pid、请求次数 AccessCount、最近请求时间 MergeTime、危害描述 HarmDescribe、修复建议SuggestScheme 【高危命令】命中规则名 RuleName、规则类别 RuleCategory、命令内容 BashCmd、数据来源 DetectBy、登录用户 User、PID Pid、发生时间 CreateTime 、危害描述 HarmDescribe、修复建议SuggestScheme 【本地提权】提权用户 UserName、父进程 ParentProcName 、父进程所属用户 ParentProcGroup、发现时间 CreateTime、危害描述 HarmDescribe、修复建议SuggestScheme 【反弹shell】连接进程 ProcessName、执行命令CmdLine、父进程ParentProcName、目标主机DstIp、目标端口DstPort、发现时间 CreateTime、危害描述 HarmDescribe、修复建议SuggestScheme 示例值： {"Id":20244023294136,"Uuid":"c7ebf82f-a039-406c-96cb-9624b3cd6826","SrcIp":"219.152.236.34","Location":"Province1-City1","UserName":"root","LoginTime":"2024-10-31 18:59:32","Status":2,"Country":1,"City":234,"Province"ayay
CreatedTime	是	否	String	入侵时间 示例值： 2021-03-30 19:17:28
EventType	是	否	Uint64	事件类型：0：文件查杀，1：异常登录， 2：密码破解，3：恶意请求，4：高危命令，5：本地提权， 6：反弹shell 示例值： 1
Id	是	否	Uint64	事件id 示例值： 1
Level	是	否	Uint64	事件统一等级 0：提示，1：低危，2：中危，3：高危，4：严重 示例值： 1
LevelZh	是	否	String	等级名字 示例值： 高危
Uuid	是	否	String	主机uuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0

Item

项

被如下接口引用：DescribeBaselineRuleIgnoreList、DescribeBaselineRuleList、ModifyBaselineRule

名称	必选	允许NULL	类型	描述
CategoryId	否	是	Int64	检测项所属分类 示例值： 50
CustomItemValues	否	是	Array of Uint64	自定义阈值 示例值： [1000]
ItemId	是	否	Int64	Id 示例值： 100
ItemName	否	否	String	名称 示例值： itemname

EmergencyResponseInfo

专家服务-应急响应信息

被如下接口引用：DescribeEmergencyResponseList

名称	必选	允许NULL	类型	描述
EndTime	是	否	String	服务结束时间 示例值： 2021-02-01 17:12:28
HostNum	是	否	Uint64	主机个数 示例值： 12
ReportPath	是	否	String	报告下载地址 示例值： http://any.domanc.com/anypath/1.pdf
StartTime	是	否	String	服务开始时间 示例值： 2021-02-01 17:12:28
Status	是	否	Uint64	服务状态 0未启动，响应中，2响应完成 示例值： 0
TaskId	是	否	String	任务id 示例值： cve2021-4451451

ProtectMachineInfo

授权机器信息

被如下接口引用：DescribeWebPageServiceInfo

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	开通时间 示例值： 2020-11-21 15:16:00
ExpireTime	是	否	String	到期时间 示例值： 2020-11-21 15:16:00
HostIp	是	否	String	机器IP 示例值： 10.0.1.92
HostName	是	否	String	机器名称 示例值： host1

CloudVendorAccountAK

云厂商账号AK信息

被如下接口引用：DescribeCloudVendorAccountAKList

名称	必选	允许NULL	类型	描述
AccessKey	否	是	String	AccessKeyId 示例值： LtDsgdo
CloudType	否	是	Int64	云厂商类型 • 阿里云: 1 示例值： 1
Id	否	是	Uint64	记录ID 示例值： 1
Message	否	是	String	提示信息 示例值： some message
Reason	否	是	String	原因 示例值： any reason
Status	否	是	Int64	AK状态 • 正常: 0 异常: 1 示例值： 0
Uid	否	是	String	所属主账号ID 示例值： 15443424353

RegionListDetail

地域列表详情

被如下接口引用：DescribeMachineRegionList

名称	必选	允许NULL	类型	描述
CloudFrom	否	是	Uint64	0 云 1 IDC机房 2 阿里云 3 华为云 4 亚马逊 5 微软 6 Google 7 Oracle 8 Digital Ocean 示例值： 0

名称	必选	允许NULL	类型	描述
MachineType	否	是	String	机器类型 CVM 云云服务器 LH 云轻量服务器 ECM 云边缘计算服务器 BM 云黑石1.0 服务器 Other 其他服务器(非云) 示例值： CVM
RegionList	否	是	Array of RegionInfo	地域列表 示例值：查看

CKafkaInstanceInfo

CKafka实例信息

被如下接口引用：DescribeLogDeliveryKafkaOptions

名称	必选	允许NULL	类型	描述
Az	是	否	String	地域 示例值： az1
Bandwidth	是	否	Int64	实例带宽，单位Mbps 示例值： 0
DiskSize	是	否	Int64	磁盘容量，单位GB 示例值： 0
Healthy	是	否	Int64	状态，1表示健康，2表示告警，3 表示实例状态异常 示例值： 1
InstanceID	是	否	String	实例ID 示例值： ins-id
InstanceName	是	否	String	实例名称 示例值： instance_name
KafkaVersion	是	否	String	版本号 示例值： 1.1.0
RouteList	是	否	Array of CKafkaRouteInfo	路由列表 示例值：查看
SubnetId	是	否	String	子网id 示例值： 1.1.1.1
TopicList	是	是	Array of CKafkaTopicInfo	主题列表 示例值：查看
VpcId	是	否	String	vpcId，如果为空，说明是基础网络 示例值： 1.1.1.1
Zone	是	否	String	可用区 示例值： zone1

AssetChangeInfo

实例修改信息

被如下接口引用：DescribeChangingAssetInfo

名称	必选	允许NULL	类型	描述
AppId	否	是	Uint64	appid信息 示例值： 1255080011
AssetId	否	是	String	资产ID 示例值： ins-36843684
Status	否	是	Int64	修改状态：0-安装中，1-卸载中，2-开通防护中 示例值： 0

PolicyRules

策略规则表达式

被如下接口引用：CheckBashPolicyParams、DescribeBashPolicies、ModifyBashPolicy

名称	必选	允许NULL	类型	描述
AProcess	否	是	CommandLine	祖先进程 示例值：查看
PProcess	否	是	CommandLine	父进程 示例值：查看
Process	否	是	CommandLine	进程 示例值：查看

PrivilegeRule

本地提权规则

被如下接口引用：DescribePrivilegeRules

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	创建时间 示例值： 2024-11-04 09:57:28
Hostip	是	否	String	主机IP 示例值： 192.168.0.204
Id	是	否	Uint64	规则ID 示例值： 10001
IsGlobal	是	否	Uint64	是否全局规则 示例值： 1
ModifyTime	是	否	String	修改时间 示例值： 2024-11-04 09:57:28
Operator	是	否	String	操作人 示例值： master
ProcessName	是	否	String	进程名 示例值： nginx
SMode	是	否	Uint64	是否S权限进程 1是 0否 示例值： 1

名称	必选	允许NULL	类型	描述
Status	是	否	Uint64	状态(0: 有效 1: 无效) 示例值： 0
Uuid	是	否	String	客户端ID 示例值： df131b24-8528-4809-9d07-a9e4d58ad566

BaselineDetectParam

基线扫描参数

被如下接口引用：StartBaselineDetect

名称	必选	允许NULL	类型	描述
HostIds	否	否	Array of String	检测的主机ID集合 示例值： ['df00265c-081a-4e47-8b92-3e59d902ayay']
ItemIds	否	否	Array of Int64	检测项集合 示例值： [1001,1002]
PolicyIds	否	否	Array of Int64	检测的策略集合 示例值： [101,102,103]
RuleIds	否	否	Array of Int64	检测的规则集合 示例值： [30]

Tag

标签信息

被如下接口引用：DescribeRansomDefenseMachineList、DescribeRansomDefenseStrategyMachines、DescribeTags

名称	必选	允许NULL	类型	描述
Count	是	否	Uint64	服务器数 示例值： 100
Id	是	否	Uint64	标签ID 示例值： 1
Name	是	否	String	标签名 示例值： business1

ComponentStatistics

组件统计数据。

被如下接口引用：DescribeComponentStatistics

名称	必选	允许NULL	类型	描述
ComponentName	是	否	String	组件名称。 示例值： nginx
ComponentType	是	否	String	组件类型。 • WEB：Web组件 • SYSTEM：系统组件 示例值： WEB
Description	是	否	String	组件描述。 示例值： nginx web
Id	是	否	Uint64	组件ID。 示例值： 100010
MachineNum	是	否	Uint64	主机数量。 示例值： 10

BashEvent

高危命令数据

被如下接口引用：DescribeBashEvents

名称	必选	允许NULL	类型	描述
BashCmd	是	否	String	执行命令 示例值： rm
CreateTime	是	否	String	发生时间 示例值： 2021-03-30 19:17:28
DetectBy	是	是	Uint64	0: bash日志 1: 实时监控(雷霆版) 示例值： 1
Exe	是	是	String	进程名称 示例值： 1.exe
HostName	否	是	String	主机名字 示例值： redis_node_cvm
Hostip	是	否	String	主机内网IP 示例值： 127.0.0.1
Id	是	否	Uint64	数据ID 示例值： 1
MachineName	是	否	String	主机名 示例值： redis_node_cvm
ModifyTime	是	是	String	处理时间 示例值： 2021-03-30 19:17:28
Pid	是	是	String	进程id 示例值： 1
Platform	是	否	Uint64	系统类型： 2 windows、4 linux 示例值： 4
Quuid	是	否	String	主机ID 示例值： 380add75-bb06-4cc4-84c5-cf806d102fba
RegexBashCmd	是	是	String	自动生成的正则表达式 示例值： rm -rf /tmp/t*
RuleCategory	是	是	Uint64	规则类别 0=系统规则，1=用户规则 示例值： 0

名称	必选	允许NULL	类型	描述
RuleId	是	否	Uint64	规则ID 示例值： 1
RuleLevel	是	否	Uint64	规则等级：1-高 2-中 3-低 示例值： 1
RuleName	是	否	String	规则名称 示例值： redis_node_use
Status	是	否	Uint64	处理状态： 0 = 待处理 1= 已处理, 2 = 已加白， 3 = 已忽略 示例值： 1
User	是	否	String	执行用户名 示例值： root
Uuid	是	否	String	主机安全ID 示例值： 380add75-bb06-4cc4-84c5-cf806d102fba

WarningObject

告警更新或插入的参数

被如下接口引用：DescribeSaveOrUpdateWarnings、ModifyWarningSetting

名称	必选	允许NULL	类型	描述
BeginTime	否	否	String	开始时间，格式: HH:mm 示例值： 19:17:28
ControlBits	否	否	String	漏洞等级控制位二进制，每一位对应页面漏洞等级的开启关闭：低中高（0:关闭；1：开启），例如：101 → 同时勾选低+高；01一(登录审计)疑似不告警，高危告警 示例值： 101
DisablePhoneWarning	否	否	Uint64	1: 关闭告警 0: 开启告警 示例值： 1
EndTime	否	否	String	结束时间，格式: HH:mm 示例值： 19:17
HostRange	否	是	Int64	告警主机范围类型，0:全部主机，1:按所属项目选，2:按云标签选，3:按主机安全标签选，4:自选主机 示例值： 0
Type	否	否	Uint64	事件告警类型；1：离线，2：木马，3：异常登录，4：爆破，5：漏洞（已拆分为9-12四种类型）6：高位命令，7：反弹sell，8：本地提权，9：系统组件漏洞，10：web应用漏洞，11：应急漏洞，12：安全基线，14：恶意请求，15: 网络攻击，16：Windows系统漏洞，17：Linux软件漏洞 示例值： 2

DeliverTypeDetails

日志投递类型细节

被如下接口引用：DescribeLogClsDeliverInfo、DescribeLogKafkaDeliverInfo、ModifyLogKafkaAccess

名称	必选	允许NULL	类型	描述
ErrInfo	否	否	String	错误信息 示例值： kafka: client has run out of available brokers to talk to: dial tcp 9.151.101.93:6232: i/o timayay
LogName	否	是	String	日志集名 示例值： web_logs
LogSetId	否	是	String	日志集ID 示例值： 269e5897-009a-4c5e-9350-5898964ayayay
LogType	是	否	Array of Int64	安全模块下的日志类型 安全模块"1-入侵检测":1文件查杀、2异常登录、3密码破解、4恶意请求5高危命令、6本地提权、7反弹Shell、8异常进程。\n 安全模块"2-漏洞管理":1应急漏洞、2Linux软件漏洞、3Windows系统漏洞、4Web-CMS漏洞、5应用漏洞、6漏洞防御。\n 安全模块"3基线管理":1安全基线。\n 安全模块"4-高级防御":1Java内存马、2核心文件监控、3攻击检测、4网页防篡改。\n 安全模块"5-客户端相关":1客户端离线、2客户端卸载。\n 安全模块"6-资产指纹":1资源监控、2账号、3端口、4进程、5软件应用、6数据库、7Web应用、8Web服务、9Web框架、10Web站点、11Jar包、12启动服务、13计划任务、14环境变量、15内核模块。\n安全模块"7-主机列表":1主机列表。\n 安全模块"8-客户端日志":1客户端日志、2dns日志、3进程快照、4网络五元组、5文件写入、6登录流水。 示例值： [1,2]
Region	否	是	String	日志集所在地域 示例值： ap-region1
SecurityType	是	否	Uint64	安全模块类型 1: 入侵检测 2: 漏洞管理 3: 基线管理 4: 高级防御 5:客户端相关 6: 资产指纹 7 主机列表 8 客户端上报 示例值： 1
Status	否	否	Uint64	投递状态，0未开启 1正常 2异常 示例值： 1
StatusTime	否	否	Int64	最近一次状态上报时间戳 示例值： 1
Switch	是	否	Uint64	投递开关 0关闭 1开启 示例值： 1
TopicId	是	否	String	主题ID 示例值： topic-70s2ayay
TopicName	是	否	String	主题名 示例值： log-recive

MaCustomPolicy

被如下接口引用：DescribeMaCustomPolicyList、ModifyMaCustomPolicy

名称	必选	允许NULL	类型	描述
ActionType	否	是	Uint64	策略动作，当前只有0 • 0 放行 • 1 告警 示例值： 0
ConEventId	否	是	Array of Uint64	加白时候历史事件ID 示例值： [201]
CreateTime	否	是	String	创建时间 示例值： 2023-10-10 00:00:00
DestHostWorkloadNum	否	是	Uint64	目标主机负载个数 示例值： 1
DestIPs	否	是	Array of String	目标IP配置 示例值： ["192.168.0.204"]
DestLabels	否	是	Array of MaLabel	目标标签配置 示例值：查看
DestPodWorkloadNum	否	是	Uint64	目标POD负载个数 示例值： 1
DestPorts	否	是	Array of String	目标端口，不填写则默认all，不填写表示全部 示例值： ["80"]

名称	必选	允许NULL	类型	描述
DestType	是	是	Uint64	目标配置类型 • 0 标签 • 1 IP • 2 工作负载 • 3 全部 示例值： 1
DestWorkloads	否	是	Array of MaCustomPolicyWorkload	目标工作负载配置 示例值：查看
Enable	是	是	Uint64	自定白名单状态 • 0 关闭 • 1 开启 示例值： 1
HandleHistory	否	是	Int64	是否处理历史事件 • 0 不处理 • 1 处理 示例值： 0
Id	否	是	Uint64	自定义白名单策略ID 示例值： 1
ModifyTime	否	是	String	更新时间 示例值： 2023-10-10 00:00:00
Name	是	是	String	自定义白名单策略名字 示例值： policy1
SrcHostWorkloadNum	否	是	Uint64	源主机负载个数 示例值： 1
SrcIPs	否	是	Array of String	源IP配置 示例值： ["192.168.0.1"]
SrcLabels	否	是	Array of MaLabel	源标签配置 示例值：查看
SrcPodWorkloadNum	否	是	Uint64	源POD负载个数 示例值： 1
SrcType	是	是	Uint64	源配置类型 • 0 标签 • 1 IP • 2 工作负载 • 3 全部 示例值： 1
SrcWorkloads	否	是	Array of MaCustomPolicyWorkload	源工作负载配置 示例值：查看
Updater	是	是	String	创建人/更新人 示例值： user1

BaselineRuleInfo

基线检测信息

被如下接口引用：DescribeBaselineRule

名称	必选	允许NULL	类型	描述
Description	是	否	String	检测项描述 示例值： 配置审核日志文件的最大大小。一旦日志达到最大大小，将对其进行轮换并启动新的日志文件。
EventId	是	否	Uint64	唯一事件ID 示例值： 3634
FixMessage	是	否	String	修复建议 示例值： 根据站点策略设置/etc/audit/auditd.conf参数：
LastScanAt	是	否	String	最后检测时间 示例值： 2024-11-04 09:57:28
Level	是	否	Uint64	基线风险等级：0低危 1中危 2高危 3严重 示例值： 3
RuleId	是	否	Uint64	检测项id 示例值： 1026
RuleName	是	否	String	检测项名称 示例值： 确保已配置审核日志存储大小低危
RuleRemark	是	否	String	具体原因说明 示例值： 日志remark
Status	是	否	Uint64	状态 示例值： 0
Uuid	是	否	String	唯一Uuid 示例值： df131b24-8528-4809-9d07-a9e4d58ad566

EventStat

未处理的安全事件统计信息

被如下接口引用：DescribeSecurityEventStat

名称	必选	允许NULL	类型	描述
EventsNum	是	否	Uint64	事件数 示例值： 0
MachineAffectNum	是	否	Uint64	受影响的主机数 示例值： 0

MaConnEvent

被如下接口引用：DescribeMaConnEventList

名称	必选	允许NULL	类型	描述
CreateTime	否	是	String	首次时间 示例值： 2023-10-10 00:00:00
DestIP	否	是	String	目标IP 示例值： 1.1.1.1

名称	必选	允许NULL	类型	描述
DestInstanceId	否	是	String	目标实例ID 示例值： ins-tsa23
DestLabels	否	是	Array of MaLabel	目标工作负载的标签，长度可能为0，长度为0表示未匹配中标签 示例值：查看
DestPodInfo	否	是	MaConnPodInfo	目标为POD的情况下，POD的基础信息 示例值：查看
DestPort	否	是	Uint64	目标端口 示例值： 8080
DestUuid	否	是	String	目标为主机的情况下主机UUID 示例值： 5a540076-d38a-4078-aa98-q45rt371d322
DestWorkloadDeleted	否	是	Uint64	目标工作负载是否删除 • 0 未删除 • 1 删除 示例值： 1
DestWorkloadId	否	是	Uint64	目标工作负载ID，可能为0，为0表示未匹配中工作负载 示例值： 1
DestWorkloadName	否	是	String	目标工作负载名字，可能为空串，为空传表示未匹配中工作负载 示例值： redis_node_cvm
DestWorkloadType	否	是	Int64	目标工作负载类型 • 0 ip • 1 主机 • 2 pod 示例值： 1
Id	否	是	Uint64	事件ID 示例值： 1
MatchCount	否	是	Uint64	匹配中的次数 示例值： 100
MatchPolicyId	否	是	Uint64	自定义策略的情况下匹配中的策略ID 示例值： 1
MatchPolicyName	否	是	String	匹配中策略的名字 示例值： policy1
MatchPolicyType	否	是	Uint64	匹配中策略类型 • 0 自学习策略 • 1 自自定义白名单策略 示例值： 1
MatchPolicyUniqueId	否	是	String	自学习策略的情况下匹配中的自学习策略唯一Key 示例值： 2514
ModifyTime	否	是	String	最近发生时间 示例值： 2023-10-10 00:00:00
PolicyDeleted	否	是	Uint64	匹配中的策略是否删除 • 0 未删除 • 1 删除 示例值： 1
Protocol	否	是	String	协议 • TCP • UDP 示例值： TCP
ServiceName	否	是	String	服务名，扩展用，当前不支持 示例值： sshd
SrcIP	否	是	String	源IP 示例值： 1.1.1.1
SrcInstanceId	否	是	String	源实例ID 示例值： instance1
SrcLabels	否	是	Array of MaLabel	源工作负载的标签，长度可能为0，长度为0表示未匹配中标签 示例值：查看
SrcPodInfo	否	是	MaConnPodInfo	源为POD的情况下，POD的基础信息 示例值：查看
SrcUuid	否	是	String	源为主机的情况下主机UUID 示例值： 5a540076-d38a-4078-aa98-q45rt371d322
SrcWorkloadDeleted	否	是	Uint64	源工作负载是否删除 • 0 未删除 • 1 删除 示例值： 1
SrcWorkloadId	否	是	Uint64	源工作负载ID，可能为0，为0表示未匹配中工作负载 示例值： 1
SrcWorkloadName	否	是	String	源工作负载名字，可能为空串，为空传表示未匹配中工作负载 示例值： 192.168.0.10
SrcWorkloadType	否	是	Int64	源工作负载类型 • 0 ip • 1 主机 • 2 pod 示例值： 0
Type	否	是	Uint64	事件类型 • 0 正常访问 • 1 异常访问 示例值： 0

AssetJarDetail

资产管理jar包详情

被如下接口引用：DescribeAssetJarInfo

名称	必选	允许NULL	类型	描述
MachineIp	是	否	String	服务器IP 示例值： 10.0.0.11

名称	必选	允许NULL	类型	描述
MachineName	是	否	String	服务器名称 示例值： redis_node_cvm
Md5	是	是	String	Jar包Md5 示例值： fc702c8398071ea3697d449c2b894dae
Name	是	否	String	名称 示例值： com.apple.utils
OsInfo	是	否	String	操作系统 示例值： 1
Path	是	否	String	路径 示例值： /root
Process	是	是	Array of AssetAppProcessInfo	引用进程列表 示例值：查看
Status	是	否	Uint64	是否可执行：0未知，1是，2否 示例值： 1
Type	是	否	Int64	类型：1应用程序，2系统类库，3Web服务自带库，8:其他， 示例值： 1
UpdateTime	是	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
Version	是	否	String	版本 示例值： 1.0.0

AssetPlanTask

资产管理计划任务列表

被如下接口引用：DescribeAssetPlanTaskList

名称	必选	允许NULL	类型	描述
Command	否	否	String	执行命令或脚本 示例值： /root/sshd
ConfigPath	否	否	String	配置文件路径 示例值： /etc/sshd
Cycle	否	否	String	执行周期 示例值： 10　*
FirstTime	否	否	String	首次采集时间 示例值： 2022-07-15 11:27:01
IsNew	否	否	Int64	是否新增[0:否
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	否	String	服务器IP 示例值： 10.0.0.11
MachineName	否	否	String	服务器名称 示例值： redis_node_cvm
MachineWanIp	否	否	String	服务器外网IP 示例值： 1.1.1.1
OsInfo	否	否	String	操作系统 示例值： centos 64bit
Quuid	否	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Status	否	否	Uint64	默认启用状态：1启用，2未启用 示例值： 1
UpdateTime	否	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
User	否	否	String	启动用户 示例值： root
Uuid	否	否	String	主机uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

AttackSource

攻击溯源

被如下接口引用：DescribeAttackSource

名称	必选	允许NULL	类型	描述
Edges	是	是	Array of AttackSourceEdge	攻击溯源节点路径 示例值：查看
EventInfoParam	是	是	String	请求节点相关事件详情的参数 示例值： params
Nodes	是	是	Array of AttackSourceNode	攻击溯源节点描述 示例值：查看

VulDefenceEventDetail

漏洞详细信息

被如下接口引用：DescribeDefenceEventDetail

名称	必选	允许NULL	类型	描述
Alias	否	否	String	主机名 示例值： redis_node_cvm
City	否	否	String	攻击源ip地址所在城市 示例值： city1
Count	否	否	Int64	事件发生次数 示例值： 1
CreateTime	否	否	String	创建事件时间 示例值： 2021-01-20 16:17:11
CveId	否	否	String	cve编号 示例值： cve-ay

名称	必选	允许NULL	类型	描述
Description	否	否	String	漏洞描述信息 示例值： 描述信息
EventDetail	否	否	String	漏洞ID相关的事件详情(json array格式 rasp特有) 示例值： [{ "name": "jndiurl", "value": "http://whoa
EventType	否	否	Uint64	0: 尝试攻击(WeDetect) 1:尝试攻击成功(WeDetect) 2:rasp防御事件 示例值： 1
ExceptionPstree	否	否	String	主机失陷事件进程树(json格式 WeDetect特有) 示例值： ppid ssh
Fix	否	否	String	修复建议 示例值： 修复建议
Id	否	否	Int64	漏洞事件id 示例值： 1
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
MachineStatus	否	否	String	ONLINE OFFLINE 示例值： ONLINE
MainClass	否	否	String	关联进程主类名 示例值： sf.class
MergeTime	否	否	String	更新事件时间 示例值： 2021-01-20 16:17:11
NetworkPayload	否	否	String	攻击payload 示例值： GET /$%7BClass.forName(%22com.opensymphony.webwork.ServletActionContext%22).getMethod
Pid	否	否	Int64	关联进程pid 示例值： 116
PrivateIp	否	否	String	内网ip 示例值： 10.2.3.1
PublicIp	否	否	String	公网ip 示例值： 111.2.3.1
Quuid	否	否	String	主机quuid 示例值： d92d723e-4aac-4f4a-bbf9-e5430e29d289
SourceIp	否	否	String	攻击源ip 示例值： 11.2.3.1
SourcePort	否	是	Array of Uint64	攻击源端口 示例值： [1,3]
StackTrace	否	否	String	堆栈信息(rasp特有) 示例值： at org.java.util
Status	否	否	Int64	状态 0: 待处理 1:已防御 2:已处理 3: 已忽略 4: 已删除 示例值： 1
VulName	否	否	String	漏洞名称 示例值： 漏洞

ReverseShellRule

反弹Shell规则

被如下接口引用：DescribeReverseShellRules

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	创建时间 示例值： 2024-11-04 09:57:28
DestIp	是	否	String	目标IP 示例值： 127.0.0.1
DestPort	是	否	String	目标端口 示例值： 80
Hostip	是	否	String	主机IP 示例值： 192.168.0.204
Id	是	否	Uint64	规则ID 示例值： 1001
IsGlobal	是	否	Uint64	是否全局规则 示例值： 1
ModifyTime	是	否	String	修改时间 示例值： 2024-11-04 09:57:28
Operator	是	否	String	操作人 示例值： root
ProcessName	是	否	String	进程名称 示例值： nginx
Status	是	否	Uint64	状态 (0: 有效 1: 无效) 示例值： 0
Uuid	是	否	String	客户端ID 示例值： df131b24-8528-4809-9d07-a9e4d58ad566

MaSelfLearnPolicy

被如下接口引用：DescribeMaSelfLearnPolicyList

名称	必选	允许NULL	类型	描述
CreateTime	否	是	String	创建时间 示例值： 2023-10-10 00:00:00
DestIP	否	是	String	策略的IP，DestLabels为空时这里会赋值 示例值： 2.2.2.2
DestLabels	否	是	Array of MaLabel	目标标签 示例值：查看
DestPort	否	是	Uint64	目标端口 示例值： 8080
Id	否	是	Uint64	自学习策略ID 示例值： 1
MatchCount	否	是	Uint64	命中的包数 示例值： 1

名称	必选	允许NULL	类型	描述
ModifyTime	否	是	String	更新时间 示例值： 2023-10-10 00:00:00
SrcIP	否	是	String	策略的IP，SrcLabels为空时这里会赋值 示例值： 1.1.1.1
SrcLabels	否	是	Array of MaLabel	源标签 示例值：查看
UniqueId	否	是	String	自学习策略的唯一ID 示例值： uniqdgs

ProtectMachine

机器授权到期信息

被如下接口引用：DescribeWebPageServiceInfo

名称	必选	允许NULL	类型	描述
HostIp	是	否	String	机器IP 示例值： 10.0.1.92
HostName	是	否	String	机器名称 示例值： host1
SafeguardDirNum	是	否	Uint64	防护目录数 示例值： 0

AssetDatabaseBaseInfo

资源管理数据库列表信息

被如下接口引用：DescribeAssetDatabaseList

名称	必选	允许NULL	类型	描述
BinPath	否	否	String	二进制路径 示例值： /usr/local/bin
ConfigPath	否	否	String	配置文件路径 示例值： /etc/sshd
DataPath	否	否	String	数据路径 示例值： /data
ErrorLogPath	否	否	String	错误日志路径 示例值： /var/log
FirstTime	否	否	String	首次采集时间 示例值： 2022-07-15 11:27:01
Id	否	否	String	数据库ID 示例值： 1
Ip	否	否	String	绑定IP 示例值： 112.52.67.8
IsNew	否	否	Int64	是否新增[0:否
LogPath	否	否	String	日志文件路径 示例值： /var/log
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	否	String	主机内网IP 示例值： 10.0.0.11
MachineName	否	否	String	主机名称 示例值： redis_node_cvm
MachineWanIp	否	否	String	主机外网IP 示例值： 112.41.55.12
Name	否	否	String	数据库名 示例值： yunding
OsInfo	否	否	String	操作系统信息 示例值： Centos 64Bit
Param	否	否	String	启动参数 示例值： --configsvr --port 27019 --keyFile /etc/mongodb/key --dbpath /data/db --replSet d1j49h6z --wiredTigerCacheSizeGB 0.43 --maxConns 10000 --auth --bind_ip_all
Permission	否	否	String	运行权限 示例值： polkitd
PlugInPath	否	否	String	插件路径 示例值： /data
Port	否	否	String	监听端口 示例值： 27019
ProjectId	否	否	Uint64	主机业务组ID 示例值： 1
Proto	否	否	String	协议 示例值： tcp
Quuid	否	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Tag	否	是	Array of MachineTag	主机标签 示例值：查看
UpdateTime	否	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
User	否	否	String	运行用户 示例值： root
Uuid	否	否	String	主机Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Version	否	否	String	版本 示例值： 1.1.1

MachineExtraInfo

服务器基础信息

被如下接口引用：DescribeAssetAppList、DescribeAssetCoreModuleList、DescribeAssetDatabaseList、DescribeAssetEnvList、DescribeAssetInitServiceList、DescribeAssetJarList、DescribeAssetMachineDetail、DescribeAssetMachineList、DescribeAssetPlanTaskList、DescribeAssetPortInfoList、DescribeAssetProcessInfoList、DescribeAssetSystemPackageList、DescribeAssetUserList、DescribeAssetWebAppList、DescribeAssetWebFrameList、DescribeAssetWebLocationList、DescribeAssetWebServiceInfoList、DescribeAttackEventInfo、

DescribeAttackEvents、DescribeAttackLogs、DescribeBaselineFixList、DescribeBaselineHostDetectList、DescribeBaselineHostIgnoreList、DescribeBaselineItemList、DescribeBashEventsNew、DescribeBruteAttackList、DescribeDefenceEventDetail、DescribeFileTamperEvents、DescribeHostLoginList、DescribeIgnoreHostAndItemConfig、DescribeJavaMemShellInfo、DescribeJavaMemShellList、DescribeJavaMemShellPluginList、DescribeLicenseBindList、DescribeLicenseBindSchedule、DescribeMachineList、DescribeMachines、DescribeMalWareList、DescribeMalwareInfo、DescribePrivilegeEvents、DescribeProtectDirRelatedServer、DescribeReverseShellEvents、DescribeRiskDnsEventInfo、DescribeRiskDnsEventList、DescribeRiskProcessEvents、DescribeScanTaskDetails、DescribeScreenMachines、DescribeVulDefenceEvent、DescribeVulEffectHostList、DescribeWebPageEventList

名称	必选	允许NULL	类型	描述
HostName	否	是	String	主机名 示例值： redis_node_cvm
InstanceID	否	是	String	实例ID 示例值： ins-1s7mkggc
NetworkName	否	是	String	网络名，vpc网络情况下会返回vpc_id 示例值： vpc-9m7rhl6w
NetworkType	否	是	Int64	网络类型，1:vpc网络 2:基础网络 3:非云网络 示例值： 1
PrivateIP	否	是	String	内网IP 示例值： 1.1.1.1
WanIP	否	是	String	公网IP 示例值： 1.1.1.1

MaGlobalConf

被如下接口引用：DescribeMaGlobalConf、ModifyMaGlobalConf

名称	必选	允许NULL	类型	描述
MonitorEnabled	是	是	Int64	监控开关 1开 0关 示例值： 1
MonitorIpRanges	否	是	Array of String	监控IP范围 示例值： ["192.168.0.1"]
MonitorLabelIds	否	是	Array of Int64	监控标签 示例值： [1]
MonitorScope	是	是	Int64	监控范围[0:全部
MonitorWorkloadIds	否	是	Array of Int64	排除负载ID列表 示例值： [1]
NewEnabled	否	是	Int64	新资产是否自动防护[1:是
NewEndTime	否	是	Datetime_iso	自学习结束时间 示例值： 2020-02-01 12:00:00
NewIpRanges	否	是	Array of String	新增资产防护IP段 示例值： ["192.168.0.1"]
NewLabelIds	否	是	Array of Int64	新增资产防护IP段 示例值： [1]
NewLearnCycle	否	是	Int64	新增资产自学习天数 示例值： 3
NewScope	否	是	Int64	新增防护范围[0:全部
NewStartTime	否	是	Datetime_iso	自学习开始时间 示例值： 2020-02-01 12:00:00

BaselineFix

基线密码修复

被如下接口引用：DescribeBaselineFixList

名称	必选	允许NULL	类型	描述
CreateTime	否	否	String	首次检测时间 示例值： 2021-02-01 12:00:00
FixTime	否	否	String	修复时间 示例值： 2021-02-01 12:00:00
HostIp	否	否	String	主机Ip 示例值： 192.168.0.204
Id	否	否	Int64	基线检测项结果ID 示例值： 1
ItemName	否	否	String	修复项名称 示例值： 确保 SSH 空闲超时时间间ayay
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
ModifyTime	否	否	String	最后检测时间 示例值： 2021-02-01 12:00:00

AgentInstallTaskResult

安全中心安装agent任务详情

被如下接口引用：DescribeAgentInstallTaskResult

名称	必选	允许NULL	类型	描述
Assets	否	是	Array of AgentInstallResult	全部实例 示例值：查看
CreateTime	否	是	String	任务启动时间 示例值： 2020-02-01 12:00:00
Id	否	是	Int64	任务ID 示例值： 1

BaselineHost

基线主机信息

被如下接口引用：DescribeBaselineHostIgnoreList、DescribeIgnoreHostAndItemConfig

名称	必选	允许NULL	类型	描述
HostId	否	否	String	主机Id 示例值： 11cb73df-ea71-4678-8114-5af94e63ayay

名称	必选	允许NULL	类型	描述
HostIp	否	是	String	内网Ip 示例值： 192.168.0.204
HostName	否	是	String	主机名称 示例值： redis_node_cvm
HostTag	否	是	String	主机标签 示例值： ["tag-01"]
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
WanIp	否	是	String	外网Ip 示例值： 192.168.0.204

Machine

主机列表

被如下接口引用：DescribeMachineList、DescribeMachines

名称	必选	允许NULL	类型	描述
BaselineNum	否	否	Int64	基线风险数。 示例值： 2
CloudFrom	否	是	Int64	云服务器厂商类型 0 云 1 IDC机房 2 阿里云 3 华为云 4 亚马逊 5 微软 6 Google 7 Oracle 8 Digital Ocean 示例值： 0
CloudTags	否	是	Array of Tags	云标签信息 示例值：查看
CyberAttackNum	否	否	Int64	网络风险数。 示例值： 2
HasAssetScan	否	否	Uint64	是否有资产扫描接口，0无，1有 示例值： 1
InstanceId	否	否	String	实例ID 示例值： ins-sad143
InstanceState	否	否	String	实例状态： PENDING表示创建中、LAUNCH_FAILED表示创建失败、RUNNING表示运行中、STOPPED表示关机、STARTING表示开机中、STOPPING表示关机中、REBOOTING表示重启中、SHUTDOWN表示停止待销毁、TERMINATING表示销毁中、TERMINATED已销毁中、TERMINATED_PRO_VERSION已销毁云镜专业版未到期 示例值： TERMINATED_PRO_VERSION
InvasionNum	否	否	Int64	入侵事件数 示例值： 1
IpList	否	是	String	主机ip列表 示例值： 1.1.1.1,2.2.2.2
IsAddedOnTheFifteen	否	是	Uint64	是否15天内新增的主机 0：非15天内新增的主机，1：15天内增加的主机 示例值： 1
IsProVersion	否	否	Bool	是否是专业版。 • true：是 • false：否 示例值： false
KernelVersion	否	否	String	内核版本 示例值： 3.10.0-1127.19.1.el7.x86_64
LicenseStatus	否	否	Uint64	防篡改 授权状态 1 授权 0 未授权 示例值： 1
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	否	String	主机IP。 示例值： 10.0.0.2
MachineName	否	否	String	主机名称。 示例值： stone
MachineOs	否	否	String	主机系统。 示例值： centos
MachineStatus	否	否	String	主机状态。 • OFFLINE: 离线 • ONLINE: 在线 • SHUTDOWN: 已关机 • UNINSTALLED: 未防护 示例值： ONLINE
MachineType	否	否	String	机器所属专区类型 CVM 云服务器, BM 黑石, ECM 边缘计算, LH 轻量应用服务器 ,Other 混合云专区 示例值： CVM
MachineWanIp	否	否	String	主机外网IP。 示例值： 114.11.12.13
MalwareNum	否	否	Int64	木马数。 示例值： 1
PayMode	否	否	String	主机状态。 • POSTPAY: 表示后付费，即按量计费 • PREPAY: 表示预付费，即包年包月 示例值： PREPAY
Platform	否	是	String	Platform 示例值： platform
ProjectId	否	否	Int64	项目ID 示例值： 1
ProtectType	否	否	String	防护版本：BASIC_VERSION 基础版， PRO_VERSION 专业版，Flagship 旗舰版，GENERAL_DISCOUNT 普惠版 示例值： BASIC_VERSION
Quuid	否	否	String	CVM或BM机器唯一Uuid。 示例值： 8c09e1b1-5611-45b3-9c02-737996011b81
RegionInfo	否	否	RegionInfo	地域信息 示例值：查看
Remark	是	是	String	备注信息 示例值： redis cvm

名称	必选	允许NULL	类型	描述
SecurityStatus	否	否	String	风险状态。 • SAFE：安全 • RISK：风险 • UNKNOWN：未知 示例值： RISK
Tag	否	否	Array of MachineTag	标签信息 示例值：查看
Uuid	否	否	String	主机安全Uuid，若客户端长时间不在线将返回空字符。 示例值： 8c09e1b1-5611-45b3-9c02-737996011b81
VpcId	否	是	String	所属网络 示例值： vpc-sda
VulNum	否	否	Int64	漏洞数。 示例值： 2

MalwareWhiteListInfo

木马白名单信息

被如下接口引用：DescribeMalwareWhiteList

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	规则创建时间 示例值： 2024-10-30 09:12:21
EventsCount	是	否	Uint64	受影响记录 示例值： 1
FileDirectory	是	否	String	文件目录；按,分割 示例值： /tmp
FileExtension	是	否	String	文件后缀；按,分割 示例值： php
FileName	是	否	String	文件名；按,分割 示例值： run.sh
Id	是	否	Uint64	唯一ID。 示例值： 1
IsGlobal	是	否	Uint64	是否全部主机； 0否，1是 示例值： 1
MatchType	是	否	Uint64	匹配模式；0精确匹配，1模糊匹配 示例值： 1
Md5List	是	否	String	md5列表 按,分割 示例值： 708cae4cf814c3deda4208da228fad4e
Mode	是	否	Uint64	白名单模式；0 MD5 ，1自定义 示例值： 1
ModifyTime	否	否	String	规则修改时间 示例值： 2024-10-30 09:12:21
QuuidList	是	否	String	cvm quuid 按,分割。 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0

AssetNetworkCardInfo

资产管理网卡信息

被如下接口引用：DescribeAssetMachineDetail、DescribeAssetMachineInfo

名称	必选	允许NULL	类型	描述
DnsServer	是	否	String	DNS服务器 示例值： 8.8.8.8
GateWay	是	否	String	网关 示例值： 10.0.0.1
Ip	是	否	String	Ipv4对应IP 示例值： 172.17.0.1
Ipv6	是	否	String	Ipv6对应IP 示例值： fe80::42:4dff:fe1b:ed6c
Mac	是	否	String	MAC地址 示例值： 16:75:bf:b8:73:9c
Name	是	否	String	网卡名称 示例值： eth1

VulDefenceRangeDetail

漏洞防御范围详情

被如下接口引用：DescribeVulDefenceList

名称	必选	允许NULL	类型	描述
CveId	是	否	String	cve id 示例值： CVE-2020-9496
CvssScore	是	否	Float	cvss 分数 示例值： 6.1
Label	是	否	String	标签 示例值： 远程利用
Level	是	否	Uint64	漏洞级别： 1低危 2中危 3高危 4严重 示例值： 2
PublishTime	是	否	String	发布时间 示例值： 2020-07-16 00:15:00
VulId	是	否	Int64	漏洞id 示例值： 105068
VulName	是	否	String	漏洞名称 示例值： Apache HTTP/2 协议拒绝服务漏洞(CVE-2023-44487)

LogStorageRecord

日志存储量记录

被如下接口引用：DescribeLogStorageRecord

名称	必选	允许NULL	类型	描述
InquireSize	否	是	Uint64	总量，字节 示例值： 0
Month	否	是	String	年月份 示例值： 202304
UsedSize	否	是	Uint64	存储量，字节 示例值： 0

MalwareRisk

恶意文件风险提示列表信息

被如下接口引用：DescribeMalwareRiskWarning

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	发现时间 示例值： 2022-01-01 00:00:00
Id	是	否	Uint64	唯一ID 示例值： 10001
MachineIp	是	否	String	机器IP 示例值： 1.1.1.1
VirusName	是	否	String	病毒名 示例值： Linux.Trojan.Downloader.Snkl

AssetInfo

实例信息

被如下接口引用：CreateAgentInstallTask、DescribeAgentInstallResult、ModifyAssetsProtectionStatus

名称	必选	允许NULL	类型	描述
AppId	否	是	Uint64	appid信息 示例值： 3680000000
AssetId	否	是	String	资产ID 示例值： ins-36843684
AssetType	否	是	String	资产类型 示例值： CVM
MemberId	否	是	String	memberid 示例值： mem-36843684
Region	否	是	String	可用区 示例值： ap-region1

HostLoginList

登录审计列表实体

被如下接口引用：DescribeHostLoginList

名称	必选	允许NULL	类型	描述
City	否	是	Uint64	城市id 示例值： 23
Country	否	是	Uint64	国家id 示例值： 1
Desc	否	是	String	高危信息说明： ABROAD - 海外IP； XTI - 威胁情报 示例值： ABROAD
Id	否	否	Uint64	记录Id 示例值： 10001
IsRiskArea	否	是	Uint64	是否命中异地登录异常 1表示命中此类异常, 0表示未命中 示例值： 1
IsRiskSrcIp	否	是	Uint64	是否命中异常IP异常 1表示命中此类异常, 0表示未命中 示例值： 1
IsRiskTime	否	是	Uint64	是否命中异常时间异常 1表示命中此类异常, 0表示未命中 示例值： 1
IsRiskUser	否	是	Uint64	是否命中异常用户异常 1表示命中此类异常, 0表示未命中 示例值： 1
Location	否	是	String	位置名称 示例值： location1:location2:location3
LoginTime	否	是	String	登录时间 示例值： 2024-10-30 15:58:43
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	是	String	主机ip 示例值： 192.168.0.204
MachineName	否	是	String	主机名 示例值： redis_node_cvm
ModifyTime	否	是	String	修改时间 示例值： 2024-10-30 15:58:43
Port	否	是	Int64	请求目的端口 示例值： 3306
Province	否	是	Uint64	省份id 示例值： 101
Quuid	否	是	String	主机quuid 示例值： 935e27b1-d675-4509-80bf-96fbf0764237
RiskLevel	否	是	Uint64	危险等级： 0 高危 1 可疑 示例值： 1

名称	必选	允许NULL	类型	描述
SrcIp	否	是	String	来源ip 示例值： 192.168.0.204
Status	否	否	Uint64	1:正常登录；2异地登录； 5已加白； 14：已处理；15：已忽略。 示例值： 1
UserName	否	是	String	用户名 示例值： root
Uuid	否	是	String	主机Uuid 示例值： 380add75-bb06-4cc4-84c5-cf806d102fba

BaselineInfo

基线信息

被如下接口引用：DescribeBaselineList

名称	必选	允许NULL	类型	描述
BaselineFailCount	是	是	Uint64	基线风险项 示例值： 0
CategoryId	是	是	Uint64	基线id 示例值： 1
HostCount	是	是	Uint64	影响服务器数量 示例值： 0
LastScanTime	是	是	String	最后检测时间 示例值： 2020-11-21 15:16:00
Level	是	是	Uint64	危害等级：1-低危；2-中危；3-高危；4-严重 示例值： 1
MaxStatus	是	是	Uint64	检测中状态: 5 示例值： 5
Name	是	是	String	基线名 示例值： Redis 基线合规检测
RuleCount	是	是	Uint64	检测项数量 示例值： 0
Status	是	是	Uint64	通过状态:0:未通过,1:已通过 示例值： 1

AssetWebLocationPath

资产管理Web站点虚拟目录

被如下接口引用：DescribeAssetWebLocationPathList

名称	必选	允许NULL	类型	描述
Group	是	否	String	文件所属组 示例值： root
Permission	是	否	String	文件权限 示例值： rwxay
RealPath	是	否	String	物理路径 示例值： /var/www/html
User	是	否	String	文件所有者 示例值： root
VirtualPath	是	否	String	虚拟路径 示例值： /var/www/html

ProtectHostConfig

防护机器信息

被如下接口引用：CreateProtectServer、ModifyWebPageProtectDir

名称	必选	允许NULL	类型	描述
AutoRecovery	是	否	Uint64	自动恢复开关 0 关闭 1开启 示例值： 0
ProtectSwitch	是	否	Uint64	防护开关 0 关闭 1开启 示例值： 0
Quuid	是	否	String	机器唯一ID 示例值： 15c76928-e4e1-4f0d-8a2a-46c7de78ayay

RiskProcessEvent

异常进程事件

被如下接口引用：DescribeRiskProcessEvents

名称	必选	允许NULL	类型	描述
CheckPlatform	否	否	Array of String	木马检测平台 [1:云查杀引擎
CmdLine	否	否	String	执行命令 示例值： /usr/sbin/sshd
DetectTime	否	否	String	最近检测时间 示例值： 2022-09-23 15:11:46
EventId	否	否	Int64	事件ID 示例值： 1
FilePath	否	否	String	文件路径 示例值： /var/www/fscan
HandleStatus	否	否	Int64	处理状态[0待处理;1已处理;2查杀中;3已查杀;4已退出;5忽略] 示例值： 1
HostIp	否	否	String	主机IP 示例值： 10.0.0.1
HostName	否	否	String	主机名称 示例值： redis_node_cvm
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看

名称	必选	允许NULL	类型	描述
OnlineStatus	否	否	Int64	主机在线状态 示例值： 1
ProcessId	否	否	Int64	进程ID 示例值： 1
ReferenceLink	否	否	String	参考链接 示例值： https://cloud.domain.com/document/product/296/9604
StartTime	否	否	String	进程启动时间 示例值： 2022-09-23 15:11:46
SuggestSolution	否	否	String	建议方案 示例值： 1.检查恶意进程及非法端口，删除可疑的启动项和定时任务； 2.隔离或者删除相关的木马文件；
ThreatDesc	否	否	String	威胁描述 示例值： 发现主机上存在代理工具进程，若不是您的主动行为，您的主机可能已经失陷。
Uuid	否	否	String	主机uuid 示例值： e05a66ec-8d54-4041-80a8-07e9ab79ayay
VirusName	否	否	String	病毒名称 示例值： Linux.Risk.Miner
VirusTags	否	否	Array of String	病毒标签 示例值： ["Miner","HackTool"]
WanIp	否	否	String	外网IP 示例值： 10.0.0.1

VulDefenceEvent

漏洞详细信息

被如下接口引用：DescribeVulDefenceEvent

名称	必选	允许NULL	类型	描述
Alias	否	否	String	主机名 示例值： redis_node_cvm
City	否	否	String	攻击源ip地址所在城市 示例值： city1
Count	否	否	Int64	事件发生次数 示例值： 1
CreateTime	否	否	String	创建事件时间 示例值： 2021-01-20 16:17:11
CveId	否	否	String	cve编号 示例值： CVE-2014-8500
EventType	否	否	Uint64	0: 尝试攻击(WeDetect) 1:尝试攻击成功(WeDetect) 2:rasp防御事件 示例值： 1
FixType	否	否	Int64	0 不支持修复，1 支持修复 示例值： 1
Id	否	否	Int64	漏洞事件id 示例值： 13844
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
MergeTime	否	否	String	更新事件时间 示例值： 2021-01-20 16:17:11
PrivateIp	否	否	String	内网ip 示例值： 10.2.3.1
PublicIp	否	否	String	公网ip 示例值： 111.2.3.1
Quuid	否	否	String	主机quuid 示例值： d92d723e-4aac-4f4a-bbf9-e5430e29d289
SourceIp	否	否	String	攻击源ip 示例值： 11.2.3.1
SourcePort	否	否	Array of Uint64	攻击源端口 示例值： [50001,50002]
Status	否	否	Int64	状态 0: 待处理 1:已防御 2:已处理 3: 已忽略 4: 已删除 示例值： 1
UpgradeType	否	否	Int64	0 专业版,1 旗舰版,2 LH普惠版（仅限LH使用）,3 CVM普惠版（仅限CVM使用） 示例值： 1
Uuid	否	否	String	主机uuid 示例值： d92d723e-4aac-4f4a-bbf9-e5430e29d289
VulId	否	否	Uint64	漏洞ID 示例值： 14004
VulName	否	否	String	漏洞名称 示例值： 漏洞

BaselineEffectHost

基线影响主机信息

被如下接口引用：DescribeBaselineEffectHostList

名称	必选	允许NULL	类型	描述
AliasName	是	是	String	主机别名 示例值： redis_node_cvm
FailCount	是	是	Uint64	风险项 示例值： 1
FirstScanTime	是	是	String	首次检测事件 示例值： 2021-10-27 00:09:38
HostIp	是	是	String	主机IP 示例值： 10.0.0.1
LastScanTime	是	是	String	最后检测时间 示例值： 2021-10-27 00:09:38
MaxStatus	是	是	Uint64	检测中状态 示例值： 0

名称	必选	允许NULL	类型	描述
PassCount	是	是	Uint64	通过项 示例值： 1
Quuid	是	是	String	主机Quuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0
Status	是	是	Uint64	风险项处理状态状态：0-未通过，1-通过 示例值： 0
Uuid	是	是	String	主机Uuid 示例值： e5b4724c-49af-46ab-bd84-cdbae897e7e0

RegionSet

地域信息

被如下接口引用：DescribeBanRegions

名称	必选	允许NULL	类型	描述
RegionName	是	否	String	地域名称 示例值： region1
ZoneSet	是	否	Array of ZoneInfo	可用区信息 示例值：查看

HostDesc

展示登录审计白名单时的主机信息实体

被如下接口引用：DescribeLoginWhiteHostList

名称	必选	允许NULL	类型	描述
MachineIp	是	否	String	机器IP:已销毁的服务器IP为空 示例值： 1.1.1.1
MachineName	是	否	String	机器名 示例值： redis_node_cvm
MachineWanIp	是	否	String	公网IP:已销毁的服务器IP为空 示例值： 1.1.1.1
Quuid	是	否	String	机器uuid 示例值： 380add75-bb06-4cc4-84c5-cf806d102fba
Tags	是	否	Array of MachineTag	标签信息数组 示例值：查看
Uuid	是	否	String	主机安全uuid 示例值： 380add75-bb06-4cc4-84c5-cf806d102fba

AssetAppBaseInfo

资源管理进程基本信息

被如下接口引用：DescribeAssetAppList

名称	必选	允许NULL	类型	描述
BinPath	否	否	String	二进制路径 示例值： /root
ConfigPath	否	否	String	配置文件路径 示例值： /root
Desc	否	否	String	应用描述 示例值： app info
FirstTime	否	否	String	首次采集时间 示例值： 2022-07-15 11:27:01
IsNew	否	是	Int64	是否新增[0:否
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	否	String	主机内网IP 示例值： 10.0.0.11
MachineName	否	否	String	主机名称 示例值： agentyo
MachineWanIp	否	否	String	主机外网IP 示例值： 192.168.0.204
Name	否	否	String	应用名称 示例值： php
OsInfo	否	否	String	操作系统信息 示例值： centos 64bit
ProcessCount	否	否	Uint64	关联进程数 示例值： 1
ProjectId	否	否	Uint64	主机业务组ID 示例值： 1
Quuid	否	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Tag	否	是	Array of MachineTag	主机标签 示例值：查看
Type	否	否	Uint64	应用类型 1: 运维 2 : 数据库 3 : 安全 4 : 可疑应用 5 : 系统架构 6 : 系统应用 7 : WEB服务 99: 其他 示例值： 1
UpdateTime	否	是	String	数据更新时间 示例值： 2011-11-11 12:12:12
Uuid	否	否	String	主机Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116

名称	必选	允许NULL	类型	描述
Version	否	否	String	版本号 示例值： 1.0

AttackSourceEdge

攻击溯源路线描述

被如下接口引用：DescribeAttackSource

名称	必选	允许NULL	类型	描述
From	是	否	String	出发节点 示例值： node_a
To	是	否	String	目标节点 示例值： node_b

MachineTag

服务器标签信息

被如下接口引用：DescribeAssetAppList、DescribeAssetDatabaseList、DescribeAssetMachineList、DescribeAssetPortInfoList、DescribeAssetProcessInfoList、DescribeAssetWebAppList、DescribeAssetWebFrameList、DescribeAssetWebLocationList、DescribeAssetWebServiceInfoList、DescribeImportMachineInfo、DescribeLoginWhiteHostList、DescribeMachineList、DescribeMachines、DescribeMachinesSimple、DescribeRansomDefenseMachineList、DescribeRansomDefenseStrategyMachines

名称	必选	允许NULL	类型	描述
Name	是	否	String	标签名 示例值： redis_node
Rid	是	否	Int64	关联标签ID 示例值： 10
TagId	是	否	Uint64	标签ID 示例值： 1010

SecurityTrend

安全趋势统计数据。

被如下接口引用：DescribeSecurityTrends

名称	必选	允许NULL	类型	描述
Date	是	否	Date	事件时间。 示例值： 2023-07-11
EventNum	是	否	Uint64	事件数量。 示例值： 10

AssetLoadSummary

资源负载概况

被如下接口引用：DescribeAssetLoadInfo

名称	必选	允许NULL	类型	描述
Counts	是	否	Array of Uint64	负载量数组，依次为： [0%或未知数量， 0%～20%， 20%～50%， 50%～80%， 80%～100%] 示例值： [0,1,1,2,3,1]
Top5	是	是	Array of AssetLoadDetail	负载Top5 示例值：查看

AttackSourceNode

攻击溯源节点

被如下接口引用：DescribeAttackSource

名称	必选	允许NULL	类型	描述
EndTime	是	否	String	结束时间 示例值： 2021-03-30 19:17:28
EventId	是	否	Uint64	事件ID，为空的时候表示没有对应事件 示例值： 1
EventType	是	否	String	BRUTEFORCE:密码破解、MALWARE:木马、BASH:高危命令、RISK_DNS:恶意请求、LOGIN:异地登录、HOST:主机节点, TIME_ORDER：通用节点 示例值： BRUTEFORCE
Ip	是	否	String	节点ip 当节点为HOST时 示例值： 10.0.0.1
Level	是	否	Uint64	等级 0：提示，1：低危，2：中危，3：高危，4：严重 示例值： 0
NodeDesc	是	否	String	通用节点的描述 示例值： desc
NodeDetail	是	否	String	节点详情 示例值： detail
NodeId	是	否	String	节点ID 示例值： node-uniqueid
StartTime	是	否	String	开始时间 示例值： 2021-03-30 19:17:28
TimeLineNum	是	否	Uint64	时间线编号，同一个编号的节点属于同一个时间线 示例值： 1

EmergencyVul

应急漏洞信息

被如下接口引用：DescribeEmergencyVulList

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
AttackLevel	否	是	Uint64	攻击热度级别，大于等于3为热点攻击 示例值： 3
Category	是	否	Uint64	漏洞分类 1 web cms漏洞,2应用漏洞,4linux软件漏洞,5windows系统漏洞 示例值： 2
CveId	是	是	String	cve编号 示例值： CVE-2021-3156
CvssScore	是	是	Float	CVSS评分 示例值： 7.4
DefenseAttackCount	是	是	Uint64	已防御的攻击次数 示例值： 12
DefenseState	否	是	Bool	是否有漏洞主机开启漏洞防御 示例值： true
HostCount	是	是	Uint64	影响机器数 示例值： 2
IsSupportDefense	是	是	Uint64	是否支持防御， 0:不支持 1:支持 示例值： 1
Labels	是	是	String	漏洞标签 多个逗号分割 示例值： tag1,tag2
LastScanTime	是	否	String	最后扫描时间 示例值： 2024-11-04 09:57:28
Level	是	否	Uint64	漏洞风险级别 0：提示，1：低危，2：中危，3：高危，4：严重 示例值： 2
Method	否	是	Uint64	检测规则 0 - 版本比对, 1 - POC验证 示例值： 0
Progress	是	否	Uint64	扫描进度 示例值： 100
PublishDate	是	否	String	发布日期 示例值： 2024-09-04
Status	是	否	Uint64	漏洞状态 0未检测 1有风险 ，2无风险 ，3 检查中展示进度Progress字段 示例值： 1
VulId	是	否	Uint64	漏洞id 示例值： 1001
VulName	是	否	String	漏洞名称 示例值： Apache HTTP/2 协议拒绝服务漏洞(CVE-2023-44487)

VulOverview

漏洞概览

被如下接口引用：DescribeVulOverview

名称	必选	允许NULL	类型	描述
TodayCount	是	否	Int64	今日新增数量 示例值： 0
TotalCount	是	否	Uint64	总数 示例值： 12

AssetWebAppBaseInfo

资源管理Web应用列表信息

被如下接口引用：DescribeAssetWebAppList

名称	必选	允许NULL	类型	描述
Desc	否	否	String	应用描述 示例值： no name
Domain	否	否	String	站点域名 示例值： www.ay.com
FirstTime	否	否	String	首次采集时间 示例值： 2022-07-15 11:27:01
Id	否	否	String	应用ID 示例值： 10001
IsNew	否	否	Int64	是否新增[0:否
MachineExtraInfo	否	是	MachineExtraInfo	附加信息 示例值：查看
MachineIp	否	否	String	主机内网IP 示例值： 10.0.0.11
MachineName	否	否	String	主机名称 示例值： agent-domain
MachineWanIp	否	否	String	主机外网IP 示例值： 192.168.0.204
Name	否	否	String	应用名 示例值： Nginx
OsInfo	否	否	String	操作系统信息 示例值： Centos 64Bit
PluginCount	否	否	Uint64	插件数 示例值： 10
ProjectId	否	否	Uint64	主机业务组ID 示例值： 1
Quuid	否	否	String	主机Quuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
RootPath	否	否	String	根路径 示例值： /root
ServiceType	否	否	String	服务类型 示例值： Web
Tag	否	是	Array of MachineTag	主机标签 示例值：查看
UpdateTime	否	是	String	数据更新时间 示例值： 2011-11-11 12:12:12

名称	必选	允许NULL	类型	描述
Uuid	否	否	String	主机Uuid 示例值： acdd5474-6360-4fd4-bfc7-843162cb8116
Version	否	否	String	版本 示例值： 1.0.1
VirtualPath	否	否	String	虚拟路径 示例值： /data/tmp

ScreenRegionInfo

地域信息

被如下接口引用：DescribeScreenMachineRegions

名称	必选	允许NULL	类型	描述
Region	是	否	String	地域 示例值： ap-region1
RegionCode	是	否	String	地域代码，如 gz，sh，bj 示例值： gz
RegionId	是	否	Uint64	地域ID 示例值： 1
RegionName	是	否	String	地域名字 示例值： region1
RegionNameEn	是	否	String	地域英文名 示例值： ap-region1

ScreenRegionMachines

大屏主机3D图 列表

被如下接口引用：DescribeScreenMachines

名称	必选	允许NULL	类型	描述
AttackCnt	是	否	Uint64	潜在风险主机数 示例值： 12
IgnoreCnt	是	否	Uint64	省略展示多少主机，等于0时没有省略展示 示例值： 1
Machines	是	否	Array of ScreenMachine	主机列表 示例值：查看
Region	是	否	String	所有区域 示例值： ap-bangkok
RegionName	是	否	String	区域描述 示例值： region1
RiskCnt	是	否	Uint64	风险主机数量 示例值： 1
SafetyCnt	是	否	Uint64	无风险主机数 示例值： 12
TotalCount	是	否	Uint64	此区域的主机总数 示例值： 34
UnAgentOfflineCnt	是	否	Uint64	离线/未安装主机数 示例值： 12

MaPod

被如下接口引用：DescribeMaPodList

名称	必选	允许NULL	类型	描述
AlarmCount	否	是	Int64	负载告警数量 示例值： 10
ClusterId	否	是	String	集群ID 示例值： cls-ogbbasz4
ClusterName	否	是	String	集群名称 示例值： any_dev1
Id	否	是	Int64	ID 示例值： 1
IsEnabled	否	是	Int64	是否开启监控[1:开启
IsNew	否	是	Int64	是否15日内新增[1:是
IsSupportMa	否	是	Int64	是否支持微告警[1:是
Labels	否	是	Array of MaLabel	标签 示例值：查看
LearnEndTime	否	是	String	单个负载结束学习时间 示例值： 2024-01-01 00:00:00
LearnStartTime	否	是	String	单个负载开始学习时间 示例值： 2024-01-01 00:00:00
Name	否	是	String	主机名称 示例值： redis_node_cvm
Namespace	否	是	String	POD命名空间 示例值： system
NotSupportMaCode	否	是	Int64	不支持微告警的原因[0:支持
PodIp	否	是	String	PodIP 示例值： 10.0.0.1
Status	否	是	String	POD状态 示例值： Running

CanFixVulInfo

批量修复漏洞二次弹窗 漏洞主机信息

被如下接口引用：DescribeCanFixVulMachine

名称	必选	允许NULL	类型	描述
FixTag	是	是	Array of String	修复提示tag 示例值：["需要重启"]
HostList	是	是	Array of VulInfoHostInfo	该漏洞可修复的主机信息 示例值：查看
VulCategory	否	是	Uint64	漏洞分类1 web cms漏洞,2应用漏洞,4linux软件漏洞,5windows系统漏洞 示例值： 1
VulId	是	是	Uint64	漏洞id 示例值： 1373
VulName	是	是	String	漏洞名称 示例值： 本地提权漏洞

RansomDefenseStrategy

主机列表查询接口相应数据HostList的TagList节点

被如下接口引用：DescribeRansomDefenseStrategyList

名称	必选	允许NULL	类型	描述
BackupType	是	是	Uint64	备份模式： 0按周，1按天 示例值： 0
CreateTime	是	是	String	创建时间 示例值： 2022-12-12 12:12:12
Description	是	是	String	策略备注 示例值： subtitle
ExcludeDir	是	是	String	包含目录，用;分隔 示例值： /usr
Hour	是	否	String	备份执行时间点(0-23): 11:00;12:00 示例值： 11:00
Id	是	否	Int64	策略id 示例值： 1
IncludeDir	是	是	String	包含目录，用;分隔 示例值： /root
IsAll	是	否	Uint64	是否对所有主机生效 示例值： 1
MachineCount	是	是	Uint64	绑定机器数 示例值： 12
ModifyTime	是	是	String	最近修改时间 示例值： 2022-12-12 12:12:12
Name	是	否	String	策略名称 示例值： strategyName
SaveDay	是	否	Uint64	保存天数，0永久保存 示例值： 5
Status	是	否	Uint64	开启状态：0关闭，1开启 示例值： 1
Uin	是	是	String	操作uin 示例值： 1
Weekday	是	是	String	备份星期天数（1-7）：1;2;3;4 示例值： 1;2;3

ProductStatusInfo

产品试用状态查询接口Data出参

被如下接口引用：DescribeProductStatus

名称	必选	允许NULL	类型	描述
CanApplyTrial	是	否	Bool	是否可以申请试用，true可以申请 示例值： true
CanNotApplyReason	是	否	String	无法试用原因，可试用为空 示例值： 不是企业用户，不符合试用条件
FWUserStatus	是	否	Uint64	防护状态，1未防护，2防护中，3试用中，4已过期 示例值： 1
LastTrialTime	是	否	String	上次试用结束时间（不存在试用记录则为空） 示例值： 2022-06-23 10:25:45

MachineSnapshotInfo

机器快照信息

被如下接口引用：DescribeMachineSnapshot

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	快照创建时间 示例值： 2021-03-11 18:15:17
DiskId	是	否	String	磁盘id 示例值： adhakdh
HostIp	是	否	String	主机ip 示例值： 145.12.3.12
HostName	是	否	String	主机名称 示例值： redis_node_cvm
InstanceId	是	否	String	实例Id 示例值： ins-xjd734
Quuid	是	否	String	cvm id 示例值： 5a540076-d38a-4078-aa98-q45rt371d322
RegionId	是	否	Uint64	地区id 示例值： 1
SnapshotId	是	否	String	快照id 示例值： ajdajd
SnapshotName	是	否	String	快照名称 示例值： backup-2021-03-01

FullTextInfo

全文索引的相关配置

被如下接口引用：DescribeLogIndex

名称	必选	允许NULL	类型	描述
CaseSensitive	是	否	Bool	是否大小写敏感 示例值： false
ContainZH	是	否	Bool	Whether to contain zh characters 示例值： false
Tokenizer	是	否	String	分词符 示例值： \n\t\r

JavaMemShellDetail

java内存马事件详细信息

被如下接口引用：DescribeJavaMemShellInfo

名称	必选	允许NULL	类型	描述
Annotations	否	否	String	注释 示例值： 注释
Args	否	否	String	java进程命令行参数 示例值： org.apache.jasper.servlet.JasperLoader
ClassContent	否	否	String	java内存马二进制代码(base64) 示例值： cGFja2FnZSBjb20uY29tcGFueTsgIHB1YmxpYyBjbGFzcyBNYWluIHsgICAgICBwdWJsaWMgc3RhdGljIHZvaQ==
ClassContentPretty	否	否	String	java内存马反编译代码 示例值： package com.company; public class Main { public static voi
ClassLoaderName	否	否	String	java加载器类名 示例值： org.apache.jasper.servlet.JasperLoader
ClassName	否	否	String	类名 示例值： main.class
CreateTime	否	否	String	首次发现时间 示例值： 2021-01-20 16:17:11
Description	否	否	String	说明 示例值： 检测到java进程pid为1128220的org.apache.catalina.startup.Bootstrap类中存在木马
EventDescription	否	否	String	事件描述 示例值： 检测到Java服务进程中存在Java内存木马。Java内存马能长期驻留在内存中，接收攻击者输入，从而达到长期远程控制服务器的目的
Exe	否	否	String	java进程路径 示例值： /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
InstanceName	否	否	String	容器名 示例值： redis_node_cvm
InstanceState	否	否	String	实例状态：RUNNING,STOPPED,SHUTDOWN 示例值： RUNNING
Interfaces	否	否	String	继承的接口 示例值： java.IO.Writer,java.IO.Reader
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息 示例值：查看
MachineState	否	否	String	agent状态：OFFLINE,ONLINE 示例值： OFFLINE
Md5	否	否	String	类文件MD5 示例值： 37e54fce63f1ca6c82927caf7aa1c412
Pid	否	否	Uint64	进程pid 示例值： 1
PrivateIp	否	否	String	内网IP 示例值： 192.168.255.10
PublicIp	否	否	String	公网IP 示例值： 110.40.207.98
RecentFoundTime	否	否	String	最近检测时间 示例值： 2021-01-20 16:17:11
SecurityAdvice	否	否	String	安全建议 示例值： 检查Java服务访问日志，评估内存马是否被访问; 检查主机高危漏洞，修复高危漏洞并重启java服务
Status	否	否	Uint64	处理状态 0 -- 待处理 1 -- 已加白 2 -- 已删除 3 - 已忽略 4 - 已手动处理 示例值： 0
SuperClassName	否	否	String	父类名 示例值： java.lang.Object
Type	否	否	Uint64	内存马类型 0:Filter型 1:Listener型 2:Servlet型 3:Interceptors型 4:Agent型 5:其他 示例值： 1

Broadcasts

安全播报列表

被如下接口引用：DescribeSecurityBroadcasts

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	发布时间 示例值： 2021-03-30 19:17:28
Id	是	否	Uint64	文章唯一id 示例值： 12
Level	是	否	Uint64	危险程度 0：无， 1：严重， 2: 高危， 3:中危， 4: 低危 示例值： 1
Subtitle	是	否	String	副标题 示例值： 新版本支持漏洞修复
Title	是	是	String	文章名字 示例值： 漏洞爆发
Type	是	是	Uint64	类型：0=紧急通知，1=功能更新，2=行业荣誉，3=版本发布 示例值： 1

HostInfo

添加登录审计白名单的主机信息实体

被如下接口引用：AddLoginWhiteLists、ModifyLoginWhiteRecord

名称	必选	允许NULL	类型	描述
Quuid	是	否	String	主机Quuid 示例值： d99a1b46-cc2d-4633-a11f-4a7663d2523e
Uuid	是	否	String	Uuid主机 示例值： d99a1b46-cc2d-4633-a11f-4a7663d2523e

Place

登录地信息

被如下接口引用：AddLoginWhiteLists、DescribeLoginWhiteCombinedList、DescribeLoginWhiteList、DescribeLoginWhiteListNew、ModifyLoginWhiteInfo、ModifyLoginWhiteRecord

名称	必选	允许NULL	类型	描述
CityId	是	否	Uint64	城市 ID。 示例值： 99
CountryId	是	否	Uint64	国家ID 示例值： 1
Location	否	否	String	位置名称 示例值： location1:location2:location3
ProvinceId	是	否	Uint64	省份 ID。 示例值： 23

BaselineItemDetect

基线检测项

被如下接口引用：DescribeBaselineItemDetectList

名称	必选	允许NULL	类型	描述
DetectResult	是	是	String	检测结果Json字符串(废弃字段) 示例值： 废弃字段
DetectStatus	是	是	Int64	0:未通过 1:忽略 3:通过 5:检测中 示例值： 1
FirstTime	是	是	String	首次检测时间 示例值： 2021-02-01 12:00:00
FixMethod	是	是	String	修复方法 示例值： 创建执行MongoDB数据库活动的专用用户（一般为mongodb），并以此专用用户运行MongoDayay
HostCount	是	是	Int64	影响服务器数 示例值： 1
ItemDesc	是	是	String	项描述 示例值： 如果 Redis 以 root 权限启动且未授权访问，则会造成任意文件写入，最终导致命令执行漏洞。
ItemId	是	是	Int64	项Id 示例值： 1401
ItemName	是	是	String	项名称 示例值： Redis 基线合规检测
LastTime	是	是	String	最后检测时间 示例值： 2021-02-01 12:00:00
Level	是	是	Int64	风险等级 示例值： 2
NotPassedHostCount	是	是	Int64	未通过的服务器数 示例值： 1
PassedHostCount	是	是	Int64	通过的服务器数 示例值： 1
RuleId	是	是	Int64	所属规则ID 示例值： 120
RuleName	是	是	String	所属规则 示例值： 弱密码

错误码

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 cor
rect."
    },
    "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。

错误码	说明
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。

业务错误码

错误码	说明
InvalidParameter.IpNoValid	IP格式不合法。
InvalidParameter.NameHasRepetition	名字已重复。
FailedOperation.OpenProVersion	开通专业版失败。
InvalidParameter.ReverShellKeyFieldAllEmpty	进程名/目标IP/目标端口，不能同时为空。

错误码	说明
InvalidParameter.IllegalRequest	非法请求。
FailedOperation	操作失败。
FailedOperation.TooManyStrategy	创建基线策略超过上限。
FailedOperation.PartSeparate	多台主机隔离，部分或全部失败。
OperationDenied	操作被拒绝。
InvalidParameter.MissingParameter	参数缺失。
FailedOperation.SingleSeparate	单台主机隔离失败。
InvalidParameter.RuleHostDuplicateErr	规则类接口，主机重复。
FailedOperation.RescanVul	重新检测漏洞失败。
FailedOperation.APIServerFail	调用API服务失败。
FailedOperation.ProtectStartFail	开启防护失败。
FailedOperation.AgentOffline	客户端已离线。
ResourceNotFound.MachineNotFound	扫描机器不存在。
InvalidParameter.RuleHostipErr	规则类接口，主机IP不正确。
InvalidParameter	参数错误。
AuthFailure.UnauthorizedOperation	当前用户鉴权失败。
InvalidParameter.ParsingError	参数解析错误。
InvalidParameterValue.TagNameLengthLimit	标签名称长度不能超过15个字符。
InvalidParameter.DateRange	时间区间格式错误。
InternalError.MainDBFail	操作数据失败。
LimitExceeded.AreaQuota	超出批量添加数量。
InvalidParameter.PortNoValid	端口格式不合法。
InvalidParameter.RegexRuleError	正则参数格式错误。
InternalError	内部错误。
LimitExceeded	超过配额限制。

错误码	说明
FailedOperation.MachineDelete	卸载主机。
FailedOperation.PrePayMode	不能关闭预付费模式专业版。
FailedOperation.Recover	回复木马失败。
UnsupportedOperation	操作不支持。
AuthFailure	CAM签名/鉴权错误。
InvalidParameterValue	参数取值错误。
FailedOperation.Export	导出文件失败。
ResourceInUse	资源被占用。
UnauthorizedOperation	未授权操作。
ResourceInsufficient	资源不足。
MissingParameter	缺少参数错误。
FailedOperation.NoProfessionHost	无专业版主机。
InvalidParameter.InvalidFormat	参数格式错误。
FailedOperation.LicenseExceeded	可用license数量不足，缺少1个license，请购买新license。
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
UnknownParameter	未知参数错误。
FailedOperation.CloseProVersion	关闭专业版失败。