Cloud Workload Protection Platform

Product Documentation

Contents

Cloud Workload Protection Platform 7
- Product Introduction 7
  - CWPP Overview 7
  - Advantages 9
  - Basic Concepts 10
  - Scenarios 11
  - Associated Products 12
- Quick Start 13
  - Quick Start 13
- Operation Guide 15
  - Security Overview 15
  - Asset Overview 18
  - Host List 21
  - Asset Fingerprint 23
  - File Detection 25
  - Abnormal Log-in 29
  - Password Cracking 32
  - Malicious Requests 35
  - Local Privilege Escalation 37
  - Rebound Shell 40
  - High-risk Commands 42
  - Network Attack 45
  - Java Memory Trojan 48
  - Core File Monitoring 50
  - Vulnerability Management 53
  - Security Baseline 57
  - Common Operations 59
    - Installing an Agent on an Unprotected Host 59
    - Vulnerability Scan for a Single Host 61
    - Baseline Scan for a Single Host 62
- Purchase Guide 66
  - Overview 66
- Troubleshooting 68
  - Troubleshooting Ideas of Linux Intrusion Issues 68
  - Troubleshooting ideas of Windows intrusion issues 73
  - Offline Troubleshooting for Linux Clients 77
  - Offline Troubleshooting for Windows Clients 79
  - Exception Login Reminder 80
- API Documentation 83
  - Cloud Workload Protection(cwp) 83
    - version(2018-02-28) 83
      - API overview 83
      - CallingMethod 101
        - signaturev1 101
        - signaturev3 109
        - request 118
        - result 119
        - PublicParameter 122
      - Advanced Defense APIs 124
        - CreateMaWorkloadLabel 124
        - CreateProtectServer 126
        - DeleteAttackLogs 128
        - DeleteMaConnEvent 130
        - DeleteMaCustomPolicy 132
        - DeleteMaLabel 134
        - DeleteMaSelfLearnPolicy 136
        - DeleteMaWhitelist 138
        - DeleteProtectDir 140
        - DeleteWebPageEventLog 142
        - DescribeAttackEventInfo 144
        - DescribeAttackEvents 146
        - DescribeAttackLogInfo 148
        - DescribeAttackLogs 151
        - DescribeAttackStatistics 153
        - DescribeAttackTop 156
        - DescribeAttackTrends 158
        - DescribeAttackVulTypeList 160
        - DescribeMaConnEventList 161
        - DescribeMaCustomPolicyList 163
        - DescribeMaGlobalConf 165
        - DescribeMaHostList 167
        - DescribeMaLabel 169
        - DescribeMaLabelList 171
        - DescribeMaLabelSourceList 173
        - DescribeMaPodList 175
        - DescribeMaSelfLearnConfig 177
        - DescribeMaSelfLearnPolicyList 180
        - DescribeMaSummary 182
        - DescribeMaWhitelist 185
        - DescribeMaWorkloadLabel 187
        - DescribeMaWorkloadList 189
        - DescribeMachineList 191
        - DescribeNetAttackSetting 193
        - DescribeProtectDirList 194
        - DescribeProtectDirRelatedServer 196
        - DescribeServerRelatedDirInfo 198
        - DescribeWebPageEventList 200
        - DescribeWebPageGeneralize 202
        - DescribeWebPageProtectStat 204

- DescribeWebPageServiceInfo ... 206
- DisableSelfLearn ... 208
- ExportAttackEvents ... 210
- ExportAttackLogs ... 212
- ExportMaConnEventList ... 213
- ExportMaCustomPolicyList ... 215
- ExportMaHostList ... 217
- ExportMaPodList ... 219
- ExportMaSelfLearnPolicyList ... 221
- ExportMaWhitelist ... 223
- ExportProtectDirList ... 225
- ExportWebPageEventList ... 226
- ModifyMaConnEventType ... 228
- ModifyMaCustomPolicy ... 230
- ModifyMaCustomPolicyStatus ... 232
- ModifyMaGlobalConf ... 234
- ModifyMaLabel ... 236
- ModifyMaSelfLearnConfig ... 238
- ModifyMaWhitelist ... 240
- ModifyMaWhitelistStatus ... 242
- ModifyMaWorkloadLabel ... 243
- ModifyMaWorkloadMonitor ... 245
- ModifyMemShellRules ... 247
- ModifyNetAttackSetting ... 249
- ModifyWebPageProtectDir ... 250
- ModifyWebPageProtectSetting ... 252
- ModifyWebPageProtectSwitch ... 254

• Asset Management APIs ... 256
- CreateIncidentBacktracking ... 256
- DeleteCloudVendorAccountAK ... 258
- DeleteMachine ... 260
- DeleteMachineTag ... 262
- DeleteTags ... 264
- DescribeAccountStatistics ... 266
- DescribeAssetAppList ... 268
- DescribeAssetAppProcessList ... 270
- DescribeAssetCoreModuleInfo ... 272
- DescribeAssetCoreModuleList ... 274
- DescribeAssetDatabaseInfo ... 276
- DescribeAssetDatabaseList ... 278
- DescribeAssetHostTotalCount ... 280
- DescribeAssetInfo ... 282
- DescribeAssetInitServiceList ... 285
- DescribeAssetJarInfo ... 287
- DescribeAssetJarList ... 289
- DescribeAssetMachineDetail ... 291
- DescribeAssetMachineList ... 293
- DescribeAssetPlanTaskList ... 295
- DescribeAssetPortInfoList ... 297
- DescribeAssetProcessInfoList ... 299
- DescribeAssetRecentMachineInfo ... 301
- DescribeAssetSystemPackageList ... 303
- DescribeAssetUserInfo ... 305
- DescribeAssetUserList ... 307
- DescribeAssetWebAppList ... 309
- DescribeAssetWebAppPluginList ... 311
- DescribeAssetWebFrameList ... 313
- DescribeAssetWebLocationInfo ... 315
- DescribeAssetWebLocationList ... 317
- DescribeAssetWebServiceInfoList ... 319
- DescribeAssetWebServiceProcessList ... 321
- DescribeCloudVendorAccountAKList ... 323
- DescribeComponentStatistics ... 325
- DescribeComponents ... 327
- DescribeExportMachines ... 328
- DescribeHistoryAccounts ... 330
- DescribeImportMachineInfo ... 332
- DescribeMachineInfo ... 333
- DescribeMachineOsList ... 336
- DescribeMachineRegionList ... 338
- DescribeMachineRegions ... 340
- DescribeMachines ... 342
- DescribeOpenPortStatistics ... 344
- DescribeProcessStatistics ... 346
- DescribeTagMachines ... 348
- DescribeTags ... 350
- EditTags ... 352
- ExportAssetCoreModuleList ... 354
- ExportAssetWebServiceInfoList ... 356
- ModifyMachineRemark ... 358
- ScanAsset ... 360
- SyncAssetScan ... 362
- UpdateMachineTags ... 363

• Baseline Management APIs ... 365
- ChangeRuleEventsIgnoreStatus ... 365
- CreateBaselineStrategy ... 367
- DeleteBaselineStrategy ... 369
- DescribeBaselineAnalysisData ... 371
- DescribeBaselineBasicInfo ... 373
- DescribeBaselineDetail ... 375
- DescribeBaselineEffectHostList ... 377

- DescribeBaselineHostTop ... 379
- DescribeBaselineList ... 381
- DescribeBaselineRule ... 383
- DescribeBaselineScanSchedule ... 385
- DescribeBaselineStrategyDetail ... 387
- DescribeBaselineStrategyList ... 389
- DescribeBaselineTop ... 391
- DescribeIgnoreBaselineRule ... 393
- DescribeIgnoreRuleEffectHostList ... 395
- DescribeStrategyExist ... 397
- ExportBaselineEffectHostList ... 399
- ExportBaselineList ... 401
- ExportIgnoreBaselineRule ... 403
- ExportIgnoreRuleEffectHostList ... 405
- UpdateBaselineStrategy ... 407

• Baseline Management APIs (New) ... 409
- DeleteBaselinePolicy ... 409
- DeleteBaselineRule ... 411
- DeleteBaselineRuleIgnore ... 413
- DeleteBaselineWeakPassword ... 415
- DescribeBaselineDetectList ... 417
- DescribeBaselineDetectOverview ... 419
- DescribeBaselineDownloadList ... 421
- DescribeBaselineFixList ... 423
- DescribeBaselineHostDetectList ... 425
- DescribeBaselineHostIgnoreList ... 427
- DescribeBaselineHostRiskTop ... 429
- DescribeBaselineItemDetectList ... 431
- DescribeBaselineItemIgnoreList ... 433
- DescribeBaselineItemInfo ... 435
- DescribeBaselineItemList ... 437
- DescribeBaselineItemRiskTop ... 439
- DescribeBaselinePolicyList ... 441
- DescribeBaselineRuleCategoryList ... 443
- DescribeBaselineRuleDetectList ... 445
- DescribeBaselineRuleIgnoreList ... 447
- DescribeBaselineRuleList ... 449
- DescribeBaselineWeakPasswordList ... 451
- DescribeHotVulTop ... 453
- DescribeIgnoreHostAndItemConfig ... 455
- DescribeVulStoreList ... 457
- ExportBaselineFixList ... 459
- ExportBaselineHostDetectList ... 461
- ExportBaselineItemDetectList ... 463
- ExportBaselineItemList ... 465
- ExportBaselineRuleDetectList ... 467
- ExportBaselineWeakPasswordList ... 469
- FixBaselineDetect ... 471
- ModifyBaselinePolicy ... 473
- ModifyBaselinePolicyState ... 475
- ModifyBaselineRule ... 477
- ModifyBaselineRuleIgnore ... 479
- ModifyBaselineWeakPassword ... 481
- StartBaselineDetect ... 483
- StopBaselineDetect ... 485
- SyncBaselineDetectSummary ... 487

• Expert Service APIs ... 489
- DescribeEmergencyResponseList ... 489
- DescribeMonthInspectionReport ... 491

• Intrusion Detection - APIs of Logins from Unusual Locations ... 493
- DeleteLoginWhiteList ... 493
- DeleteNonlocalLoginPlaces ... 495
- DescribeHostLoginList ... 497
- DescribeLoginWhiteCombinedList ... 499
- DescribeLoginWhiteList ... 501
- DescribeUsualLoginPlaces ... 503
- ExportNonlocalLoginPlaces ... 505

• Intrusion Detection - File Scanning and Cleaning APIs ... 507
- CreateNetAttackWhiteList ... 507
- CreateScanMalwareSetting ... 509
- DeleteMalwareScanTask ... 511
- DeleteMalwares ... 513
- DeleteNetAttackWhiteList ... 515
- DescribeJavaMemShellList ... 517
- DescribeMalWareList ... 518
- DescribeMalwareFile ... 520
- DescribeMalwareInfo ... 522
- DescribeMalwareRiskWarning ... 524
- DescribeMalwareTimingScanSetting ... 526
- DescribeNetAttackWhiteList ... 528
- DescribeScanMalwareSchedule ... 530
- DescribeServersAndRiskAndFirstInfo ... 532
- ExportMalwares ... 534
- ModifyMalwareTimingScanSettings ... 536
- ModifyNetAttackWhiteList ... 538
- RecoverMalwares ... 540
- SeparateMalwares ... 542
- TrustMalwares ... 544
- UntrustMalwares ... 546

• Intrusion Detection - High-Risk Command APIs ... 548
- CheckBashRuleParams ... 548

- DeleteBashEvents ... 550
- DeleteBashRules ... 552
- DescribeBashEvents ... 554
- DescribeBashEventsNew ... 556
- DescribeBashRules ... 558
- EditBashRules ... 560
- ExportBashEvents ... 562
- SetBashEventsStatus ... 564
- SwitchBashRules ... 566

• Intrusion Detection - Local Privilege Escalation APIs ... 568
- DeletePrivilegeEvents ... 568
- DeletePrivilegeRules ... 570
- DescribePrivilegeEvents ... 572
- DescribePrivilegeRules ... 574
- ExportPrivilegeEvents ... 576

• Intrusion Detection - Malicious Request APIs ... 578
- DeleteMaliciousRequests ... 578
- DescribeMaliciousRequestWhiteList ... 580
- DescribeRiskDnsList ... 582
- ExportMaliciousRequests ... 584

• Intrusion Detection - Password Cracking APIs ... 585
- DeleteBruteAttacks ... 585
- DescribeBanMode ... 587
- DescribeBanRegions ... 589
- DescribeBanStatus ... 591
- DescribeBanWhiteList ... 593
- DescribeBruteAttackList ... 595
- DescribeBruteAttackRules ... 596
- ExportBruteAttacks ... 598
- ModifyBanMode ... 599
- ModifyBanStatus ... 601
- ModifyBruteAttackRules ... 603
- StopNoticeBanTips ... 605

• Intrusion Detection - Reverse Shell APIs ... 607
- DeleteMemShellRules ... 607
- DeleteReverseShellEvents ... 609
- DeleteReverseShellRules ... 611
- DeleteReverseShellRulesAggregation ... 613
- DescribeMemShellRules ... 615
- DescribeReverseShellEvents ... 617
- DescribeReverseShellRules ... 619
- DescribeReverseShellRulesAggregation ... 621
- DescribeReverseShellSystemPolicyConfig ... 623
- DescribeShellPolicyList ... 625
- ExportReverseShellEvents ... 627
- ModifyReverseShellRulesAggregation ... 629
- ModifyReverseShellSystemPolicyConfig ... 631
- ModifyShellPolicyStatus ... 633

• Other APIs ... 635
- CreateLoginPermissionPush ... 635
- DeleteLogClsDeliverInfo ... 638
- DeleteScanTask ... 639
- DescribeAssetEnvList ... 641
- DescribeClientException ... 643
- DescribeClsAccountStatus ... 645
- DescribeClsLogsets ... 647
- DescribeClsTopics ... 649
- DescribeCustomerDetail ... 651
- DescribeGeneralStat ... 653
- DescribeLogClsDeliverInfo ... 655
- DescribeLogStorageConfig ... 657
- DescribeLogStorageRecord ... 659
- DescribeLoginPermission ... 661
- DescribeMachineInfoByHashKey ... 663
- DescribeMachineLoginType ... 665
- DescribeMachineLoginTypeStatus ... 667
- DescribeOrderList ... 669
- DescribeOverviewStatistics ... 671
- DescribeProVersionInfo ... 673
- DescribeProVersionStatus ... 675
- DescribeRecommendedProtectCpu ... 677
- DescribeScanState ... 679
- DescribeScanTaskDetails ... 681
- DescribeSecurityDynamics ... 684
- DescribeSecurityEventStat ... 686
- DescribeSecurityEventsCnt ... 689
- DescribeSecurityTrends ... 692
- DescribeTaskDuration ... 695
- DescribeTrialReport ... 697
- DescribeUsersConfig ... 699
- DescribeVersionStatistics ... 701
- DescribeVulTrend ... 703
- ExportScanTaskDetails ... 705
- ExportSecurityTrends ... 706
- ExportTasks ... 708
- ModifyEventAttackStatus ... 709
- ModifyLogClsDeliverInfo ... 711
- ModifyLogClsDeliverSwitch ... 713
- ModifyLogStorageConfig ... 714
- ModifyMachineLoginType ... 716
- ModifyOrder ... 718

- ModifyUsersConfig ... 719
- ModifyVulDefenceSwitch ... 721
- Security Operations APIs ... 723
  - CreateSearchLog ... 723
  - CreateSearchTemplate ... 725
  - DeleteSearchTemplate ... 727
  - DescribeESAggregations ... 729
  - DescribeHistoryService ... 731
  - DescribeIndexList ... 732
  - DescribeLogStorageStatistic ... 734
  - DescribeSearchExportList ... 736
  - DescribeSearchLogs ... 738
  - DescribeSearchTemplates ... 740
- Settings Center APIs ... 742
  - CreateAgentInstallTask ... 742
  - CreateLicenseOrder ... 744
  - DeleteLicenseRecord ... 746
  - DescribeAgentInstallResult ... 748
  - DescribeAgentInstallTaskResult ... 750
  - DescribeChangingAssetInfo ... 752
  - DescribeLicenseBindList ... 754
  - DescribeLicenseBindSchedule ... 755
  - DescribeLicenseGeneral ... 757
  - DescribeLicenseList ... 759
  - DescribeSaveOrUpdateWarnings ... 760
  - DescribeWarningList ... 762
  - DescribeWarningServiceIPList ... 764
  - DestroyOrder ... 766
  - ExportLicenseDetail ... 768
  - ModifyAssetsProtectionStatus ... 770
  - ModifyAutoOpenProVersionConfig ... 772
  - ModifyLicenseBinds ... 774
  - ModifyLicenseOrder ... 775
  - ModifyLicenseUnBinds ... 777
  - ModifyOrderAttribute ... 778
  - ModifyWarningSetting ... 780
- Vulnerability Management APIs ... 782
  - CancelIgnoreVul ... 782
  - CreateEmergencyVulScan ... 784
  - DescribeEmergencyVulList ... 786
  - DescribeInjectRiskyServiceSwitch ... 788
  - DescribeScanSchedule ... 789
  - DescribeScanVulSetting ... 791
  - DescribeUndoVulCounts ... 793
  - DescribeVulCountByDates ... 795
  - DescribeVulDefenceOverviewCount ... 796
  - DescribeVulDefenceSettingList ... 798
  - DescribeVulEffectHostList ... 800
  - DescribeVulHostCountScanTime ... 801
  - DescribeVulHostTop ... 803
  - DescribeVulInfoCvss ... 804
  - DescribeVulLevelCount ... 805
  - DescribeVulList ... 806
  - DescribeVulTop ... 808
  - ExportVulDetectionExcel ... 809
  - ExportVulDetectionReport ... 810
  - ExportVulEffectHostList ... 811
  - ExportVulList ... 812
  - IgnoreImpactedHosts ... 814
  - ModifyInjectRiskyServiceSwitch ... 816
  - ScanVul ... 817
  - ScanVulAgain ... 819
  - ScanVulSetting ... 821
- Data structure ... 822
- ErrorCode ... 866

Product Introduction
CWPP Overview

Cloud Workload Protection Platform (CWPP) Overview

A CWPP is a security solution that protects cloud workloads like virtual machines, containers, and serverless functions across public, private, and hybrid clouds. It provides continuous monitoring, threat detection, vulnerability management, and policy enforcement to keep cloud applications secure and compliant.

Qualifications

The CWPP holds several prestigious international certifications, including the CSA CSTR (Cloud Security Technology Review) from the Cloud Security Alliance./B100: Achieved certification 42 times consecutively with a perfect 100% pass rate

- AV-Comparatives (AV-C): Awarded 29 A+ ratings and recognized as a Top Rated product for three consecutive years
- Gartner: Included in the Market Guide for Cloud Workload Protection Platforms
- AMTSO: Active member of the Anti-Malware Testing Standards Organization
- AVAR: Member of the Association of Anti-Virus Asia Researchers
- EICAR: Member of the European Institute for Computer Anti-Virus Research

How It Works

Install the CWPP agent on the server to enable protection. When you initiate a detection task through the CWPP console, the agent carries out the task and sends the results back. You can then review and manage security events directly from the CWPP console.

Term	Description
CWPP Console	Converge Cloud’s independently developed cloud-native security system offers a comprehensive, all-in-one solution for cloud workload protection, covering prevention, defense, detection, and response.

Term	Description
Agent	The official security plugin for CWPP, designed for servers operating in hybrid cloud environments. It synchronizes risk information to the CWPP in real time and executes detection or processing tasks assigned by the CWPP Console.
Converge Cloud Servers	CVM, Lighthouse, and ECM.
Non-Converge Cloud Servers	Third-party servers and IDC servers
	A Cloud Workload Protection Platform (CWPP) is a centralized security processing hub designed to continuously monitor and analyze data from various servers. It provides comprehensive protection by leveraging six core security engines, each addressing different aspects of server security: 1. TAV Engine specializes in the efficient detection and removal of binary Trojan viruses. 2. BinaryAI Engine is a deep learning-powered binary analysis engine that effectively identifies and eliminates malicious software samples. 3. Cloud Security Engine utilizes a multi-engine cloud detection system and deep self-learning algorithms to detect and remove common Trojans and viruses globally. 4. Threat Intelligence Engine draws from a vast, constantly updated threat intelligence database to identify malicious files, IP addresses, and domain names. 5. Anti-Attack Engine monitors and defends against real-time cyberattacks, including Webshell threats, exploitation of Struts vulnerabilities, code repository access, code injection, and brute force attacks, offering automated defense mechanisms. 6. Unusual Behavior Engine analyzes abnormal behavior patterns to detect complex, multi-stage threats and provides real-time alerts on suspicious intrusions.

Advantages

Advantages

Con Cloud CWPP offers the following benefits:

Advantage	Converge Cloud CWPP	Other Host Security Products
Unauthorized Access Behavior Monitoring	By leveraging threat intelligence gathered from across the global Internet, CWPP can detect hacker attacks in real time.	The analysis relies on behavior data from a single server, resulting in limited detection capability and delayed response times.
Trojan Threat Detection	The CWPP backend integrates Converge PC Manager's next-generation TAV antivirus engine and the Hubble Analysis System to provide instant responses to unknown threats. Additionally, its machine learning-powered WebShell detection engine effectively identifies and neutralizes encrypted and obfuscated malicious scripts.	Without the capability to detect executable malicious files, WebShell detection relies solely on regular expressions and character logic matching, which often results in high rates of false positives and false negatives.
	Operational data from cloud platform servers is automatically linked and ready for use as soon as you purchase a CVM instance. Security policies are updated automatically in the cloud, eliminating the need for manual management of security detection scripts.	Manual installation of the product requires logging into each individual server, and configuring security policies demands personnel with specialized security expertise.
	Security events can be centrally managed through the console, removing the need to access multiple servers individually. This centralized server asset management allows you to swiftly build a visualized security platform.	You must log in to each server individually to handle security events one at a time.
	Using self-developed lightweight agents, CWPP performs the majority of its computing and protection tasks in the cloud, minimizing the consumption of server resources.	Software clients use a significant amount of memory (typically over 100 MB), which can negatively impact server performance during peak periods.

Basic Concepts

Basic Concepts

Common concepts of CWPP are as follow.

- A security baseline refers to a defined set of standards and fundamental requirements that system and service security settings must comply with to fulfill security objectives. Various configuration and policy areas such as account settings, password policies, authorization controls, log management, and network configurations are assessed to determine whether a product meets the security baseline. The evaluation results provide an indication of the overall security posture of the server.
- A Trojan virus is malicious code or a backdoor program concealed within legitimate applications. It can damage or delete files, steal passwords, record keystrokes, launch DDoS attacks, and perform other harmful actions.
- A WebShell is a command execution environment embedded in webpage files like .asp, .php, .jsp, or .cgi, functioning as a type of web backdoor. Once hackers gain access to a website, they typically hide these backdoor files among the regular webpage files within the website server's WEB directory. This allows them to access the asp or php backdoor through a browser, providing a command execution environment to control the website server.
- Host vulnerability detection is a process performed by a CWPP agent to identify vulnerabilities on a server. The vulnerability detection module operates directly on the server, either verifying or gathering information to assess the presence of security weaknesses.
- Generally, a component (or common component) at the server layer refers to a web container or software associated with a specific service or application, such as Nginx or WordPress. In contrast, a system component typically refers to non-web system software.
- A common component vulnerability (also known as a common vulnerability) primarily refers to a security flaw found in widely used components rather than in business-specific code. Examples include SQL injection in WordPress or the ShellShock vulnerability in the Bash component.
- Unauthorized access is an issue that arises from failing to meet the security baseline, primarily due to insufficient restrictions on access conditions for certain services, such as weak password settings or lack of access source controls. This allows anyone to connect to the service and perform operations, leading to security vulnerabilities.
- By gathering RDP and SSH login logs from the server, details including the source IP address, username, login time, and location are transmitted to the cloud for risk analysis, enabling real-time alerts for unauthorized login attempts.
- Isolation technology separates and contains malicious Trojan and virus files to prevent their spread.

Scenarios

Scenarios

When a server is compromised, it can lead to:

- Business Disruption: Critical databases and files may be altered or deleted, rendering services unavailable and potentially paralyzing your entire system.
- Data Breaches: Cybercriminals can exfiltrate sensitive data and sell it, leading to customer privacy violations, loss of trust, and long-term damage to your brand reputation.
- Ransomware Attacks: Hackers can infiltrate your server and deploy ransomware that encrypts your data, demanding payment for decryption often with no guarantee of recovery.
- Service Instability: Unauthorized mining software or DDoS malware can be installed to exploit your server resources for profit, severely degrading system performance and causing service outages.

CWPP provides strong protection against these threats by proactively securing your servers, reducing security vulnerabilities, and maintaining stable and continuous system operations.

Associated Products

Associated Products

The following Converge Cloud products are involved while using CWPP:

Converge Cloud	CWPP Feature Involved	Description
CVM	All features	CVM is a computing service protected by CWPP.
Cloud Block Storage	Vulnerability fix	The auto fix of vulnerabilities feature of CWPP requires snapshot backup, which is supported by CBS.

Quick Start
Quick Start

*

Step 1: Install Host Security

The CWP client is a Protection Plugin provided by CWP. To use CWP functionality, you must first install this plugin.
1.Log in to the tenant console, select Product Management > Security > CWPP, and enter the CWPP tenant console.
2.In the left sidebar, select Asset Management > Host List and click to view the installation guide.

Step 2: Operate the CWP

The tenant side of CWPP supports displaying the security risk events of the host, detecting and isolating Trojan files, detecting vulnerabilities, detecting and recognizing suspicious login behaviors and performing allowlist processing on them, configuring password cracking behavior blocking settings, and configuring alarms. For details, see Operation Guide.

Step 3: Troubleshooting

If the host is hacked, you can follow the intrusion troubleshooting guide to troubleshoot the problem and restore the normal running of the website or system. For details, see Linux intrusion troubleshooting ideas or Windows intrusion troubleshooting ideas.

Step 4: Uninstall Host Security

If you no longer need CWP protection, you can uninstall the CWP client. There are two ways to uninstall CWP: console uninstallation and system uninstallation. The following is a detailed introduction:

Uninstall in the Console
1.Log in to the CWPP tenant console, in the left sidebar, select Asset Management > Host list, and check whether your CVM has installed CWP.
2.In the server list, select the server for which you want to uninstall the CWP client. Click

Enter the System to Uninstall

- Windows system: Follow the path C:\Program Files\QCloud\cwpp\uninst.exe , find uninst.exe and double-click the file to uninstall.
- Linux system: Enter the command: if [-w '/usr']; then /usr/local/qcloud/cwpp/uninst.sh ; else /var/lib/qcloud/cwpp/uninst.sh ; fi to uninstall.

Operation Guide
Security Overview

This document will introduce the features and directions of each module of Security Overview.

Overview

The security overview of Cloud Workload Protection Platform (CWPP) displays your cloud workload protection score, pending risks, security protection status, risk trends and real-time dynamics of CWPP in real time; it offers documentation and upgrade service recommendations for CWPP to help you defend against hacker intrusion risks and attack threats, ensuring the security of enterprise hosts.

Operation Guide

1.Log in to the tenant-side console of CWPP.
2.Select Security Overview in the left navigation to view security overview information and related processing operations. The module descriptions are as follows.

Security Status

1. In the security status, your cloud workload protection score and the following three types of security risks are shown, and a quick processing entry is provided.
    - Intrusion detection: includes 7 features of the intrusion detection module, namely malicious file scan, abnormal login, password cracking, malicious request, rebound Shell, local privilege escalation, high-risk command, and consolidated statistics of the number of pending risks and number of affected hosts.
    - Vulnerability risk: includes Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, application vulnerabilities, and consolidated statistics of the number of pending risks and number of affected hosts.
    - Baseline risk: only count the number of pending baseline risks and the number of affected hosts.
2. The CWP status is divided into 3 levels:

Level	Health Checkup Score	Text Color	Status Description

Level	Health Checkup Score	Text Color	Status Description
Excellent	90-100 points	Green	The asset safety status is good and needs to be maintained and inspected regularly.
Medium-risk	60-89 points	Orange	There are relatively many security risks in assets. It is recommended that you handle security incidents in a timely manner.
High-risk	20-59 points	Red	Serious security risks exist in the assets. Handle the security incident as soon as possible.

> Note:
>
> The lowest health checkup score for CWPP status is 20 points.

Deduction items will be calculated based on the classification of security incidents. The following are the security incident classification and deduction rules:

Security Event (Counted by Number of Events)	Point Deduction Per Instance	Maximum Points Lost
Severe	Trojans, viruses, and successful brute force attacks.	50 points
High-risk	High-risk vulnerabilities, high-risk baselines, remote log-in, local privilege escalation, rebound shell, and high-risk commands.	10 points
Medium-risk	Medium-risk vulnerabilities, medium-risk baselines.	3 points
Low-risk	Low-risk vulnerabilities and low-risk baselines.	2 points
Others	Basic editions (non-protected state).	1 point

Security Protection

1. In Security Protection, show the full-process solution (prevention-defense-detection-response) provided by CWPP to deal with intrusion attacks, and display in detail the security protection items required at each stage. If all protection features are activated, intuitively understand the current situation of your host security and provide quick access to security risk handling.

Protection Detail

In Protection Detail, you can view the total number of hosts, total number of online hosts, number of shutdown or offline hosts, number of hosts without client installation, number of protected hosts, number of Ultimate Edition hosts, number of Basic Edition hosts. It also provides asset update time, virus database update time, vulnerability database update time, and security engine protection information.

> Note:
>
> Since the protection level of the basic edition host is relatively weak, the number of protected hosts contains only Ultimate Edition hosts.

Risk Trend

The risk trend feature uses a line chart to show you the security risk and threat trends in the past 7 days, 14 days, or 30 days, and supports filtering and viewing by time period. Hovering the mouse over the trend chart will display the number of security events such as file detection, password cracking, exception log-in, vulnerability risk, baseline risk, etc. on that date. Click the upper right corner to download the security event count for the selected date to your computer.

> Note:
>
> The data source is the number of newly added pending events on the day, which is updated every hour. Historical events will be retained and will not change.

Real-Time Dynamic

The real-time dynamic feature displays discovered host risks and threat events in real time in reverse chronological order. Click the host IP in the blue field to navigate to Host Details, where you can view various risks of this host security; click View Detail to jump to the corresponding event handling page.

Asset Overview

this document guides you through the feature modules and operations of Asset Overview.

Overview

Asset Overview statistically inventories and visually presents host and key asset fingerprint data from the asset dimension, making it user-friendly to understand asset status.

Prerequisites

Only Ultimate Edition hosts support asset fingerprint data collection and synchronization. Basic edition or unprotected hosts do not support it.

Background Information

Only hosts of the paid protection edition can collect asset fingerprint data.
The asset fingerprints supported by each edition are as follows:

CWP Protection Version	Collected Asset Fingerprint Item
Professional Edition	Ten Items: resource monitoring, account, port, process, software application, database, web application, web service, web framework, website

CWP Protection Version	Collected Asset Fingerprint Item
Flagship edition	16. Resource monitoring, account, port, process, software application, database, Web application, Web service, Web framework, website, Jar package, startup service, scheduled task, environment variable, kernel module

> Note:
>
> Asset fingerprint data are automatically collected every 8 hours. Manual collection is supported.

Overview

Log in to the CWPP tenant-side console, choose Asset Management > Overview in the left sidebar to access the overview page.

1. Asset overview panel, which allows you to view all hosts and the statistical data of each asset fingerprint.

2. Host overview trend chart (total number of hosts, number of online hosts, number of offline hosts, number of hosts at risk) supports querying time periods no longer than the past 3 months and supports download and export; TOP 5 host tags, showing the 5 most commonly used tags among all hosts.

3. Resource monitoring overview, which allows you to view CPU load, memory usage, hard disk usage distribution and corresponding TOP 5.

   > Note:
   >
   > About CPU load, currently only support retrieval of CPU load of servers running Linux system. Windows system is currently unidentified.

4. View TOP 5 accounts, TOP 5 ports, TOP 5 processes, TOP 5 software applications, TOP 5 databases, TOP 5 Web applications, TOP 5 Web services, TOP 5 Web frameworks, TOP 5 Web sites.

   > Note:

> The TOP 5 asset fingerprints are the data of the TOP 5 items sorted in descending order according to the quantity of servers to which the fingerprints (account, port, process, software application, database, Web application, Web service, Web framework, website) belong.

Host List

This document describes the various functional modules and operations of the host list.

Overview

The host list allows you to view information about all servers currently connected to CWP, helping you fully understand the security status of your assets.

Use Limits

Host range that can be integrated with CWPP

Specific Host Types	Linux System	Windows System
overlay host	Supported architectures: x86, arm	Supported architecture: x86.
underlay host	Supported architectures: x86, arm	Supported architecture: x86.

Operation Steps

1. Log in to the CWPP tenant-side console. In the left sidebar, select Asset Management > Host List.
2. On the host list page, you can perform operations such as querying asset status, installing/ uninstalling the CWP client.

Host Status

In Host Status, you can view the total number of hosts, the number of defended hosts (since the protection level of the basic edition host is relatively weak, only the number of Ultimate Edition hosts is included here), the number of hosts with risks, the number of unprotected hosts, and the number of hosts whose authorization will expire soon.

Install CWP Client

Click Install CWP Client to show the installation guidance of the CWP client. Select the server type and operating system for correct installation. It can be integrated with overlay and underlay servers. After installation, verify if installed successfully.

Edition Upgrade

Click Upgrade Version to navigate to Authorization Management page. You can bind an Ultimate Edition license to a basic edition host to enable Ultimate Edition protection.

Filter and Export

- Supports filtering by server area, region, host status (all hosts, risk host, flagship edition or professional edition host, basic edition host, no client installed, offline, shut down), tag, and server IP or name search. the export button to export data from currently filtered machines.

List Operations

- Supports setting tags and associated tags.
- Supports uninstalling the CWP client and authorization management. Click Authorization Management to navigate to the authorization management page. Supports operations such as authorized binding, unbinding, and scale-out.
- Click the numeric value of intrusion detection, vulnerability risk, and baseline risk to redirect to view risk details.

Asset Fingerprint

This document describes how to view asset fingerprint statistics.

Overview

Asset fingerprint data collection can help you quickly understand the overview and operating status of your assets.

Use Limits

Only hosts of the Professional Edition or Ultimate Edition can collect asset fingerprint data.
The asset fingerprints supported by each edition are as follows:

CWP Protection Version	Collected Asset Fingerprint Item
Professional Edition	Ten Items: resource monitoring, account, port, process, software application, database, web application, web service, web framework, website
Flagship edition	16. Resource monitoring, account, port, process, software application, database, Web application, Web service, Web framework, Web site, Jar package, startup service, scheduled task, environment variable, kernel module

> Note:
>
> Asset fingerprint data is automatically collected every 8 hours and manual collection is supported.

Operation Steps

1. Log in to the CWPP tenant-side console. In the left sidebar, select Asset Management > Asset Fingerprint.
2. In Asset Fingerprint, the asset fingerprint classification list is displayed, including each asset fingerprint item and the number of corresponding servers. After selecting an item in the asset fingerprint classification list on the left, fingerprint details will be displayed on the right. The query and export of fingerprint data are supported.

   > Note:
   >
   > All asset fingerprint search features support fuzzy search.

Asset Fingerprint Classification Description:

- Resource monitoring: Collect data on server CPU load, memory usage, and disk usage.
- Account: Collect all accounts on the server.
- Port: Collect all used ports on the server.
- Process: Collect all running processes of the server.
- Software application: Collect all software applications running on the server.
- Database: Collect data from all databases running on the server.
- Web application: Collect all web applications running on the server.
- Web service: Collect all web services running on the server.
- Web framework: Collect web frameworks of all applications on the server.
- Deployed website: Collect all deployed websites on the server.
- Jar package: Collect all Jar packages on the server.
- Startup service: Collect all startup services of the server.
- Scheduled tasks: Collect all scheduled tasks of the server.
- Environment variable: Collect all environment variables on the server.
- Kernel module: Collect all kernel modules on the server.

File Detection

This document will guide you on how to operate and process Trojan files in the CWP console.

File Scan Settings

1. Log in to the CWPP tenant-side console. In the left sidebar, select Intrusion Detection > Malicious File Scan.
2. In malicious file scan, click Detection Setting in the upper right corner. The detection setting page pops up on the right. Scanning mode can be set.

   > Note:
   >
   > - The following two are common Trojan file detections:
   >   - Webshell detection: Provide detection of common Web script Trojan backdoors, including scripting languages such as ASP/PHP/JSP/Python.
   >   - Binary detection: Provides virus and Trojan detection for binary executable files, such as DDoS trojans, remote control software, mining software, etc. File types include exe, dll, bin, etc., and alarm users.

3. In Detection Setting, scheduled scan, real-time monitoring and automatic isolation settings are supported.

- Scheduled scan: click to enable Scheduled detection, set the detection mode, cycle and range, and then click Save to regularly scan host Trojan virus files and enhance security. Field Description:
  - Detection mode: includes quick detection mode and full-disk detection mode, which can detect running processes, critical directories, driver loading, etc. Among them, the duration of full-disk detection is related to the number of server disk files. It is recommended to choose more than 4 hours to avoid incomplete scanning or timeout.
  - Detection cycle: available every day, every 3 days or every 7 days.
  - Detection range: support selecting all Ultimate Edition servers, selected servers.
- Real-time monitoring: click to enable Real-time Monitoring, select the monitoring mode, and then click Save to monitor Web directories and key system directories in real time and detect and kill Trojan virus files. Field Description:
  - Monitoring mode
    - Standard: monitor and scan to detect incremental files in common directories.
    - Depth: monitor and scan to detect incremental files in all directories.
- Automatic isolation: click to enable Automatic isolation > Save, and detected malicious files will be automatically isolated. Manual confirmation of isolation is still required for some malicious files. It is

recommended to check all security events in the file detection list and ensure all processed.

> Note:
>
> If a file is misisolated, please restore it in the isolated list. Turning on or off automatic isolation requires configuration, and there is a several minutes delay before taking effect.

Inspection Setup Overview

1. Log in to the CWPP tenant console. In the left sidebar, select Intrusion Detection > Malicious File Scan.
2. On the file detection page, click one-click detection to start setting manual detection mode.
3. In the one-click detection setting pop-up window, after confirming the detection mode, engine mode, and host range, you can also configure the timeout period (detection may result in longer execution time due to too many files or directories).
4. After clicking Start Detection, detection will be carried out according to the detection settings. Click View Detail to view detection details.
   List field description for detection details
   - Affect the server: the IP and name of the server.
   - Operating system: the operating system of the server.
   - Detection status: detection complete, detecting, detection failure (reason: might be detection timeout failure. It is recommended to increase timeout and recheck; might be client offline. It is recommended to restart or reinstall the client and recheck).
   - Pending risks: the number of pending risk files detected on the server.
   - Detection start time: the start time of this detection.
   - Detection end time: the time when server detection is complete.
   - Perform operations
     - Recheck: If you want to recheck a server whose detection status is detection completed, detection stopped, or detection failure, you can click Recheck.
     - Stop the detection: If you want to stop detecting a server whose detection status is in detection, you can click Stop the detection. The server will not be detected. Operate with caution due to possible risks.
   - View detail: If you want to view the detection result of the target server, you can click View detail.

View Alarm List

1. Log in to the CWPP tenant console. In the left sidebar, select Intrusion Detection > Malicious File Scan.

2. On the file detection page, you can view the detection status of Trojan files in the currently protected servers, as shown in the figure below: List field description for Alarm List
    - Host name/instance ID: the server name and instance ID under detection.
    - IP address: the server IP address under detection.
    - Path: Risk file path.
    - Virus name/detection engine: The virus name of the intrusion risk file.
    - First detected time: the time when this risk file was first detected.
    - Latest detection time: the latest time when this risk file was detected.
    - Processing status: the processing status of the risk file. For events in the pending status, a prompt will display the existence of files and processes during the most recent detection of this file.
    - Perform operations
        - Details: view malicious file details.
        - Isolate: isolate this virus file to prevent hackers from starting it again, making it convenient for you to locate the virus file and scan and disinfect it. (Note: on a windows system, if the file is running, isolation will fail.) Support isolating and terminating related processes of this file. Recommend checking.
        - Mark as processed: It is recommended that you handle the issue by referring to the "Repair advice" in the alarm details. After processing, you can mark the alarm as processed.
        - Add to allowlist: If you confirm that the process execution is normal behavior, you can add the process to the whitelist exemption rules. Subsequently, when this process runs again, it will be directly released without interception or Alarm.
        - Ignore: Only ignore this alarm. If the same situation occurs again, an alarm will still be triggered.
        - Delete a record: Delete this alarm record. The console will no longer display it. Deleted records cannot be restored. Proceed with caution.

FAQs

Why Does a Trojan File Fail to Be Isolated?

Failure to isolate Trojan files is generally caused by Trojan files fighting against security software. It is recommended to delete the alarm file in the server first. If the issue still cannot be resolved, please contact us for processing. For Windows systems, you can also try using PC manager to scan and disinfect.

Next Steps

- Linux intrusion issue troubleshooting guide.
- Windows intrusion issue troubleshooting guide.

Abnormal Log-in

This document describes the functions and operations related to abnormal log-in.

Overview

When a server log-in behavior that does not meet the allowlist condition (common source IP, common username, common log-in location, common log-in time) is detected, an abnormal log-in alarm will be generated. If the source IP of the abnormal log-in is from an overseas IP (including Hong Kong, Macao, and Taiwan) or a malicious IP in threat intelligence, it will be marked as High Risk. Otherwise, it will be marked as Suspicious.

Restriction Description

- Hosts with the CWP client installed (client online) will monitor abnormal log-in behaviors in real time.
- The CWP console only retains abnormal log-in events in the last 6 months, and expired event data will no longer be displayed.

Operation Guide

1. Log in to the tenant-side console of CWPP.
2. In the left sidebar, select Intrusion Detection > Abnormal Login. Each function is described as follows.

Alarm List

On the alert list page, you can view and process abnormal login risks detected by CWPP.

Field Description:

- Host name/instance ID: the server that has been abnormally logged in.
- IP address: the server IP address that has been abnormally logged in.
- Source IP address: login source IP, generally company network egress IP or network proxy IP.
- Origin: the region of the login source IP.
- Login username: the login username used when successfully logging in to the server.
- Log-in time: the time of successful log-in to the server (time zone time on the server).
- Danger level: suspicious/high risk.
- status
    - Abnormal login: This log-in involves an abnormal region, abnormal username, abnormal login

time, or source IP address login.
    - Allowlisted: The login source IP has been added to the allowlist (a combination of login source IP, login username, login time, common login location, and effective scope constitutes the allowlist determination rules).
    - Processed: The user has manually processed and marked the event as processed.
    - Ignored: User has ignored this alarm event.
- Perform operations
    - Handle
        - Mark as processed: If you have manually processed this risk event, you can mark the event as processed.
        - Add to allowlist: After the add to allowlist operation, no Alarm will be triggered when the same event occurs again. Proceed with caution.
        - Ignore: Only ignore this alarm event. Alarm will still be triggered for the same event.
        - Delete a record: Delete the event record. The console will no longer display it. Deleted records cannot be restored. Proceed with caution.

Allowlist Management

On the allowlist management page, you can add/delete/modify/search for the allowlist of abnormal log-ins.
Field Description:

- Server IP/name: The server where the allowlist is effective.
- Source IP: allowlisted log-in source IP.
- Common login location: The login location added to the allowlist.
- Login username: allowlisted username.
- Log-in time: allowlisted log-in time period.
- Creation time: The creation time of this allowlist.
- Modification time: The last time the allowlist was modified.
- Perform operations
    - Edit: You can re-edit the login source IP, login username, login time, common log-in location, effective scope, etc.
    - Delete: You can perform deletion operations on the allowlist.

FAQs

How to Handle after Receiving an Abnormal Login Alert?

Determine whether the log-in behavior is your operation.

- If it is your own login behavior and you don't want to see the Alarm anymore, click Handle and select

Add to Allowlist. Configure the common log-in source IP, login username, login location, login time, and effective scope.

Log-in source IP is empty: It means that no alarm will be generated when IPs from all sources log in to the server.
Log-in username is empty: It means that no alarm will be generated when any username logs in to the server.
Log-in location is empty: It means no alarm will be generated regardless of the log-in location.
Log-in time is empty: It means no alarm will be generated regardless of the log-in time.

> Note:
>
> Login source IP, login username, login location and login time cannot be empty at the same time.

- If the login is not one's action, please change server log-in password immediately (suggested modification: a strong password of more than 10 characters, including uppercase and lowercase letters and special characters).
  If the server has been logged in abnormally, the logging-in user may have intruded on your server and left malicious files. It is recommended that you immediately perform file detection and elimination, vulnerability detection, and baseline detection to strengthen your server security.

How to Set Up the Allowlist to Meet the Needs of Most Users?

- Scenario 1: Log-in sources from a static IP range can use any username to log in to the server without generating abnormal log-in alarms.
  You can input the IP range in the login source IP and select the effective server range.
- Scenario 2: The log-in source IP is dynamically changing. To support IPs from Hong Kong (China) as the log-in location to log in to the server using any username at any time without generating abnormal log-in alarms.
  You can select Hong Kong Special Administrative Region in the common log-in location and select the effective server range.

  > Note:
  >
  > Login conditions support combination.

How to Turn Off Abnormal Log-In Alarms?

Please go to Settings Center > Alarm Settings to turn off the abnormal log-in alarm switch. If you keep the alarm switch on, it is recommended to tick the high-risk option to only trigger alarms for high-risk abnormal log-in behaviors.

Password Cracking

Host security password cracking, based on network security defense and host intrusion detection capabilities, provides real-time monitoring of password brute force cracking behavior for the host.

Operation Guide

View Password Cracking Events

Log in to the tenant-side console of CWPP. In the left sidebar, select Intrusion Detection > Password Cracking to open the password cracking page, where you can view the password cracking event list.

Field Description:

- Host name/Instance ID: server name and instance ID where the system has detected password cracking behavior.
- IP address: server IP address where the system has detected password cracking behavior.
- Source IP: attack source IP address.
- Origin: located area of the attack source IP.
- Protocol: the protocol used by attacker, including ssh/rdp.
- Login username: the login username used by the attacker.
- Port: the port used by the attacker to log in.
- First attack time: the time when CWPP first monitors password cracking behavior.
- Recent attack time: the most recent occurrence time of this event.
- Number of attempts: the count statistics of the number of attempts by the attack IP to crack the password.
- Cracking status: successful cracking, cracking failure.
- Blocking status: blocked, unblocked.
- Alarm status: pending processing, allowlisted, processed, ignored.
- Operation
    - Mark as processed: If you have manually handled the alarm, you can mark the alarm as processed.
    - Add to allowlist: Create a release policy for the domain name of the current alarm. When the identical attack occurs again, the alarm will no longer execute. Meanwhile, the current alarm status will change to "allowlisted".
    - Ignore: Only ignore this alarm. If the same situation occurs again, an alarm will still be triggered.
    - Delete a record: Delete this alarm record. The console will no longer display it. Deleted records cannot be restored. Proceed with caution.

Configure the Allowlist

After the allowlist is configured, password cracking from allowlisted source IPs will not be blocked or trigger alarms. The directions are as follows:

1. Log in to the tenant console of CWPP. In the left sidebar, select Intrusion Detection > Password Cracking. Open the password cracking page.
2. On the password cracking page, click Allowlist Management. Enter the allowlist management page.
3. On the allowlist management page, click Add to Allowlist. Open the allowlist creation page.
4. In the pop-up window on the right, fill in the source IP and effective scope.

> Note:
>
> After adding to the allowlist, the password cracking behavior from this source IP will not be blocked or trigger alarms. Proceed with caution. If a non-allowlisted source IP attempts to log in and hits the brute force cracking rules, the system will automatically issue an exception alarm or block.

Field Description:

- Source IP: Support filling in a single IP, IP range (such as 1.1.1.1-1.1.1.10) or IP segment (such as 1.1.1.0/24).
- Effective scope
  - All servers (choose carefully): Add trust to the allowlist condition for all servers under user AppID.
  - Custom server range: Self-define and add the server range that trusts the allowlist condition.
- Remarks: It is recommended that you enter relevant rule remarks.

Enable Alarm Notification

Log in to the tenant-side console of CWPP. In the left sidebar, select Settings Center > Alarm Settings. In the alarm settings, turn on the alarm notification switch. When a password cracking event occurs, you will be notified via the message center, SMS, email, WeCom, etc.

Guide for Handling Password Cracking Events

1. When the user receives a password cracking event alarm, log in to the tenant-side console of CWPP. In the left sidebar, select Intrusion Detection > Password Cracking. Open the password cracking page.
2. View the corresponding attack source IP in the alarm event list.

- If it is confirmed as a trusted source IP, in the operation column on the right side of the event, the user needs to click Handle > Add to Allowlist, and set allowlist conditions and effective scope (please add to allowlist with caution). After successful configuration, it is estimated to take effect within 5 minutes. Subsequently, password cracking behavior from this source IP will no longer be alarmed or blocked.
- If it is confirmed as an untrusted source IP, and the server password has been successfully cracked by the attacker.
  For servers that have been hacked following password cracking, you are recommended to immediately reset a complex password (a 12-16-digit complex password consisting of uppercase + lowercase + special characters + numbers) and check whether there are any unfamiliar accounts in the account list. If there are any unfamiliar accounts, delete or disable them and check for system exceptions.

Malicious Requests

this document guides you How to view and operate the malicious request alert list and policy configuration.

Background Information

The malicious request feature provides the ability to monitor and handle external request behaviors in real time, effectively identifying malicious request behaviors. If a host initiates a request to a malicious domain name, it will be identified and recorded. Upon detecting such malicious request behaviors, the system will provide you with real-time alerts.

Restriction Description

- Malicious request monitoring supports professional edition and flagship edition hosts.
- Malicious request interception only supports flagship edition hosts of Linux systems, and only supports blocking servers for DNS queries, not blocking traffic forwarding.

Alarm List

1. Log in to the tenant-side console of Cloud Workload Protection Platform. In the left sidebar, select Intrusion Detection > Malicious Request to enter the malicious request page.
2. On the malicious request page, the malicious request alert list can be viewed and related operations can be performed.

- Filter: Support by hit policy type, status, last request time, inputting the host name in the search box, instance ID, IP address, malicious request domain name.
- Process: mark as processed, add to allowlist, create blocking strategy, ignore, delete records.

Policy Configuration

Policy Management

Select Policy Configuration above the malicious request page to enter the policy configuration page.

- Filter: Support by policy type, execution action, effective status, keywords filtering.

  > Note:

- System policies are built-in policies. Support switch, but not support adding, editing, or deleting.
- It is recommended to keep system policies (standard) enabled. It is advisable to enable system policies (critical maintenance period) on demand during the critical maintenance period.
- In user-defined policies, interception policies are only applicable to flagship hosts.

Local Privilege Escalation

This document describes how to view and handle the details of privilege escalation events and guides you on how to create an allowlist to set the allowed privilege escalation behaviors.

Background Information

If someone enters the system with low privileges and uses certain means to elevate privileges to obtain high privileges, it is very likely an attack by a hacker, which will endanger the security of the host. The local privilege escalation feature can monitor privilege escalation events on your cloud virtual machine in real time and can view and handle privilege escalation event details. It also supports the allowlist creation feature for setting allowed privilege escalation behaviors.

Operation Steps

Alarm List

1. Log in to the tenant-side console of CWPP. In the left sidebar, select Intrusion Detection > Local Privilege Escalation to enter the event list tab of local privilege escalation.
2. On the event list tab of local privilege escalation, you can view the list of local privilege escalation events and perform related operations.
   On the alarm list tab, you can view information such as the hostname/instance ID, IP address, elevated user, parent process, parent process user, discovery time, and status of the host where the privilege escalation event occurred. The list display fields are customizable.
   - Filter event: The local privilege escalation event list supports selecting a date to view corresponding events, supports querying events by keyword and tag (multiple keywords are separated by the vertical bar "|", and multiple filter tags are separated by the Enter key), and simultaneously supports filtering events by status.
   - Customize list fields: Above the local privilege escalation alarm list, click the setting icon to set the list display field. After completing the selection, click Confirm to complete the setting.
   - Event export: Above the local privilege escalation alarm listto export the local privilege escalation alarm list.
   - Detailed information: In the right operation column of local privilege escalation event, click Details to view local privilege escalation event details.
     - Mark as processed: If you have manually processed the alarm, you can mark the alarm as processed.
     - Add to allowlist: Add the privilege escalation process of the current alarm server to the

allowlist. Subsequently, no alarms will be generated when the same privilege escalation behavior is detected again.

- Ignore: Only ignore this alarm. If the same situation occurs, an alarm will still be triggered.
- Delete a record: Delete the alarm record. The console will no longer display it. Deleted records cannot be restored. Proceed with caution.

Allowlist Management

The local privilege escalation feature supports adding an allowlist. By setting allowlist privilege escalation conditions, events that meet the conditions are marked as part of the allowlist.

1. Log in to the tenant-side console of CWPP. In the left sidebar, select Intrusion Detection > Local Privilege Escalation to open the Local Privilege Escalation page.

2. On the Local Privilege Escalation page, select Allowlist Management > Add Allowlist.

3. In the pop-up window for adding to allowlist, set privilege escalation conditions, including: processes with S permissions, custom privilege escalation process (support multiple process names, separated by commas, for example, 123.exe,test.exe), and at the same time select the server range covered by the condition, click OK.

   > Note:
   >
   > - s permission: grant file permissions of the file owner during the execution phase, equivalent to temporarily assuming the identity of the file owner.
   > - When ticking two conditions, they need to be satisfied simultaneously to hit allowlist.
   > - If the server range is set to all servers, trust will be added to all servers under the user's APPID for this allowlist condition. Proceed with caution.

4. After the settings are completed, you can view the condition in the allowlist management list. Events in the alarm list that meet the condition will be marked as allowlist events.

5. On the allowlist management page, you can perform filter and delete operations on the allowlist.

   - Filtering: The configured allowlist supports querying by keywords and tags (multiple keywords are separated by the vertical bar "|", and multiple filter tags are separated by the Enter key). It also supports filtering by whether S permissions are granted.
   - Customize list fields: Above the allowlist, you can set the list display field. After completing the selection, click Confirm to successfully set.
   - Edit: In the right operation column of the target allowlist, click Edit to edit the created allowlist.
   - Delete: In the allowlist, deletion of the configured allowlist is supported.

Rebound Shell

This document describes how to view and process the details of the rebound shell, and guide you how to create an allowlist to set the allowed reverse connection behavior.

Background Information

Reverse shell functionality is based on multidimensional and multiple methods to identify and record the Shell reverse connection behavior on the server, providing your Cloud Virtual Machine with real-time monitoring capabilities for the reverse shell behavior.

Operation Steps

Alarm List

1. Log in to the tenant console of Cloud Workload Protection Platform. In the left sidebar, select Intrusion Detection > Rebound Shell to enter the Rebound Shell Alarm List Page.
2. On the Rebound Shell Alarm List tab page, you can view the rebound shell event list and perform related operations.
   You can view the name of the host/instance ID, IP address, connection process, etc. where the reverse Shell occurred. The list display fields are customizable.
   - Filter: The Rebound Shell Alarm List supports selecting a date to view corresponding events, querying events by keyword and tag (multiple keywords are separated by the vertical bar "|", and multiple filter tags are separated by the Enter key), and filtering alarms by status (all, pending, and confirmed).
   - Customize list fields: Above the Rebound Shell Alarm List to set the list display field. After completing the selection, click OK to successfully set.
   - Event export: Above the Rebound Shell Alarm List to export the Rebound Shell Alarm List.
   - Detailed information: In the right operation column of the target reverse Shell event, click Details to view the detailed information of the reverse Shell event.
     - Mark as processed: It is recommended that you manually handle the alarm by referring to the "Repair advice" in the alarm details. After handling, you can mark the alarm as processed.
     - Add to allowlist: After the add to allowlist operation, when the same situation occurs again, no Alarm will be triggered. Proceed with caution.
     - Ignore: Only ignore this Alarm. If the same situation occurs again, an alarm will still be triggered.

- Delete a record: Delete this alarm record. The console will no longer display it. Deleted records cannot be restored. Proceed with caution.

Allowlist Management

Rebound Shell supports adding allowlists. By setting allowlist conditions, events that meet the conditions are marked as allowlisted.

1. Log in to the tenant console of CWPP. In the left sidebar, select Intrusion Detection > Rebound Shell to enter the Rebound Shell page.
2. On the Rebound Shell page, select Allowlist Management > Add Allowlist.
3. In the Add Allowlist pop-up window, set the rebound Shell conditions, including: destination host, custom connection process (support multiple process names, separated by commas). At the same time, select the server range covered by the condition and click confirm.
   Field Description:
   - IP address format: single IP (127.0.0.1), IP range (127.0.0.1-127.0.0.254), IP network segment (127.0.0.1/24).
   - Port format: 80,8080 (separated by commas for multiple ports. Leave blank for no port limit).
   - Tick two conditions. They need to be satisfied simultaneously to hit allowlist.
   - If the server scope is set to all servers, add trust to all servers under the user's APPID for this allowlist condition. Proceed with caution.
4. After the settings are completed, you can view the condition in the allowlist management list. Events that meet the condition in the alarm list will be marked as allowlist events.
5. On the allowlist management page, you can perform filter and delete operations on the allowlist.
   - Filtering: The configured allowlist supports querying by keyword and tag (multiple keywords are separated by the vertical bar "|", and multiple filter tags are separated by the Enter key).
   - Customize list fields: Above the allowlist to set the list display field. After completing the selection, click OK to successfully set.
   - Edit: In the right operation column of the target allowlist, click Edit to edit the created allowlist.
   - Deletion: In the allowlist, deletion of the configured allowlist is supported.

High-risk Commands

This document will introduce you how to view and operate the list of high-risk command events.

Background Information

Based on multi-dimensional and multi-method means, CWP can monitor commands in the system in real time, and classify the degree of danger of commands by configuring rules. If a high-risk command is detected, the system will provide you with real-time alarm notification.

Operation Steps

Alarm List

1. Log in to the CWPP tenant-side console. In the left sidebar, select Intrusion Detection > High-risk Command to enter the alarm list tag page of high-risk commands.
2. On the alarm list tag page of high-risk commands, you can view the high-risk command alarm list and perform related operations. On the alarm list interface, information such as the hostname/ instance ID, IP address, hit policy type, hit policy, and threat level of the host with a high-risk command alarm can be shown. The list display fields can be customized.
    - Filter: The high-risk command alert list supports selecting a date to view, supports querying events by keyword and tag (multiple keywords are separated by the vertical bar "|", and multiple filter tags are separated by the Enter key), and simultaneously supports filtering events by threat level and status.
    - Customize list fields: Above the list of high-risk command events to set the list display field. After completing the selection, click OK to successfully set.
    - Event list export: Above the high-risk command alert list to export the high-risk command alert list.
    - Detailed information: Click Detailed Information to view high-risk command alarm details and process tree information.
        - Mark as processed: It is recommended that you manually handle this alarm by referring to the "Repair Advice" in the alarm details. After handling, you can mark the alarm as processed.
        - Add to allowlist: Create a release policy for the domain name of the current alarm. When the identical attack occurs again, no alarm will be triggered. Meanwhile, the current alarm status will change to "Added to allowlist".
        - Create a blocking strategy: Create a blocking strategy for the domain name of the current

alarm, and automatic interception will be performed when the identical attack occurs again.
- Ignore: Only ignore this alarm. If the same situation occurs again, an alarm will still be triggered.
- Delete a record: Delete this alarm record. The console will no longer display it. Deleted records cannot be restored. Proceed with caution.

Policy Configuration

Creating Custom Policy

The high-risk command feature supports creating custom policies to perform corresponding actions on threat commands by setting policies.

1. Log in to the CWPP tenant console. Select Intrusion Detection > High-risk Commands in the left sidebar to enter the high-risk commands page.
2. Select Policy Settings > Create a Policy to enter the create policy page.
3. On the create policy page, fill in the basic information of the policy, including the Policy Name, policy description and enable status.
4. Fill in the policy details, including selecting the blocklist/allowlist and the corresponding execution action, filling in the regular expression, selecting the threat level, and selecting the effective host range.

   - Blocklist rule: An alarm notification will be generated when a threat command is detected on a host.

     > Description
     >
     > - The interception policy refers to automatically intercepting the execution of threat commands when a threat command is detected on the host and sending alarm notifications.
     > - The interception policy is only supported on flagship edition machines.

   - Allowlist rule: It refers to allowing threat commands to pass through, with no alarm reported or blocking behavior performed.

     > Description

> - If all Ultimate Edition hosts are selected as the effective host range, newly-added Ultimate Edition hosts will automatically be included in the policy effective range.
> - You can check to execute the operation of this policy rule for the historic "Pending" Alarms that

> comply with this policy rule.

5. After the settings are completed, you can view them in the policy list. Policies applied to the blocklist in the list will be marked with the corresponding threat level.
6. Policies in the policy list can be filtered, edited, and deleted.
    - Filter: Configured policies support filtering by keyword and tag (multiple keywords are separated by the vertical bar "|", and multiple filter tags are separated by the Enter key). Filtering is supported by threat level (all/high risk/medium risk/low risk/none), by execution action (alarm/block/pass), and by effective status (effective/not applied).
    - Customize list fields: Above the policy list to set the list display field. After completing the selection, click OK to successfully set.
    - Enable status: The list supports setting the enable status of policies. In the enable status column, click Enable switch to determine whether to enable this policy.
    - Edit: In the right operation column of the policy list, click Edit to proceed with editing the created policy.
    - Delete: In the policy list, deletion of configured policies is supported.

System Policy

The high-risk command function adds new system auto interception rules. Once enabled, it supports automatically intercepting detected high-risk system commands. Partial content still requires you to manually configure policies.

- High-risk system commands: High-risk system commands accumulated by host security operation experts and algorithm experts. High-risk commands in this list can be automatically blocked.
- Interception principle explanation: For high-risk command auto-blocking, it uses the way of scanning and killing processes that hit the rules. For example, if process A attempts to create a "/bin/bash -i" process (assuming "bash -i" has been added to the blocklist), then this attempted "/bin/bash" process will be terminated (or creation failed), while process A itself will not be affected.

  > Note:
  >
  > - If you detect a false positive blocking scenario, you can create a custom policy for allowlist processing.
  > - System auto interception rules are only for use on flagship edition hosts.

Network Attack

Network attacks, supported by the security attack and defense team's technical support, automatically monitor malicious traffic for you. Combined with malicious behaviors generated during the intrusion process, real-time automated correlation analysis is performed on attacks and alarms, outputting attack traffic data and notifying attack events. This document guides you on how to view and handle network attack alerts.

Restriction Description

- Detection object: Only supported on Linux hosts of the pro edition/flagship edition.
- Detection range: Only detects hotspot vulnerability attack behaviors that partially occur with EXP and have successful attack cases in the cloud.
- Vulnerability defense: Only supported on Linux hosts of the flagship edition.

Defense Status Description

- Supported vulnerability defense (not enabled): Host security supports defending against this vulnerability, but this host has not enabled defense for it.
- Supported vulnerability defense (enabled): Host security supports defending against this vulnerability, and this host has enabled defense for it.
- Vulnerability defense not supported yet: Host security does not support defending against this vulnerability.

  > Note:
  >
  > - Possible reasons for not enabling vulnerability defense: The defense switch is not enabled, the host is a non-flagship edition, or the host is not in the protection host range.
  > - Attack events indicate that there are currently hackers exploiting this vulnerability's attack techniques, but it does not mean that this vulnerability exists on the current machine.

Alert Statistics

1. Log in to the CWPP tenant-side console. In the left sidebar, select Intrusion defense > Network attack.
2. On the Network Attack Page, support viewing the vulnerability defense status in network attacks, statistics of pending alert-related data, and the Top 5 situations. Field Description:

- Vulnerability defense status: Reflect the status of the vulnerability defense switch.
- Pending network alerts: The current alarm count to be processed.
- Number of attacked assets: The number of attacked assets involved in the current pending alarms.
- Number of attacked ports: The number of attacked ports involved in the current pending alarms.
- Number of attack source IPs: The number of attack source IPs in the current pending alarms.

View Alarms

On the Network Attack Page, support viewing network attack details, including hostname, instance ID, IP, destination port, etc.

Field Description:

- Hostname/Instance ID: The hostname and instance ID of the affected host.
- IP: The public network/private network IP of the attack host.
- Destination port: Attacked port.
- Source IP/address of the attack: The source IP and location of the attacker.
- Vulnerability name: Refers to the attack technique used by the attacker to exploit a certain vulnerability, as well as the current status of the vulnerability defense.
- Attack status: Refers to the result of an attacker's attack, attempted attack (attacked but not successfully attacked), successful attack (confirmed attack).
- Last attack time: The time when the latest attack behavior was detected.
- Number of attacks: Cumulative number of identical attacks detected.
- Processing status: Pending, Processed, Whitelisted, Ignored.
- Details: Support viewing alarm details, severity description, solution.

Handling Alerts

1. In the list of network attack alerts, click Handle in the Action column.

   > Note:
   >
   > Select one or more Alarms, and you can click Mark as processed, Ignore, or Delete records in the upper left corner to perform batch operations.

2. Support marking pending alerts as processed, enabling vulnerability defense, adding to allowlist, ignoring, and deleting records.
   - Mark as processed: Manually handle the alarm and mark it as "processed" after processing.
   - Add to allowlist: Add the attack source IP to the allowlist. Subsequently, CWPP will no longer trigger an alarm for the cyber attack behavior of this source IP. Proceed with caution.

- Ignore: Only ignore this alarm. If the same situation occurs again, an alarm will still be triggered.
- Delete a record: Delete this alarm record. The console will no longer display it. Deleted records cannot be restored. Proceed with caution.

Java Memory Trojan

Overview

Host security (CWP) supports real-time monitoring, capturing unknown classes in the memory of Java Web service processes. Combined with security attack and defense experience and expert knowledge, it can automatically identify memory trojans. If a Java memory Trojan is detected, the system will provide you with real-time alarm notification.

Operation Steps

1. Log in to the CWPP tenant-side console. In the left sidebar, select Intrusion Defense > Java Memory Horse to open the Java Memory Horse page.
2. Select Plug-in Configuration. Plug-in configuration is a prerequisite for monitoring Java memory Trojans. You can turn the plug-in on and off for flagship hosts and observe the specific running status of the plug-in.

> Note:
>
> - After enabling the Java Memory Trojan plugin, CWPP will automatically detect the Java Web service process on the host and inject a detection probe into the service process to monitor in real time the Java Memory Trojan injected by hackers through vulnerabilities, Shell, etc.
> - Hosts injected with Java memory Trojan plugins will monitor in real time and capture unknown classes in the memory of Java Web service processes. Combining security attack and defense experience and expert knowledge, they can automatically identify memory trojans. If a Java memory Trojan is detected, the system will provide you with real-time alarm notifications.

<Field Description:

- Enable/disable the plugin: Java Memory Horse Plugin is off by default. It supports users to manually set the switch. It can be set for a single host or in batch for multiple selected hosts.
- Plug-in status: all normal, existence of anomalies, not enabled.
- Initial start time: the time when the plug-in is enabled for the first time.
- Update time: the time when the plug-in was recently enabled or disabled.
- Details: You can view the running state of the currently injected Java Memory Horse Plugin, including process PID, main class name of process, plug-in status (injecting, injection successful, plugin timed out, insertion and exit, injection failure), injection log.

After the Java Memory Trojan plugin is enabled, you can select the Alarm List to view detected Java Memory Trojan events and perform related processing operations.

Field Descriptions:

- Host name/instance ID: the host name and instance ID of the host where Java Memory Trojan has been detected.
- Host IP address where Java Memory Trojan has been detected.
- Memory trojan types of Java: including Filter type, Listener type, Servlet type, Interceptors type, Agent type, and other.
- Summary: summarize the general overview of Java Memory Trojan.
- First detected time: the time when this Java Memory Trojan was first detected.
- Latest detection time: the time when detection found this Java Memory Trojan still exists recently.
- Status: to be processed, processed, ignored.
- Operation
    - Click Details to view details of the memory Trojan event.
    - Click View Files in Memory Horse Details to view the decompiled Java file of the landing file. Copying is supported. Support downloading decompiled Java files or original Class files.
    - Click Handle to mark the event as processed, ignored, or delete the record. You can process events individually or select multiple events for batch processing.

Core File Monitoring

The monitoring rules of core file monitoring are divided into system rules and custom rules. The system rules are rule configurations accumulated through multi-models by host security operation experts and algorithm experts, which are applicable to most tamper monitoring requirements for user configuration. You can also customize rules according to business needs. Custom rules support editing, copying and deleting.

> Note:
>
> - Core file monitoring is a feature of CWP Ultimate Edition.
> - Core file monitoring currently supports operating systems with a Linux kernel version of 3.10 or higher.

Create Rule

1. Log in to the tenant-side console of CWPP. In the left sidebar, select Intrusion defense > Core file monitoring.
2. On the Monitoring rule configuration page, click Add Rule in the upper left corner. A new rule popup pops up on the right.
3. In the Add Rule pop-up window, sequentially configure basic setting, rule content settings and effective server range parameter.

    - Basic setting

      Field Description:

      - Rule Name: Custom name.
      - Threat level: You can choose high risk, medium risk, low risk or none according to actual needs.
      - Enable status: Enable or disable this new rule.

    - Rule content settings: click Add Rule, and you can add multiple rows, with a maximum of 20 rows.

      Field Description:

      - Monitoring behavior: modify files/read files.
      - Process file path: the path to process file that initiates the file tampering action. For example, for the program /usr/bin/vi, the corresponding rule can be */vi.

- File path: for example, /etc/cron.d/attack. The corresponding rule can be /etc/cron.d/*.
- Execution action: Alarm refers to generating an automatic alarm event for file system changes and recording event details; Allow operation refers to performing an allow operation on file system change events and recording event details.

> Note:
>
> When the alert bypass process path and the accessed file match, and there is an overlap in the effective servers, no alarm will be generated for the overlapping part of the servers (i.e., the release conditions take precedence).

- Effective host range: You can select all servers or selected servers according to actual needs.

4. After the configuration is complete, click Save just.

Manage Rules

Edit Rule

1. The newly added rules are shown in Core File Monitoring > Monitoring Rule Configuration. The operation list supports Copy, Edit, and Delete.

> Note:
>
> Once deleted, the rule cannot be restored. Proceed with caution.

Alarm List

The alarm list supports viewing core file anomaly alert records. Alarm records can be processed (marked as processed, added to allowlist, ignored), or deleted.

Handling Alarm Records

1. Log in to the tenant console of CWPP. In the left sidebar, select Intrusion Defense > Core File Monitoring.
2. On the Alarm List page, select the required alarm record, click Handle, and select Mark as Processed, Add to Allowlist, Ignore, or Delete Record. Field Descriptions:
   - Mark as processed: Manually handle the alarm and mark the alarm as processed after handling.
   - Add to allowlist: Add the current file path to the allowlist. Subsequently, no alarm will be reported for corresponding read/modify actions. Proceed with caution.
   - Ignore: Only ignore this alarm. If the same situation occurs again, an alarm will still be

triggered.

- Delete a record: Delete this alarm record. The console will no longer display it. Deleted records cannot be restored. Proceed with caution.

Deleting Alarm Records

1. On the Alarm List page, you can delete alarm records individually or in batches.
   - Each: Select the required alarm record, click Delete, and a confirm deletion dialog box pops up.
   - Batch: Select one or more alarm records, click Delete in the upper left corner, and a confirm deletion dialog box pops up.
2. In the confirm deletion dialog box, click OK to delete the selected alarm record.

> Note:
>
> Deleted alarm records will no longer be displayed on the console. Deleted records cannot be restored. Proceed with caution.

Vulnerability Management

Vulnerability management aims to help customers scan security vulnerabilities in the system and provide vulnerability information, repair suggestions, etc. Some vulnerabilities can enable precise defense and can be automatically repaired. This document guides you on how to perform vulnerability management.

Restriction Description

- Vulnerability management range description: the following

Vulnerability Management Feature	Vulnerability Type	Linux System	Windows Systems
Vulnerability Scanning Pro edition, flagship edition host applicable	Linux Software Vulnerabilities	✓	×
	Windows System Vulnerabilities	×	✓
	Web-CMS Vulnerabilities	✓	✓
	Application Vulnerabilities	✓	✓
Vulnerability Defense Flagship edition host applicable	Linux Software Vulnerabilities	×	×
	Windows System Vulnerabilities	×	×
	Web-CMS Vulnerabilities	Only support some vulnerabilities.	×
	Application Vulnerabilities	✓Only some vulnerabilities are supported.	×
Automatic Vulnerability Repair Flagship edition host applicable	Linux Software Vulnerabilities	✓ Only some vulnerabilities are supported.	×
	Windows System Vulnerabilities	×	×

Vulnerability Management Feature	Vulnerability Type	Linux System	Windows Systems
	Web-CMS Vulnerabilities	✓ Only some vulnerabilities are supported.	✓ Only some vulnerabilities are supported.
	Application Vulnerabilities	×	×

- Since vulnerability repair may disrupt user business, automatic vulnerability repair is not performed immediately after vulnerability detection. Users must understand the vulnerability, click Repair, and back up data before automated repair can be performed.

Vulnerability Scanning

1. Log in to the tenant-side console of Cloud Workload Protection Platform, and click Vulnerability Management in the left sidebar.
2. In the vulnerability scanning module, support one-click scan, scheduled scan settings.
    - Click One-Click Scan , and the one-click scan settings popup will open. You can configure the vulnerability type, vulnerability level, scan timeout duration, and scan server range for this scan.
    - Click Scan Setting to open the vulnerability settings pop-up and anchor to Scheduled Scan. You can configure the scheduled scan switch, period, vulnerability level, and vulnerability type.
    - Click Details to view the details of the last scan. PDF scan reports and Excel scan results are supported for download.

Vulnerability Defense

In the Vulnerability Defense module, you can enable/disable the vulnerability defense switch, view the number of protected hosts, the successful prevention count, and defense trends.

- Click Defense Setting to open the vulnerability settings pop-up and anchor to Vulnerability Defense. You can set the vulnerability defense switch, view protectable vulnerabilities, select the protection host range, and view the defense plugin details.
- Click Successful Prevention Count, and you can view the attacks that have been successfully defended against currently and view attack details.

Vulnerability Handling

1. Below the vulnerability management page, you can view the statistical data and detailed vulnerability list of the currently detected vulnerabilities.
2. In the [Vulnerability Overview] module, the vulnerability detection status, frequency of network attack events, and today's additions are displayed, as well as the total count of the host security vulnerability database. Field Descriptions:
    - The total number of all vulnerabilities: the number of detected Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities.
    - Number of affected hosts: the number of hosts where vulnerabilities are detected.
    - Network attack events: statistics of the number of network attack events within the last month.
    - Supported vulnerabilities: You can view the vulnerability database supported by CWPP for detection. You can perform up to 20 retrievals each day. A single search can show up to 100 results.
3. In the Vulnerability List module, show the current detected specific vulnerabilities, which are divided into two categories: Urgent Vulnerability and All Vulnerabilities. The functionality of the two is not very different. Below, take All Vulnerabilities as an example to introduce vulnerability handling. Field Descriptions:
    - Vulnerability name/tag: The vulnerability name refers to the currently detected vulnerability, and the tag refers to the tag of the vulnerability (such as RemoteExploit, service restart, exist EXP, etc.).
    - Vulnerability type: Linux software vulnerability, Windows system vulnerability, Web-CMS vulnerability, application vulnerability.
    - Threat level: critical, high risk, medium risk, low risk.
    - CVSS: Refers to the score of the common vulnerability scoring system. The score range is from 0 to 10. 0 represents the least severe, and 10 represents the most severe.
    - CVE No.: The unique number to identify the security vulnerability in the public vulnerability exposure database.
    - Last scan time: the time when this vulnerability was last detected.
    - Number of affected hosts: the number of hosts with this vulnerability.
    - Processing status: to be fixed, in remediation, scan in progress, fixed, ignored.
    - Defense status: defending.
    - Perform an operation
        - Repair plan: For vulnerabilities that cannot be fixed automatically, click Repair Plan to open the vulnerability details pop-up and manually fix vulnerabilities according to the repair plan.
        - Automatic fix: Some Linux software vulnerabilities and Web-CMS vulnerabilities support automatic fix. Click Automatic Fix to open the vulnerability details pop-up, select the servers that need to be repaired, and proceed with the necessary fixes.
        - More: Rescan (rescan this vulnerability); Ignore (ignore this vulnerability and do not scan the host for this vulnerability in the future).

Security Baseline

This document describes how to use the baseline management feature to help you manage baseline security in your server.

Background Information

The Cloud Workload Protection Platform (CWPP) supports periodic and one-click detection of baseline detection items, detection of specified baseline items on designated hosts, understanding baseline pass rates and risk situations through detection policies. It provides risk levels and repair suggestions for baselines and detection items, and provides default baseline policies, helping you better manage baseline security in your server.

Operation Guide

1. Log in to the tenant-side console of CWPP. In the left sidebar, select Baseline Management > Security Baseline to go to the Security Baseline page.
2. The Security Baseline page enables one to set baseline policies, detect periodically, and detect specified policies with one click. It supports viewing the pass rate and risk status of the baseline policy, as well as the list of baseline detection results. It also supports viewing the baseline and detection item details and repair plans and can ignore the detection items of specified servers.

Baseline Policy

The baseline policy is a collection of baseline detection items based on user-defined settings. It understands the pass rate and risk situation of the baseline based on the policy dimension.

- Cloud platform default baseline policy: Cloud platform host security provides you with a default baseline detection policy based on the mainstream baseline detection content of network security, including: International Standard Baseline, weak password, unauthorized access, level-2 cybersecurity classified protection, level-3 cybersecurity classified protection, and cloud security standard policy. You can add detection items to the default baseline policy and servers to be detected. This policy, by default, detects all Ultimate Edition or flagship edition servers at 00:00 on the 7th day every 7 days.
- Adding Baseline Policy

1. In the upper-right corner of the Security Baseline page, click Baseline Detection Setting.
2. In Detection Policy Settings, click Add Policy.
3. In the pop-up window for adding a policy, enter a policy name (cannot be the same as an existing

policy name), select a detection period, baseline options, and application assets, click Save and update.

> Note:
>
> CWP supports creating a maximum of 20 baseline policies. After the number of baseline policies reaches 20, you are not allowed to create more. However, you can delete the existing baseline and create another one.

Baseline Detection

CWPP supports periodic detection and one-click detection of baseline detection items, and supports the detection of specified baseline items on specified CVMs.

- One-Click Detection
  1.Click One-click Detection, select the baseline policy to detect and issue detection (the detection usually lasts 2 - 5 minutes). After the detection is completed, the detection results will be displayed at the bottom of the Security Baseline page.
- Periodic Detection

1. In the upper-right corner of the Security Baseline page, click Baseline Detection Setting.
2. In Detection Policy Settings, you can set periodic detection.

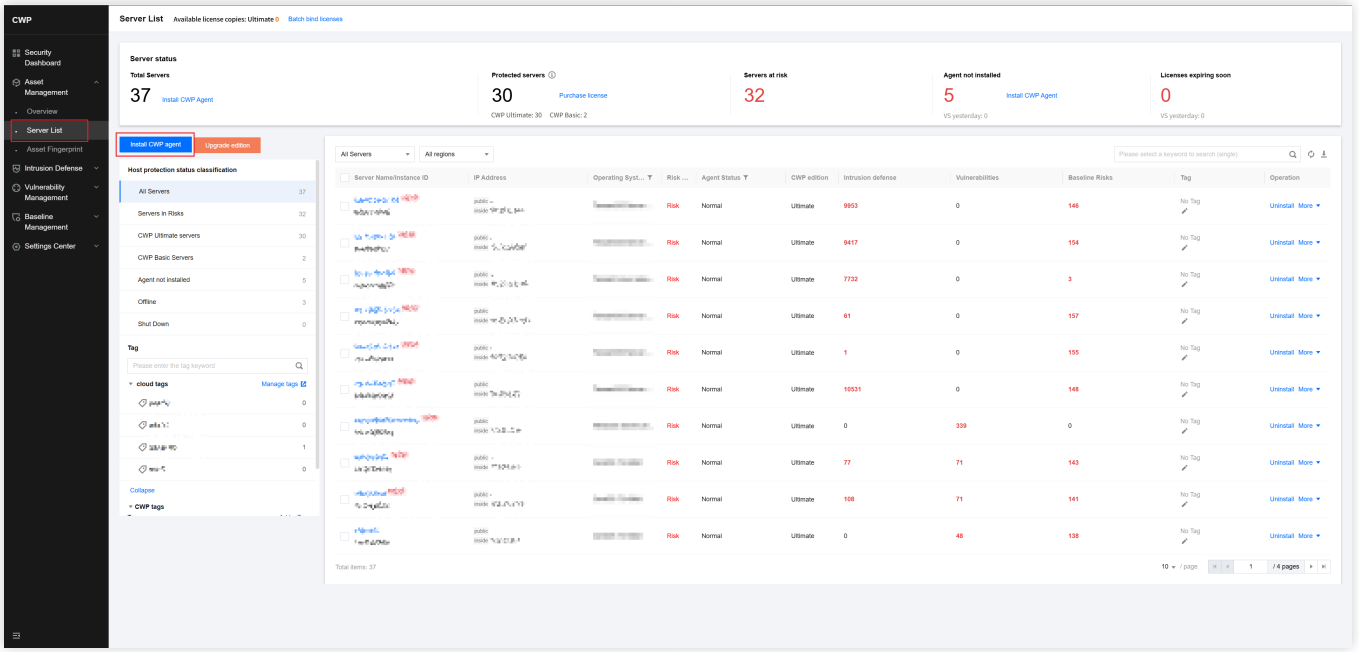
List of Baseline Detection Results

Below the Security Baseline page, you can view the list of baseline detection results, view baseline detection details, fuzzily search and filter the status of a single baseline, and download all tables.

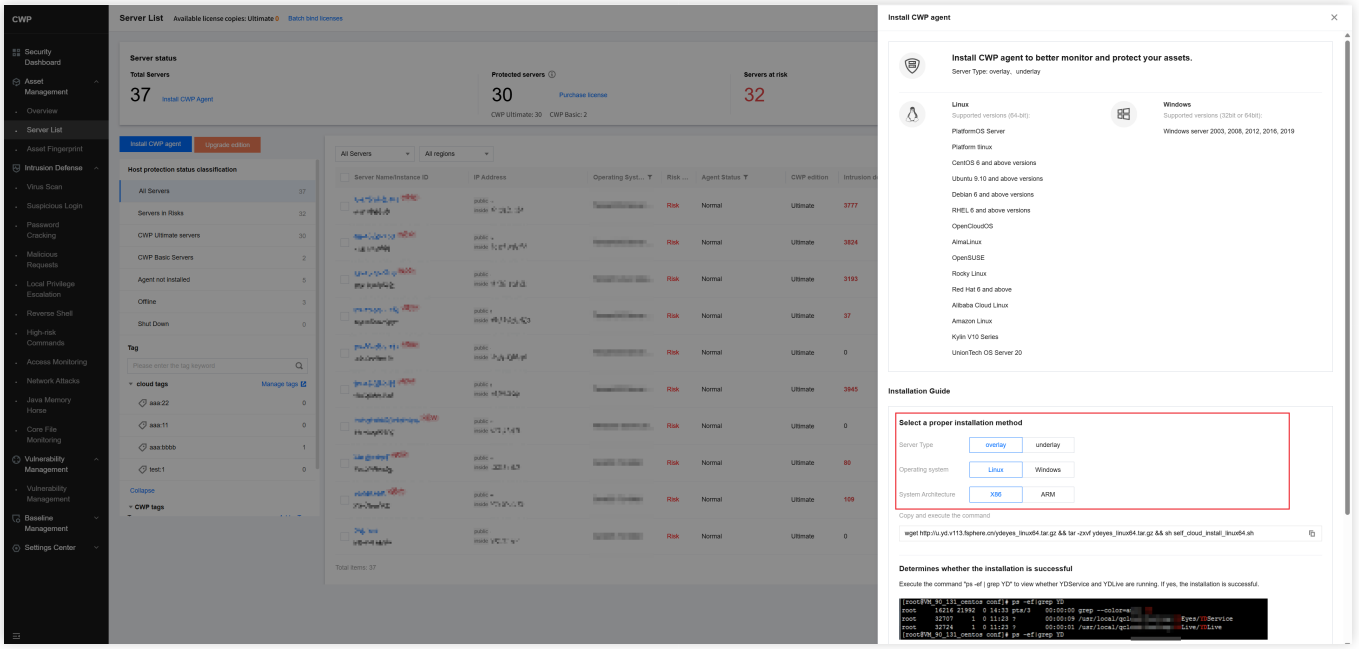
- Detection rule name: Baseline detection rule name, containing several detection items of the same category. - Specific detection item: Total number of detection items under this detection rule. - Number of detected servers: The number of servers detected by this detection rule. - Last detection time: The time when this detection rule was last detected. - Processing status: failed, approved. - Perform operations - Recheck: You can re-detect this detection rule. - View detail: server inspection results and associated detection items are viewable.

Common Operations
Installing an Agent on an Unprotected Host

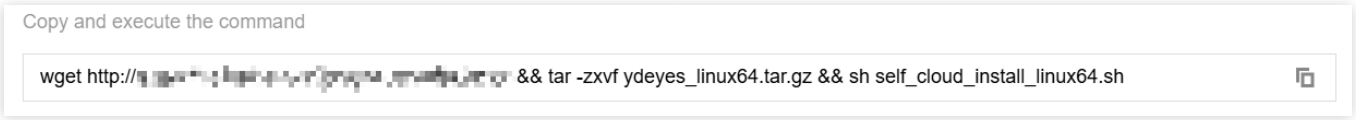
1. Log in to the CWP tenant console and choose Asset Management > Server List > Install CWP Client.



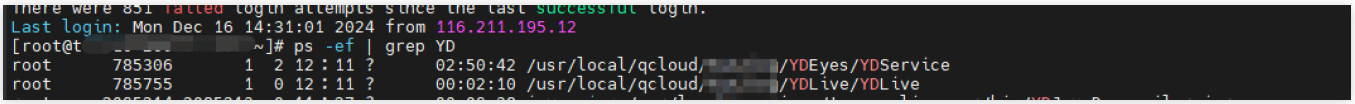
2.Select the appropriate installation link based on the architecture and type of the server.



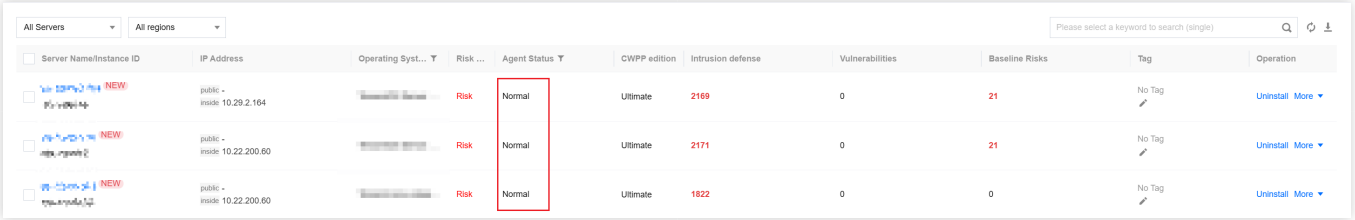
3.Copy the installation link of the CWP agent and execute it on the target server as a root user.



4.After execution, execute ps -ef | grep YD to check whether the CWP agent has started normally.

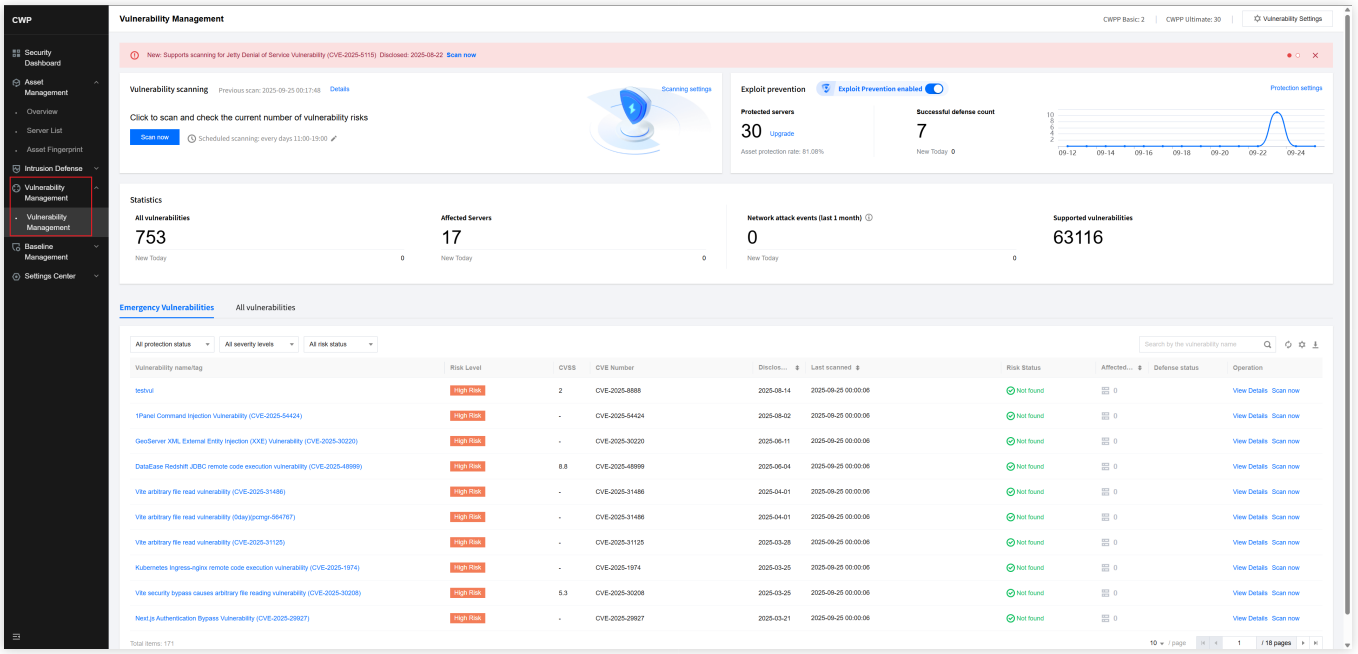


5.Once the server is connected, its status will display as Protected in the CWP console.

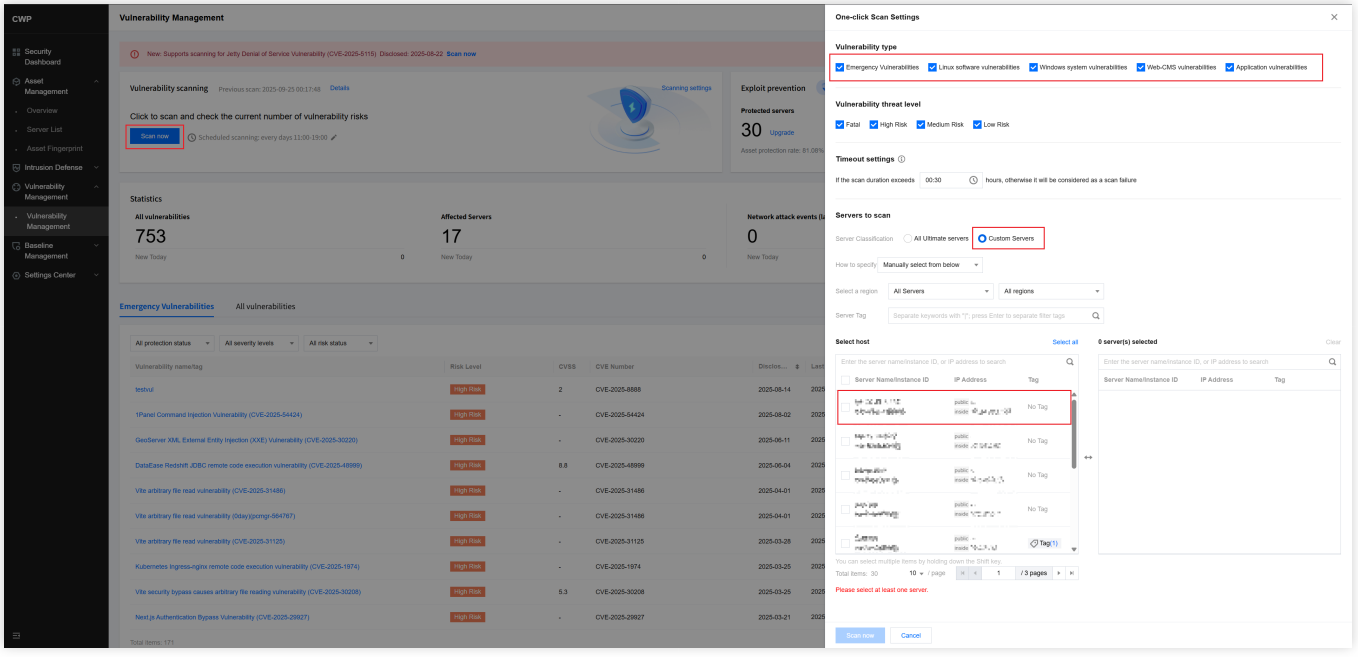


Vulnerability Scan for a Single Host

1. Log in to the CWP tenant console and go to Vulnerability Management > Vulnerability Management.



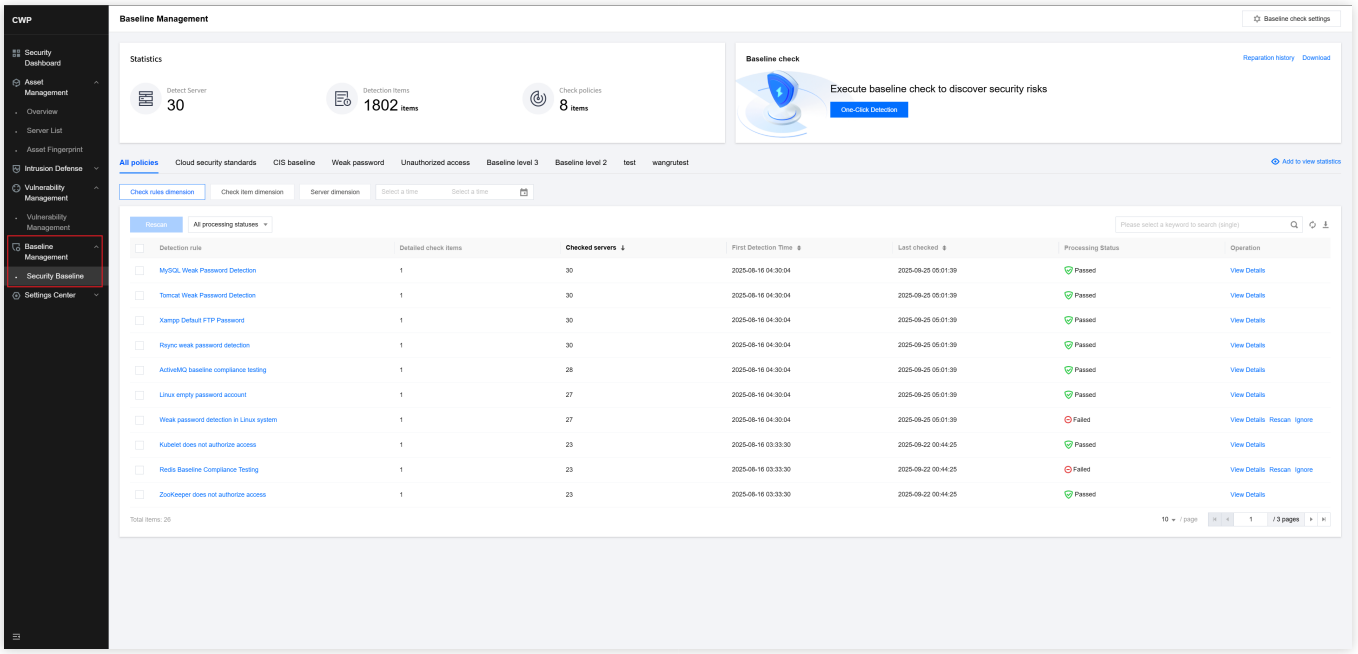
2. Click One-click Scan, select the types of vulnerabilities to scan, and select the target server.



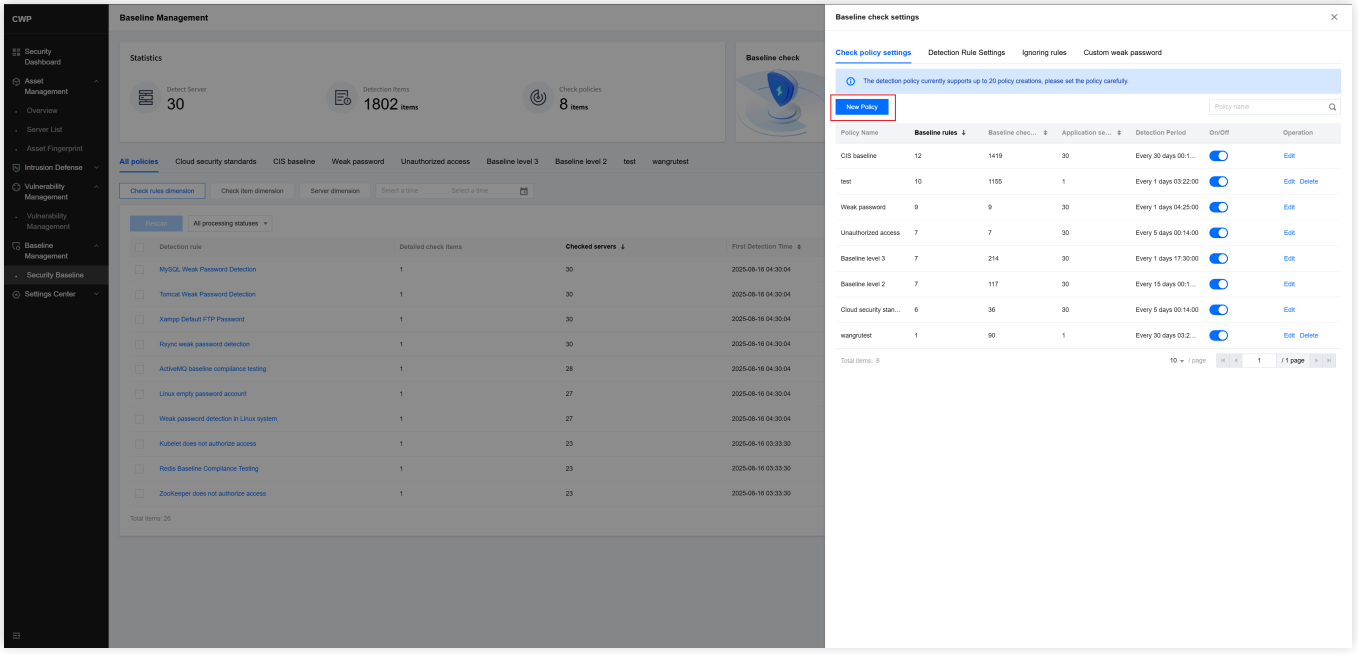
3. After completing all configurations, click One-click Scan at the bottom to start the vulnerability scan for the selected server.

Baseline Scan for a Single Host

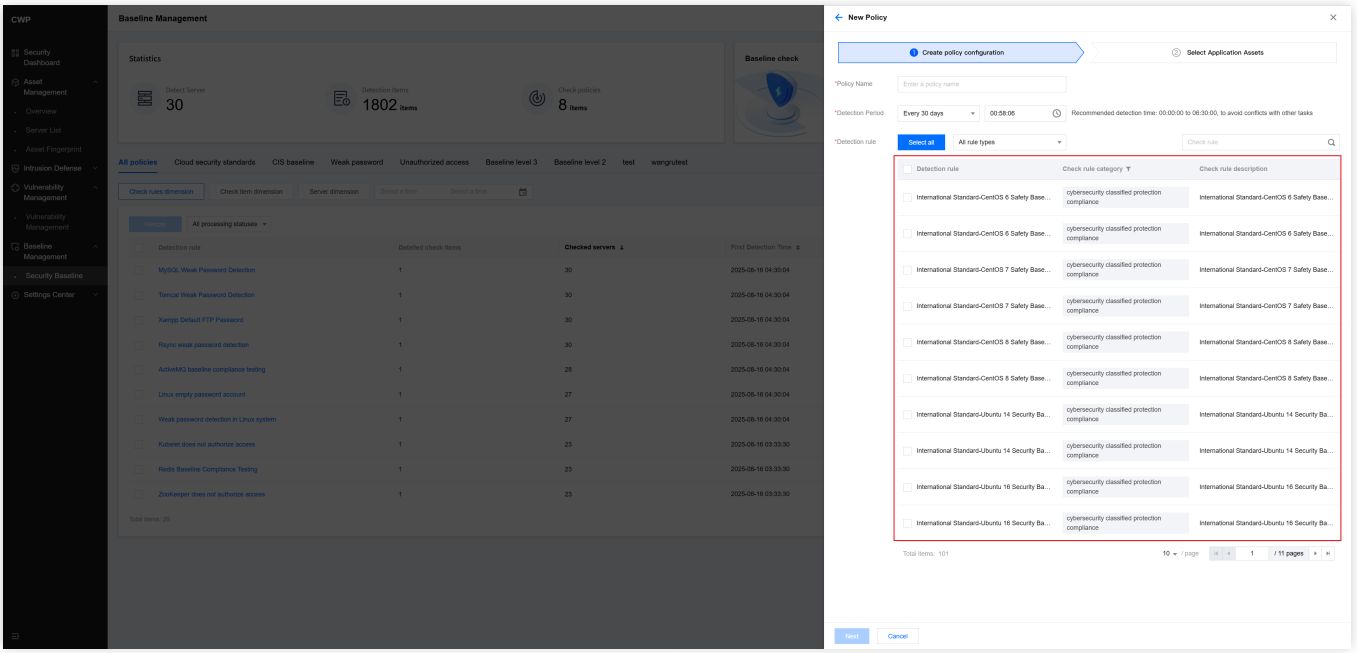
1. Log in to the CWP tenant console and go to Baseline Management > Security Baseline.



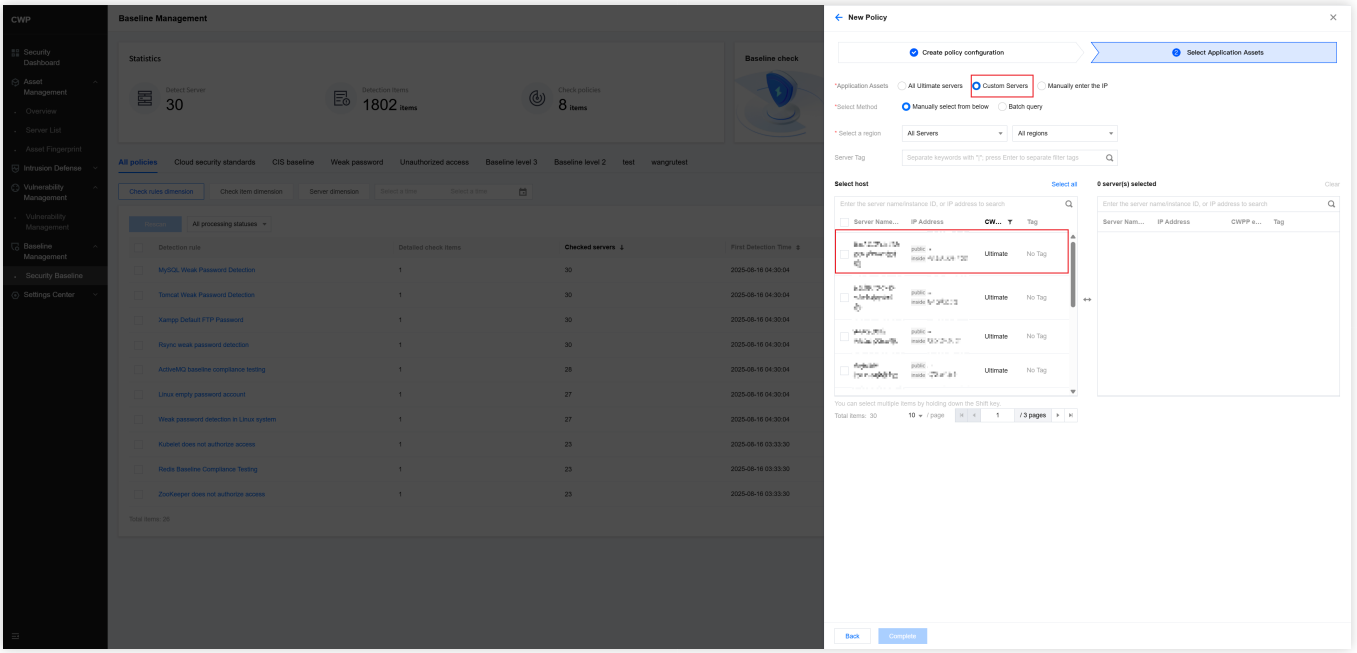
2. In the upper-right corner, click Baseline Detection Setting > Create New Policy.



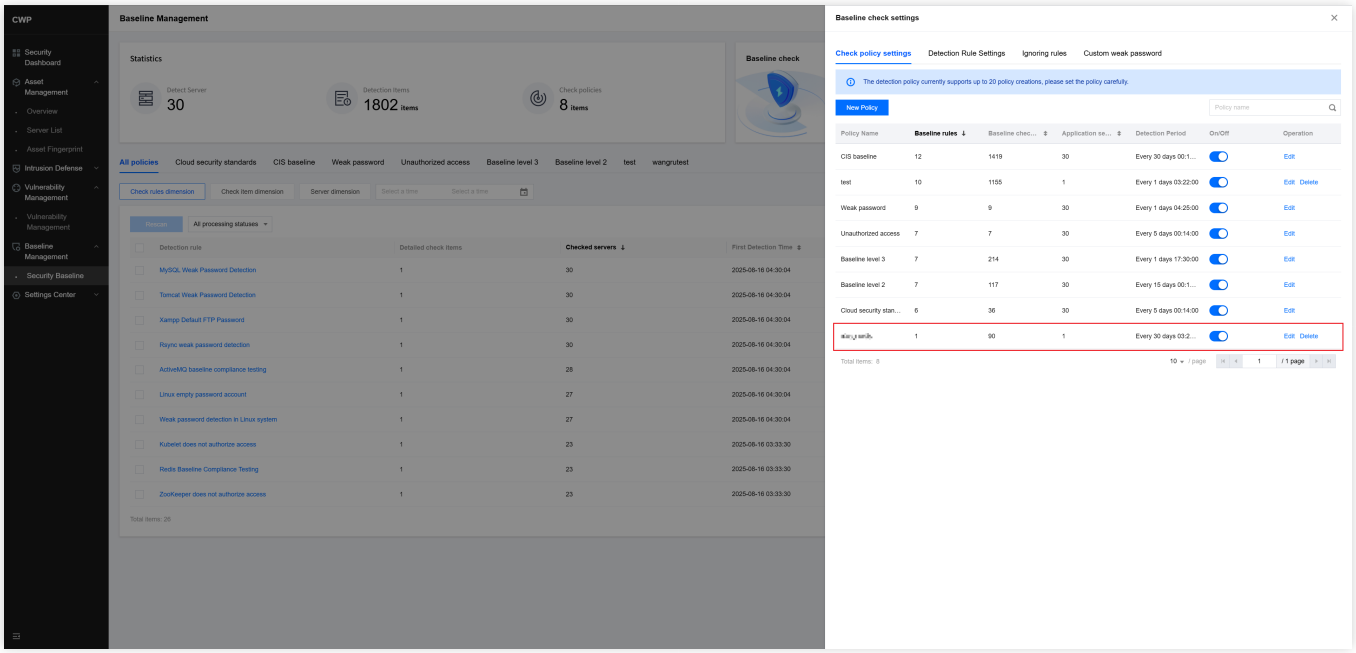
3. On the Policy Creation page, select the baseline check items as needed.



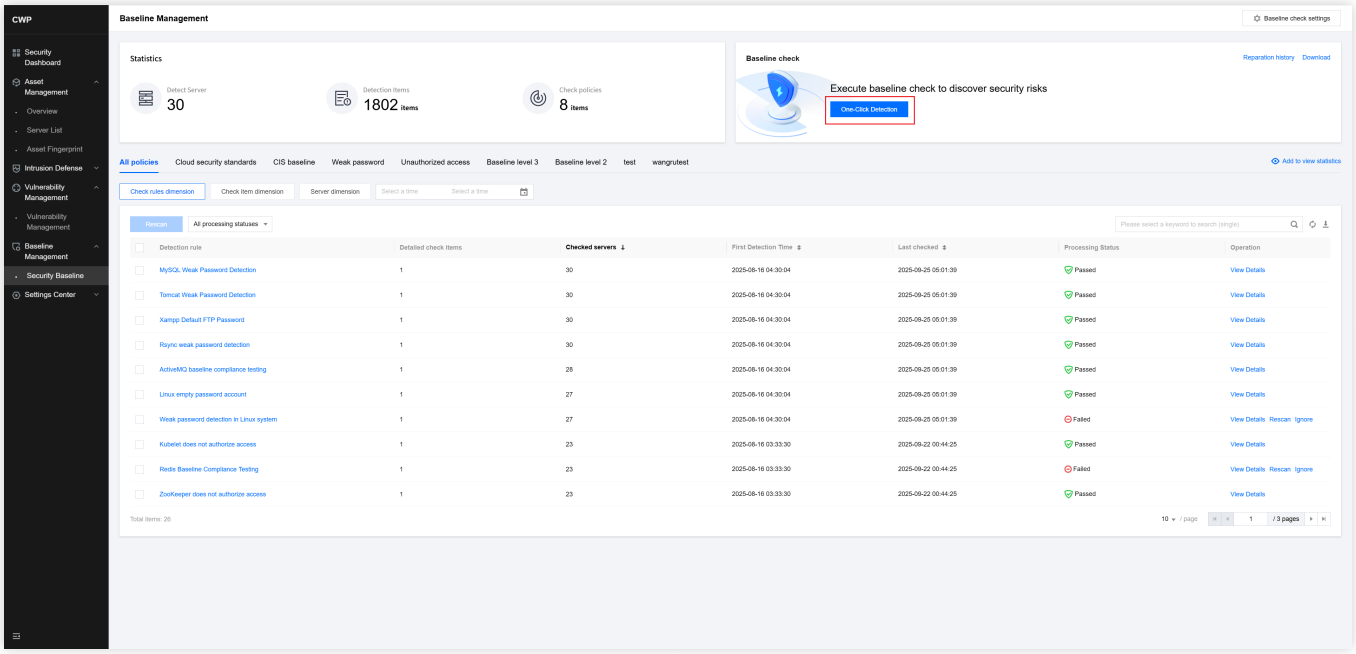
4. After selection, click Next and select the hosts to which the policy should be applied.



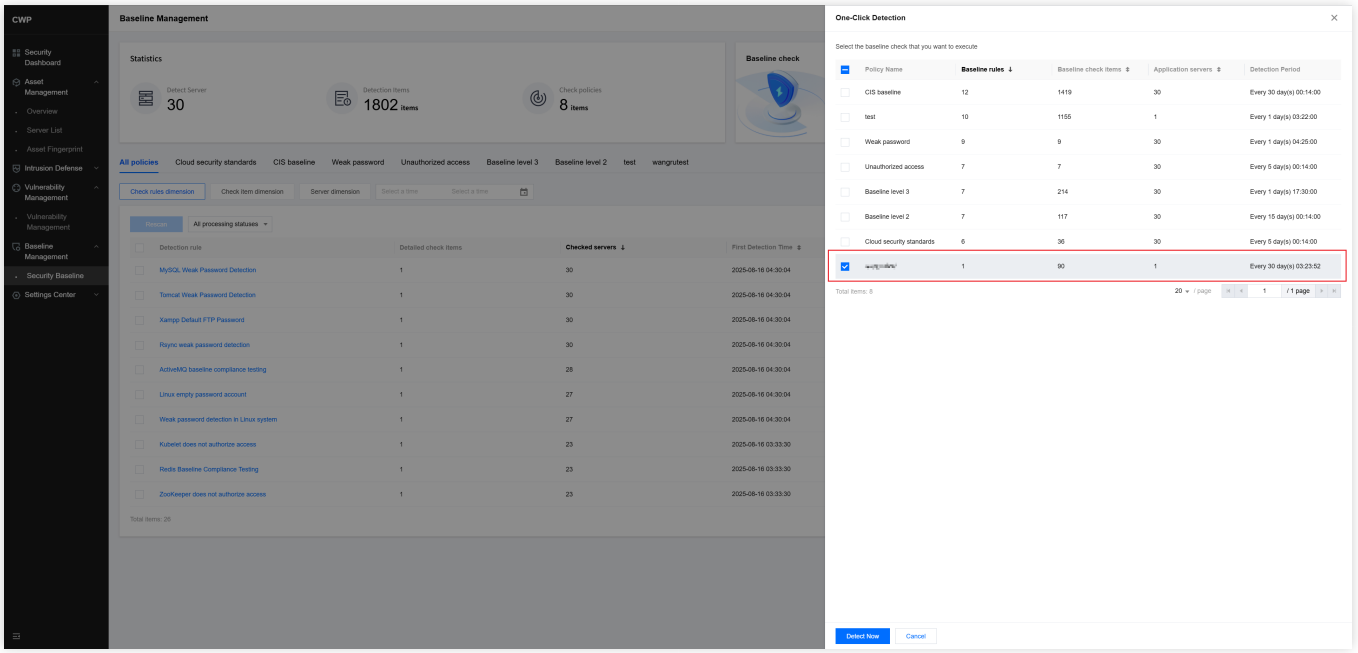
5. Click Next to create the policy. You will be redirected back to the Baseline Detection Settings page, where the new policy is displayed.



6. Return to the Security Baseline page and click One-Click Scan.



7. Select the baseline detection policy you created.



Click Detect Now to immediately begin the baseline scan.

Purchase Guide
Overview

Cloud Workload Protection (CWP) Purchase Guide

The purpose of this document is to provide a practical guide for understanding, selecting, and purchasing the appropriate Cloud Workload Protection (CWP) solution based on specific security requirements, deployment environments, and cost considerations.

It is intended for:

- Cloud administrators
- Security teams
- Procurement or compliance officers

This guide outlines available CWP editions, core features, pricing models, and deployment recommendations to help organizations make informed decisions and ensure effective protection of their cloud workloads.

Cloud Workload Protection (CWP) is a cloud-native security solution designed to protect your cloud servers (virtual machines) from attacks, vulnerabilities, and misconfigurations.

It provides:

- Real-time threat detection
- Malware and ransomware protection
- Vulnerability scanning
- Asset management
- Compliance support (e.g., for regulatory standards like MLPS)

CWP works by deploying lightweight agents on your cloud or on-prem servers, offering centralized visibility and protection across your workloads.

Protection Licenses Overview

The following table provides the billing instructions for different CWPP protection licenses. For the features

in different editions, see Features in Different Editions.

Protection License	Billing Instructions
CWPP Basic	Free of charge. Servers with a CWPP agent enjoy basic protection. A CWPP agent is automatically installed for the purchased CVM, Lighthouse, and ECM by default.
CWPP Pro	Monthly subscription: 12 USD/license/month. The subscription fee is deducted directly when the order is placed.
CWPP Ultimate	Monthly subscription: 27 USD/license/month. The subscription fee is deducted directly when the order is placed. It cannot be downgraded to CWPP Pro.

Note:
Protection licenses are available to all Converge Cloud users after identity verification.

Purchase Method

Protection licenses can be purchased through the CWPP purchase page. You can select the server to be bound when purchasing a license, or bind a server later after purchasing a license.

Overdraft and Renewal

If auto-renewal has been set, but the deduction is unsuccessful because the relevant account has an insufficient balance or is overdrawn (balance below 0), the original license will be automatically unbound from the server (which means the protection will be stopped) and will enter a 30-day isolation period. If the license is not renewed during this period, the license order will expire and terminated.

Troubleshooting
Troubleshooting Ideas of Linux Intrusion Issues

This document will guide you on how to troubleshoot Linux intrusion issues and provide security optimization suggestions after the intrusion.

> Notes:
>
> If you have identified the intrusion as a mining script or Trojan, see Mining Trojan Self-Service Cleanup Guide.

Analyzing and Identifying the Cause of Intrusion

1. Checking for Hidden Accounts and Weak Passwords

1. Check for weak passwords in the system and application accounts.
    - Description: Check whether administrator accounts, database accounts, MySQL accounts, Tomcat accounts, or website administrator accounts are using weak passwords. Weak passwords are easy targets for brute force cracking.
    - Solution: Log in to the system or application backend as an administrator and change the password to a strong password.
    - Risk level: High.
2. Execute the `last` command to check recent login records for suspicious accounts or IP addresses.
    - Description: Attackers or malicious software often inject hidden system accounts into the system to escalate privileges or carry out other malicious activities.
    - Solution: If suspicious users are found, execute the `usermod -L username` command to disable the user or the `userdel -r username` command to delete the user.
    - Risk level: High.
3. Execute the command `less /var/log/secure|grep 'Accepted'` to check for suspicious IP addresses that logged in to the server.
    - Description: Attackers or malicious software often inject hidden system accounts into the system to escalate privileges or carry out other malicious activities.
    - Solution: If suspicious users are found, execute the `usermod -L <username>` command to disable the user or the `userdel -r <username>` command to delete the user.
    - Risk level: High.
4. Check whether the system uses the default management port.

- Check whether the management ports used by the system, such as SSH, FTP, MySQL, and Redis®, are default ports. These default ports are often easily exploited by automated tools through brute force cracking.

- Solution:
  a. You can edit port 22 in the `/etc/ssh/sshd_config` file, change it to a non-default port, and restart the ssh service.

  > Notes:
  >
  > After modifying the port, update the inbound rules of the CVM's security group in the CVM console to allow traffic on the new port.

  b. You can execute the /etc/init.d/sshd restart (CentOS) or /etc/init.d/ssh restart (Debian / Ubuntu) command to restart the system for the configuration to take effect.
  c. Modify the default listening ports (such as 21 for FTP, 3306 for MySQL, and 6379 for Redis®) in the respective configuration files.
  d. You can restrict the IP logged in remotely by editing /etc/hosts.deny and /etc/hosts.allow files.

- Risk level: High.

5. Check the /etc/passwd file for unauthorized accounts.
   - Description: Attackers or malicious software often inject hidden system accounts into the system to escalate privileges or carry out other malicious activities.
   - Solution: Execute the `usermod -L username` command to disable the user or the `userdel -r username` to delete the user.
   - Risk level: Medium.

2. Checking for Malicious Processes and Unauthorized Ports

1. Execute the `netstat -antp` command to check whether unauthorized ports are being listened on, and identify the corresponding PID.
   - Description: Check whether the server has any unauthorized processes listening on ports. Malicious processes often open listening ports to communicate with external control servers.
   - Solution: If unauthorized processes are found, execute `ls -l /proc/$PID/exe` or `file /proc/$PID/exe` (where $PID is the corresponding PID) to check the file path of the process.
     If it is a malicious process, you can delete the corresponding file.
   - Risk level: High.
2. Execute the `ps -ef` and `top` commands to check for abnormal processes.
   - Description: Execute the above commands. If you detect unauthorized processes that change their name continuously and occupy excessive system CPU or memory resources, they may be

malicious programs.
- Solution: After confirming the process is malicious, terminate the process with `kill -9 PID` or block the external connections of the process through a firewall.
- Risk level: High.

3. Checking for Malicious Programs and Suspicious Startup Items

1. Execute the `chkconfig --list` and `cat /etc/rc.local` commands to check for abnormal startup services.
   - Description: Attackers often configure malicious programs in the startup configuration for automatic startup.
   - Solution: If malicious processes are found, execute the `chkconfig service_name off` command to disable them or check for abnormal entries in `/etc/rc.local` and comment out any suspicious lines.
   - Risk level: High.
2. Check the cron directory for illegal scheduled tasks or scripts.
   - Description: Check the content of `/etc/crontab`, `/etc/cron.d`, `/etc/cron.daily`, `cron.hourly/`, `cron.monthly`, and `cron.weekly/` for suspicious scripts or programs.
   - Solution: If you identify an unknown scheduled task, check whether it is part of the normal workload operations. If not, you may comment out the task or remove the corresponding script.
   - Risk level: High.

4. Checking for Vulnerabilities in Third-Party Software

1. If your server runs applications such as web services or databases, restrict application accounts' write permissions to the file system, and run applications as a non-root user.
   - Description: Running applications as a non-root user ensures that even if the application is compromised, attackers cannot immediately gain remote control of the server, thus minimizing damage.
   - Solution: Go to the root directory of the web service or the database configuration directory. You can run the `chown -R apache:apache /var/www/xxxx` and `chmod -R 750 file1.txt` command to configure website access permissions.
   - Risk level: Medium.
   - For more information, see the example of directory file permissions for a website.
2. Upgrade and patch application vulnerabilities
   - One common cause of server intrusions is the use of outdated application software versions that contain unpatched vulnerabilities, which attackers can exploit.
   - Solution: Common vulnerabilities include ImageMagick, OpenSSL, and glibc. You can follow security advisories or execute apt-get/yum to upgrade and patch the software.
   - Risk level: High.

Example of directory file permissions for a website: Scenario:
Assume the HTTP server runs under the user and user group www, the website user is centos, and the website root directory is /home/centos/web .
Methods/Steps:

1. Set the website directory and file owner and group to centos and www, and execute the following command:

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

2. Set the website directory permissions to 750, which indicates that the centos user has read, write, and execute permissions, the group has read and execute permissions, and other users have no permissions.

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

3. Set the website file permissions to 640, which indicates that only the centos user can modify the files, the HTTP server can read the files but cannot modify them, and other users have no permissions.

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

4. Grant write permissions to specific directories as needed. For example, cache directories or the /data/ directory of Discuz X2 require write access for the HTTP server.

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

Security Optimization Recommendations After an Intrusion

- It is recommended to use SSH keys for login to reduce the risk of brute force cracking.
- Change the SSH port by editing /etc/ssh/sshd_config and setting Port 22 to another non-default port. After modification, execute the following command to restart the SSH service:

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

> Notes:
>
> After modifying the port, update the inbound rules of the CVM's security group in the CVM console to allow traffic on the new port.

- If SSH passwords are required for management, set a strong password.
- Set complex, unique passwords for all application management backends (such as websites, middleware, and Tomcat), remote SSH, remote desktop, and databases.
- Example of strong passwords (spaces are allowed):
  1qtwo-threeMiles3c45jia and
  caser, lanqiu streets .
- Examples of weak passwords, which are often based on common phrases or personal information:
  The company name and date, such as coca-cola2016xxxx, and
  common phrases, such as Iamagoodboy.
- Execute the following command to check open ports and close non-workload ports on your host:

netstat -antp

- Use security group firewall rules or edit /etc/hosts.deny and /etc/hosts.allow to allow access only from specified IP addresses.
- Applications should avoid using root permissions whenever possible.
- Programs such as Apache, Redis®, MySQL, and Nginx should avoid running with root permissions whenever possible.
- Fix privilege escalation vulnerabilities in the system and programs running as a root user to prevent malware from gaining root access and installing backdoors.
- Update systems and applications regularly, including programs such as Struts2, Nginx, ImageMagick, and Java.
- Disable remote management features of applications such as Redis® and NTP. If remote management is not required, disable external listening ports or related configurations.
- Regularly back up workload data from CVM.
- Perform cross-region or cloud backups for important workload data to ensure recovery after an intrusion.
- In addition to backing up /home and /root directories, you should also back up /etc and /var/log, which are crucial for forensic analysis.
- Install a CWP agent to identify risks in the event of an attack.

> Notes:
>
> If the preceding steps do not resolve the issue, it is recommended to contact the Ops personnel for support.

Troubleshooting ideas of Windows intrusion issues

This document describes how to troubleshoot Windows intrusion issues.

Analyzing and Identifying the Cause of Intrusion

1. Checking for Accounts and Weak Passwords

1. Check for weak passwords in the system or application accounts.
    - Description: Check whether system administrator accounts, website backend accounts, database accounts, and other application accounts (such as FTP, Tomcat, and phpMyAdmin) for weak passwords.

      > Notes:
      >
      > It is recommended to set a complex password that is 12 to 16 characters in length and includes uppercase and lowercase letters, digits, and special characters. You may also use a password generator to automatically generate complex passwords.

    - Method: Check the passwords manually based on the actual environment.
    - Risk level: High.
2. Check for accounts that are not created by the system or legal users.
    - Description: Hackers often create abnormal accounts, which are typically visible in the local user group list.
    - Method: First, open the Command Prompt (CMD) and enter the command lusrmgr.msc . Then, check for new accounts, especially those in the Administrator group. If such accounts are found, disable or delete them immediately.
    - Risk level: High.
3. Check for hidden account names.
    - Description: To avoid detection, hackers may create hidden accounts that are not visible in the local user list.
    - Method: (You can also use the LP_Check security tool to identify hidden accounts.)
      a. Open the Run dialog box on the desktop (you can use the shortcut keys Win + R to open it), enter regedit, and you can open the registry editor.
      b. Select HKEY_LOCAL_MACHINE/SAM/SAM. By default, you cannot view the content of this

option. Right-click the menu and select Permissions to open the Permission Management window.

c. Select the current user (usually Administrator), check Full Control under permissions, click OK, and then close the Registry Editor.

d. Open the Registry Editor again and select HKEY_LOCAL_MACHINE/SAM/SAM/Domains/Account/Users.

e. Under Names, you can see all the usernames of the instance. If there is an account that does not exist in the local account, it is a hidden account. After it is confirmed as a non-system user, you can delete this user.

- Risk level: High.

2. Checking for Malicious Processes and Ports

1. Check whether malicious processes are running in the backend.
   - Description: After gaining access, attackers often run malicious processes to communicate externally. By analyzing outbound connections, you can identify the control process used in the intrusion.
   - Method:

     a. Log in to the server and select Start > Run.

     b. Enter cmd , then enter netstat –nao and check whether there are any unauthorized ports being listened on the server.

     c. Open the Task Manager and check whether the process corresponding to the PID process number is a normal one. For example, you can check the path of the running file through the PID number and delete the corresponding path file. You can also use the Process Explorer tool provided by Microsoft for troubleshooting.
   - Risk level: High.

3. Checking for Malicious Programs and Startup Items

1. Check for abnormal startup items in the system.
   - Description: After compromising a system, attackers often configure malicious programs in the startup configuration for automatic startup.
   - Method:

     a. Log in to the server and select Start> All Programs >Start.

     b. By default, this directory is an empty one. Check whether there are any non-business programs in this directory.

     c. Select Start > Run, enter msconfig , check whether there are any startup items with exception names. If so, untick the startup items with exception names and delete the files in the path displayed in the command.

d. Select Start > Run, enter regedit , open Registry,and check if startup items are normal. Pay special attention to the following three Registry entries:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
Check if there are any abnormal startup items on the right side of the Registry. If so, please delete them and consider installing antivirus software for a virus scan to clear out any cruft, viruses, or Trojans.

- Risk level: High.

2. Check active sessions.
   - Description: Check sessions or scheduled tasks between the server and other servers on the network.
   - Method:
     a. Log in to the server and select Start > Run.
     b. Enter cmd , then enter netstat -ano , check the session between the server and other servers on the network, and confirm whether it is a normal connection. Enter schtasks to check the scheduled tasks on the server and confirm whether they are normal scheduled tasks.
   - Risk level: Medium.

4. Checking for Vulnerabilities in Third-Party Software

1. If your server hosts publicly accessible applications, such as World Wide Web (WWW) and File Transfer Protocol (FTP), configure the software to restrict its permissions, and disable directory browsing and file write access where not required.
2. Enable WAF for protection and check its attack logs.

FAQs

How Can I Recover a Website or System After It Has Been Compromised?

After a system is confirmed to have been intruded, the system files are often changed and replaced. At this point, the system has become untrustworthy. The best method is to reinstall the system and install all patches for the new system at the same time.

How Can I Prevent the System or Website from Being Compromised Again?

1. Change all system account passwords to complex passwords and ensure they differ from pre-compromise passwords.
2. Perform the following operations to modify the default remote desktop port:

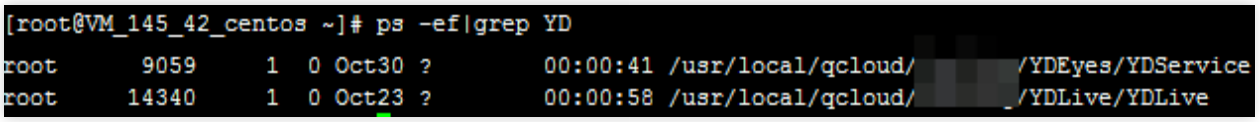
   i. Go to Start > Running and enter regedit .
   ii. Open the registry, and enter the following path: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp.
   iii. KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Tenninal Server\WinStations\RDP-Tcp
   iv. Modify the PortNumber value on the right.
3. Configure your security group firewall to allow remote desktop access only from specified IP addresses.
4. Regularly back up important workload data and files.
5. Regularly update the operating system and application components, such as FTP servers and Struts2, to avoid exploitation through known vulnerabilities.
6. Install a CWP agent and antivirus software to perform regular system health checks and malware scans.

Offline Troubleshooting for Linux Clients

This document describes how to perform offline troubleshooting on Linux clients, including troubleshooting when client processes fail to start and troubleshooting network failures.

Troubleshooting Client Process Startup Issues

1. Check whether the CWP process is running by executing the following command: ps -ef|grep YD . Under normal conditions, two processes should be running for CWP, as shown in the figure below:



- If the process is not found, the following possible causes are included:
- The CWP is not installed, or the client has been uninstalled. In this case, see Quick Start to reinstall the client.
- The client may have encountered an abnormal conflict or crash, preventing the process from starting.

2. If CWP or the client is installed on the server, you can use the following methods to troubleshoot the startup issue for the client process:

- Check the client logs, which are stored at /usr/local/qcloud/YunJing/log .
- Execute the following command to start the CWP service: sh /usr/local/qcloud/YunJing/startYD.sh .

Troubleshooting Network Issues

If the process exists but the CWP is not online, it is mostly because the network is not connected. Please take the following troubleshooting steps:

1. If the CWP domain name cannot be accessed, try modifying the Domain Name System (DNS) settings. You can execute the following command to check whether the CWP domain name is accessible.
    - For VPC and CBM servers, execute telnet s.yd.convergecloud.com 5574 .
      Under Normal Circumstances: Returns the result as shown in the figure below.



If your access attempt fails:

a. You can try modifying dns nameserver field: vim /etc/resolv.conf . nameserver master address

b. After the modification is completed, re-execute telnet s.yd.convergecloud.com 5574 to check whether the connection is established.

c. If the connection is successful, wait for a few minutes (the length of time depends on the network conditions), and the console will be able to see that the corresponding server is back online.

- For servers on the basic network (non-VPC servers), execute telnet s.yd.convergecloud.com 5574 .

  Under Normal Circumstances: Returns the result as shown in the figure below.



If your access attempt fails:

a. Edit the DNS settings by modifying dns nameserver field: vim /etc/resolv.conf . You should comment out the existing nameserver fields and add a nameserver field with the relevant IP address.

b. After the modification is completed, re-execute telnet s.yd.convergecloud.com 5574 to check whether the connection is established.

c. If the connection is successful, wait for a few minutes (the length of time depends on the network conditions), and the console will be able to see that the corresponding server is back online.

2. Firewall policy restrictions: Ensure that the following TCP ports are open on the Linux client: 5574, 8080, 80, and 9080.
3. If the CWP process is running and the client is offline for reasons other than network issues, please package the client logs that are located at /usr/local/qcloud/YunJing/log and contact a technical support engineer for assistance.

Offline Troubleshooting for Windows Clients

Troubleshooting Client Process Startup Issues

Check whether the CWP process is running.
Open the Windows Task Manager and check whether a process named YDService.exe is running.

1. If the process is not found, the following possible causes are included:
    - The CWP is not installed, or the client has been uninstalled. In this case, see Quick Start to reinstall the client.
    - The client may have encountered an abnormal conflict or crash, preventing the process from starting.
2. Troubleshooting methods:
    - Check the client logs, which are stored at C:\Program Files\QCloud\YunJing\log .
    - You can execute the following command to manually start the client: sc start ydservice .

Troubleshooting Network Issues

If the process exists but the CWP Client is offline, it is probably because the network is unavailable. Follow the steps below to troubleshoot:

1. Check whether the DNS has been modified by executing the following command lines. If any one of them returns a normal result, it indicates that DNS functions properly.
    - For servers on the basic network (non-VPC servers), execute telnet s.yd.convergecloud.com 5574 .
    - For VPC and CBM servers, execute telnet s.yd.convergecloud.com 5574.
2. Firewall policy restrictions: Ensure that the following ports are open: 5574, 8080, 80, and 9080.
3. If the CWP process is running and the client is offline for reasons other than network issues, please package the client logs that are located at C:\Program Files\QCloud\YunJing\log and contact a technical support engineer for assistance.

Exception Login Reminder

Symptom

You can receive an alarm notification about abnormal login attempts to your server. The following figure is an example of such a notification delivered via SMS.

Possible Causes

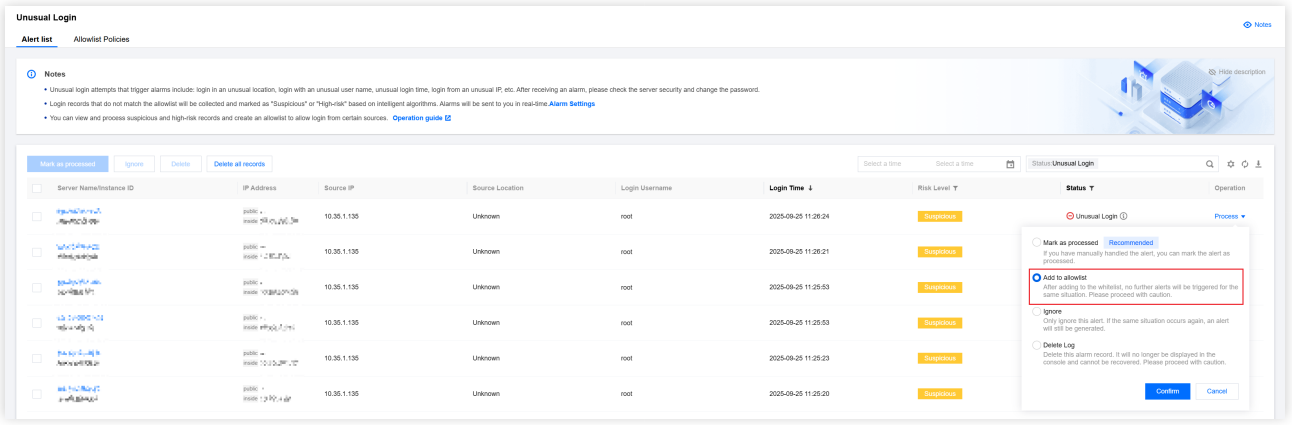
When a login activity is detected on a server under your account, and this login does not match the login allowlist, CWP will mark the login as suspicious or high-risk based on an intelligent algorithm and trigger a real-time alarm.

> Note:
> - By default, only high-risk abnormal login events will trigger an alarm. You can enable or disable this alarm through Settings Center > Alarm Settings. - The risk level of an abnormal login is determined by algorithms that comprehensively assess the server's historical login behaviors.

Handling Steps

After the exception login alarm is received, follow the steps below:

1. Check whether this login activity is legal.
   - If the login activity is legal, add this login record to the allowlist. When the same event happens again, it will not trigger an alarm.



   - If the login activity is illegal, proceed with Step 2.
2. If the login is confirmed to be illegal, the abnormal login may result from a compromised account, especially one that is rarely used. In this case, it is recommended that you immediately change the login password and update any stored login credentials on the server. For more information about the routine inspection procedures on the server, see Linux Intrusion Troubleshooting Guide and Windows Intrusion Troubleshooting Guide.

Hardening Methods

You can subsequently use the following enhancement methods to improve server security:

- Set a complex password for the server that is 12 to 16 characters in length and includes uppercase and lowercase letters, digits, and special characters.
- Modify the default remote login port for Linux systems on cloud servers.
  File editing path: /etc/ssh/sshd_config.

Change Port 22 to a port number below 65534. Port 22 is typically located on the third or fourth line, and the hash symbol should be removed if present.

You can use the vi command in a remote connection, or download it to a local computer via sftp and modify it. After modification, use the following command to restart the ssh service.

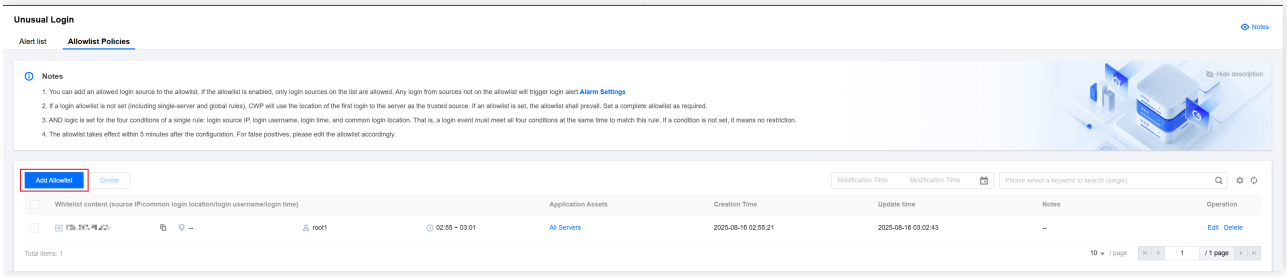
```
/etc/init.d/sshd restart #For CentOS systems, use the ssh restart command.
/etc/init.d/ssh restart #For Debian/Ubuntu systems, use the ssh restart command.
```

Use the security group feature on the platform to allow only required service protocols and ports. Do not allow all protocols or ports.
Configure the CVM system firewall. You are recommended to enable the cloud firewall.
Make sure that the CVM has installed the protection software CWP client process and that it is in normal running and real-time alarm is enabled. When there is an exception login, feedback is given to you in time.
Fix in time the security vulnerabilities in the CVM system components and Web components.

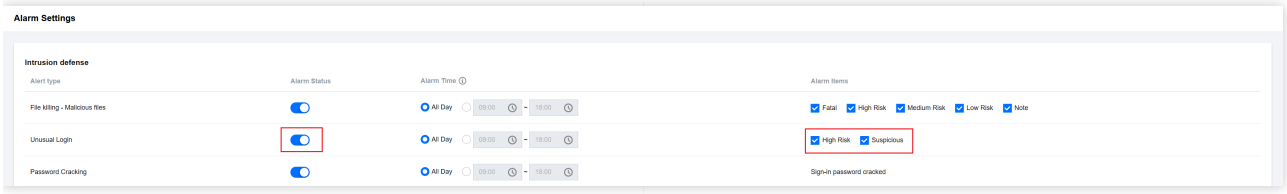
> Notes:
>
> While the above security protection practices for CVMs significantly reduce risks, they do not guarantee absolute protection. Therefore, it is recommended to perform regular security inspections and data backups to prevent data loss or service interruption caused by unexpected events.
> It is also recommended to create system images and data snapshots, and configure automatic scheduled snapshots.

FAQs

Can I disable exception login detection?
No. Abnormal login detection cannot be disabled.
If you do not want to receive exception login alerts, you can configure a complete login allowlist or disable exception login alarms.
Completing the login allowlist: On the Abnormal Login page, choose Allowlist Management > Add to Allowlist, and add frequently used login source IP addresses to the allowlist.



Disabling abnormal login alarms: On the Settings Center page, you can disable the alarm notifications or uncheck the high-risk or suspicious alarm items.



API Documentation
Cloud Workload Protection(cwp)
version(2018-02-28)
API overview

API version

V3

Advanced Defense APIs

Interface name	Interface function
CreateMaWorkloadLabel	CreateMaWorkloadLabel
CreateProtectServer	CreateProtectServer
DeleteAttackLogs	DeleteAttackLogs
DeleteMaConnEvent	DeleteMaConnEvent
DeleteMaCustomPolicy	DeleteMaCustomPolicy
DeleteMaLabel	DeleteMaLabel
DeleteMaSelfLearnPolicy	DeleteMaSelfLearnPolicy
DeleteMaWhitelist	DeleteMaWhitelist
DeleteProtectDir	DeleteProtectDir
DeleteWebPageEventLog	DeleteWebPageEventLog
DescribeAttackEventInfo	DescribeAttackEventInfo
DescribeAttackEvents	DescribeAttackEvents
DescribeAttackLogInfo	DescribeAttackLogInfo
DescribeAttackLogs	DescribeAttackLogs

Interface name	Interface function
DescribeAttackStatistics	DescribeAttackStatistics
DescribeAttackTop	DescribeAttackTop
DescribeAttackTrends	DescribeAttackTrends
DescribeAttackVulTypeList	DescribeAttackVulTypeList
DescribeMaConnEventList	DescribeMaConnEventList
DescribeMaCustomPolicyList	DescribeMaCustomPolicyList
DescribeMaGlobalConf	DescribeMaGlobalConf
DescribeMaHostList	DescribeMaHostList
DescribeMaLabel	DescribeMaLabel
DescribeMaLabelList	DescribeMaLabelList
DescribeMaLabelSourceList	DescribeMaLabelSourceList
DescribeMaPodList	DescribeMaPodList
DescribeMaSelfLearnConfig	DescribeMaSelfLearnConfig
DescribeMaSelfLearnPolicyList	DescribeMaSelfLearnPolicyList
DescribeMaSummary	DescribeMaSummary
DescribeMaWhitelist	DescribeMaWhitelist
DescribeMaWorkloadLabel	DescribeMaWorkloadLabel
DescribeMaWorkloadList	DescribeMaWorkloadList
DescribeMachineList	DescribeMachineList
DescribeNetAttackSetting	DescribeNetAttackSetting
DescribeProtectDirList	DescribeProtectDirList
DescribeProtectDirRelatedServer	DescribeProtectDirRelatedServer
DescribeServerRelatedDirInfo	DescribeServerRelatedDirInfo
DescribeWebPageEventList	DescribeWebPageEventList
DescribeWebPageGeneralize	DescribeWebPageGeneralize

Interface name	Interface function
DescribeWebPageProtectStat	DescribeWebPageProtectStat
DescribeWebPageServiceInfo	DescribeWebPageServiceInfo
DisableSelfLearn	DisableSelfLearn
ExportAttackEvents	ExportAttackEvents
ExportAttackLogs	ExportAttackLogs
ExportMaConnEventList	ExportMaConnEventList
ExportMaCustomPolicyList	ExportMaCustomPolicyList
ExportMaHostList	ExportMaHostList
ExportMaPodList	ExportMaPodList
ExportMaSelfLearnPolicyList	ExportMaSelfLearnPolicyList
ExportMaWhitelist	ExportMaWhitelist
ExportProtectDirList	ExportProtectDirList
ExportWebPageEventList	ExportWebPageEventList
ModifyMaConnEventType	ModifyMaConnEventType
ModifyMaCustomPolicy	ModifyMaCustomPolicy
ModifyMaCustomPolicyStatus	ModifyMaCustomPolicyStatus
ModifyMaGlobalConf	ModifyMaGlobalConf
ModifyMaLabel	ModifyMaLabel
ModifyMaSelfLearnConfig	ModifyMaSelfLearnConfig
ModifyMaWhitelist	ModifyMaWhitelist
ModifyMaWhitelistStatus	ModifyMaWhitelistStatus
ModifyMaWorkloadLabel	ModifyMaWorkloadLabel
ModifyMaWorkloadMonitor	ModifyMaWorkloadMonitor
ModifyMemShellRules	ModifyMemShellRules
ModifyNetAttackSetting	ModifyNetAttackSetting

Interface name	Interface function
ModifyWebPageProtectDir	ModifyWebPageProtectDir
ModifyWebPageProtectSetting	ModifyWebPageProtectSetting
ModifyWebPageProtectSwitch	ModifyWebPageProtectSwitch

Asset Management APIs

Interface name	Interface function
CreateIncidentBacktracking	CreateIncidentBacktracking
DeleteCloudVendorAccountAK	DeleteCloudVendorAccountAK
DeleteMachine	DeleteMachine
DeleteMachineTag	DeleteMachineTag
DeleteTags	DeleteTags
DescribeAccountStatistics	DescribeAccountStatistics
DescribeAssetAppList	DescribeAssetAppList
DescribeAssetAppProcessList	DescribeAssetAppProcessList
DescribeAssetCoreModuleInfo	DescribeAssetCoreModuleInfo
DescribeAssetCoreModuleList	DescribeAssetCoreModuleList
DescribeAssetDatabaseInfo	DescribeAssetDatabaseInfo
DescribeAssetDatabaseList	DescribeAssetDatabaseList
DescribeAssetHostTotalCount	DescribeAssetHostTotalCount
DescribeAssetInfo	DescribeAssetInfo
DescribeAssetInitServiceList	DescribeAssetInitServiceList
DescribeAssetJarInfo	DescribeAssetJarInfo
DescribeAssetJarList	DescribeAssetJarList
DescribeAssetMachineDetail	DescribeAssetMachineDetail

Interface name	Interface function
DescribeAssetMachineList	DescribeAssetMachineList
DescribeAssetPlanTaskList	DescribeAssetPlanTaskList
DescribeAssetPortInfoList	DescribeAssetPortInfoList
DescribeAssetProcessInfoList	DescribeAssetProcessInfoList
DescribeAssetRecentMachineInfo	DescribeAssetRecentMachineInfo
DescribeAssetSystemPackageList	DescribeAssetSystemPackageList
DescribeAssetUserInfo	DescribeAssetUserInfo
DescribeAssetUserList	DescribeAssetUserList
DescribeAssetWebAppList	DescribeAssetWebAppList
DescribeAssetWebAppPluginList	DescribeAssetWebAppPluginList
DescribeAssetWebFrameList	DescribeAssetWebFrameList
DescribeAssetWebLocationInfo	DescribeAssetWebLocationInfo
DescribeAssetWebLocationList	DescribeAssetWebLocationList
DescribeAssetWebServiceInfoList	DescribeAssetWebServiceInfoList
DescribeAssetWebServiceProcessList	DescribeAssetWebServiceProcessList
DescribeCloudVendorAccountAKList	DescribeCloudVendorAccountAKList
DescribeComponentStatistics	DescribeComponentStatistics
DescribeComponents	DescribeComponents
DescribeExportMachines	DescribeExportMachines
DescribeHistoryAccounts	DescribeHistoryAccounts
DescribeImportMachineInfo	DescribeImportMachineInfo
DescribeMachineInfo	DescribeMachineInfo
DescribeMachineOsList	DescribeMachineOsList
DescribeMachineRegionList	DescribeMachineRegionList
DescribeMachineRegions	DescribeMachineRegions

Interface name	Interface function
DescribeMachines	DescribeMachines
DescribeOpenPortStatistics	DescribeOpenPortStatistics
DescribeProcessStatistics	DescribeProcessStatistics
DescribeTagMachines	DescribeTagMachines
DescribeTags	DescribeTags
EditTags	EditTags
ExportAssetCoreModuleList	ExportAssetCoreModuleList
ExportAssetWebServiceInfoList	ExportAssetWebServiceInfoList
ModifyMachineRemark	ModifyMachineRemark
ScanAsset	ScanAsset
SyncAssetScan	SyncAssetScan
UpdateMachineTags	UpdateMachineTags

Baseline Management APIs

Interface name	Interface function
ChangeRuleEventsIgnoreStatus	ChangeRuleEventsIgnoreStatus
CreateBaselineStrategy	CreateBaselineStrategy
DeleteBaselineStrategy	DeleteBaselineStrategy
DescribeBaselineAnalysisData	DescribeBaselineAnalysisData
DescribeBaselineBasicInfo	DescribeBaselineBasicInfo
DescribeBaselineDetail	DescribeBaselineDetail
DescribeBaselineEffectHostList	DescribeBaselineEffectHostList
DescribeBaselineHostTop	DescribeBaselineHostTop
DescribeBaselineList	DescribeBaselineList

Interface name	Interface function
DescribeBaselineRule	DescribeBaselineRule
DescribeBaselineScanSchedule	DescribeBaselineScanSchedule
DescribeBaselineStrategyDetail	DescribeBaselineStrategyDetail
DescribeBaselineStrategyList	DescribeBaselineStrategyList
DescribeBaselineTop	DescribeBaselineTop
DescribeIgnoreBaselineRule	DescribeIgnoreBaselineRule
DescribeIgnoreRuleEffectHostList	DescribeIgnoreRuleEffectHostList
DescribeStrategyExist	DescribeStrategyExist
ExportBaselineEffectHostList	ExportBaselineEffectHostList
ExportBaselineList	ExportBaselineList
ExportIgnoreBaselineRule	ExportIgnoreBaselineRule
ExportIgnoreRuleEffectHostList	ExportIgnoreRuleEffectHostList
UpdateBaselineStrategy	UpdateBaselineStrategy

Baseline Management APIs (New)

Interface name	Interface function
DeleteBaselinePolicy	DeleteBaselinePolicy
DeleteBaselineRule	DeleteBaselineRule
DeleteBaselineRuleIgnore	DeleteBaselineRuleIgnore
DeleteBaselineWeakPassword	DeleteBaselineWeakPassword
DescribeBaselineDetectList	DescribeBaselineDetectList
DescribeBaselineDetectOverview	DescribeBaselineDetectOverview
DescribeBaselineDownloadList	DescribeBaselineDownloadList
DescribeBaselineFixList	DescribeBaselineFixList

Interface name	Interface function
DescribeBaselineHostDetectList	DescribeBaselineHostDetectList
DescribeBaselineHostIgnoreList	DescribeBaselineHostIgnoreList
DescribeBaselineHostRiskTop	DescribeBaselineHostRiskTop
DescribeBaselineItemDetectList	DescribeBaselineItemDetectList
DescribeBaselineItemIgnoreList	DescribeBaselineItemIgnoreList
DescribeBaselineItemInfo	DescribeBaselineItemInfo
DescribeBaselineItemList	DescribeBaselineItemList
DescribeBaselineItemRiskTop	DescribeBaselineItemRiskTop
DescribeBaselinePolicyList	DescribeBaselinePolicyList
DescribeBaselineRuleCategoryList	DescribeBaselineRuleCategoryList
DescribeBaselineRuleDetectList	DescribeBaselineRuleDetectList
DescribeBaselineRuleIgnoreList	DescribeBaselineRuleIgnoreList
DescribeBaselineRuleList	DescribeBaselineRuleList
DescribeBaselineWeakPasswordList	DescribeBaselineWeakPasswordList
DescribeHotVulTop	DescribeHotVulTop
DescribeIgnoreHostAndItemConfig	DescribeIgnoreHostAndItemConfig
DescribeVulStoreList	DescribeVulStoreList
ExportBaselineFixList	ExportBaselineFixList
ExportBaselineHostDetectList	ExportBaselineHostDetectList
ExportBaselineItemDetectList	ExportBaselineItemDetectList
ExportBaselineItemList	ExportBaselineItemList
ExportBaselineRuleDetectList	ExportBaselineRuleDetectList
ExportBaselineWeakPasswordList	ExportBaselineWeakPasswordList
FixBaselineDetect	FixBaselineDetect
ModifyBaselinePolicy	ModifyBaselinePolicy

Interface name	Interface function
ModifyBaselinePolicyState	ModifyBaselinePolicyState
ModifyBaselineRule	ModifyBaselineRule
ModifyBaselineRuleIgnore	ModifyBaselineRuleIgnore
ModifyBaselineWeakPassword	ModifyBaselineWeakPassword
StartBaselineDetect	StartBaselineDetect
StopBaselineDetect	StopBaselineDetect
SyncBaselineDetectSummary	SyncBaselineDetectSummary

Expert Service APIs

Interface name	Interface function
DescribeEmergencyResponseList	DescribeEmergencyResponseList
DescribeMonthInspectionReport	DescribeMonthInspectionReport

Intrusion Detection - APIs of Logins from Unusual Locations

Interface name	Interface function
DeleteLoginWhiteList	DeleteLoginWhiteList
DeleteNonlocalLoginPlaces	DeleteNonlocalLoginPlaces
DescribeHostLoginList	DescribeHostLoginList
DescribeLoginWhiteCombinedList	DescribeLoginWhiteCombinedList
DescribeLoginWhiteList	DescribeLoginWhiteList
DescribeUsualLoginPlaces	DescribeUsualLoginPlaces
ExportNonlocalLoginPlaces	ExportNonlocalLoginPlaces

Intrusion Detection - File Scanning and Cleaning APIs

Interface name	Interface function
CreateNetAttackWhiteList	CreateNetAttackWhiteList
CreateScanMalwareSetting	CreateScanMalwareSetting
DeleteMalwareScanTask	DeleteMalwareScanTask
DeleteMalwares	DeleteMalwares
DeleteNetAttackWhiteList	DeleteNetAttackWhiteList
DescribeJavaMemShellList	DescribeJavaMemShellList
DescribeMalWareList	DescribeMalWareList
DescribeMalwareFile	DescribeMalwareFile
DescribeMalwareInfo	DescribeMalwareInfo
DescribeMalwareRiskWarning	DescribeMalwareRiskWarning
DescribeMalwareTimingScanSetting	DescribeMalwareTimingScanSetting
DescribeNetAttackWhiteList	DescribeNetAttackWhiteList
DescribeScanMalwareSchedule	DescribeScanMalwareSchedule
DescribeServersAndRiskAndFirstInfo	DescribeServersAndRiskAndFirstInfo
ExportMalwares	ExportMalwares
ModifyMalwareTimingScanSettings	ModifyMalwareTimingScanSettings
ModifyNetAttackWhiteList	ModifyNetAttackWhiteList
RecoverMalwares	RecoverMalwares
SeparateMalwares	SeparateMalwares
TrustMalwares	TrustMalwares
UntrustMalwares	UntrustMalwares

Intrusion Detection - High-Risk Command APIs

Interface name	Interface function
CheckBashRuleParams	CheckBashRuleParams
DeleteBashEvents	DeleteBashEvents
DeleteBashRules	DeleteBashRules
DescribeBashEvents	DescribeBashEvents
DescribeBashEventsNew	DescribeBashEventsNew
DescribeBashRules	DescribeBashRules
EditBashRules	EditBashRules
ExportBashEvents	ExportBashEvents
SetBashEventsStatus	SetBashEventsStatus
SwitchBashRules	SwitchBashRules

Intrusion Detection - Local Privilege Escalation APIs

Interface name	Interface function
DeletePrivilegeEvents	DeletePrivilegeEvents
DeletePrivilegeRules	DeletePrivilegeRules
DescribePrivilegeEvents	DescribePrivilegeEvents
DescribePrivilegeRules	DescribePrivilegeRules
ExportPrivilegeEvents	ExportPrivilegeEvents

Intrusion Detection - Malicious Request APIs

Interface name	Interface function
DeleteMaliciousRequests	DeleteMaliciousRequests
DescribeMaliciousRequestWhiteList	DescribeMaliciousRequestWhiteList
DescribeRiskDnsList	DescribeRiskDnsList

Interface name	Interface function
ExportMaliciousRequests	ExportMaliciousRequests

Intrusion Detection - Password Cracking APIs

Interface name	Interface function
DeleteBruteAttacks	DeleteBruteAttacks
DescribeBanMode	DescribeBanMode
DescribeBanRegions	DescribeBanRegions
DescribeBanStatus	DescribeBanStatus
DescribeBanWhiteList	DescribeBanWhiteList
DescribeBruteAttackList	DescribeBruteAttackList
DescribeBruteAttackRules	DescribeBruteAttackRules
ExportBruteAttacks	ExportBruteAttacks
ModifyBanMode	ModifyBanMode
ModifyBanStatus	ModifyBanStatus
ModifyBruteAttackRules	ModifyBruteAttackRules
StopNoticeBanTips	StopNoticeBanTips

Intrusion Detection - Reverse Shell APIs

Interface name	Interface function
DeleteMemShellRules	DeleteMemShellRules
DeleteReverseShellEvents	DeleteReverseShellEvents
DeleteReverseShellRules	DeleteReverseShellRules
DeleteReverseShellRulesAggregation	DeleteReverseShellRulesAggregation
DescribeMemShellRules	DescribeMemShellRules

Interface name	Interface function
DescribeReverseShellEvents	DescribeReverseShellEvents
DescribeReverseShellRules	DescribeReverseShellRules
DescribeReverseShellRulesAggregation	DescribeReverseShellRulesAggregation
DescribeReverseShellSystemPolicyConfig	DescribeReverseShellSystemPolicyConfig
DescribeShellPolicyList	DescribeShellPolicyList
ExportReverseShellEvents	ExportReverseShellEvents
ModifyReverseShellRulesAggregation	ModifyReverseShellRulesAggregation
ModifyReverseShellSystemPolicyConfig	ModifyReverseShellSystemPolicyConfig
ModifyShellPolicyStatus	ModifyShellPolicyStatus

Other APIs

Interface name	Interface function
CreateLoginPermissionPush	CreateLoginPermissionPush
DeleteLogClsDeliverInfo	DeleteLogClsDeliverInfo
DeleteScanTask	DeleteScanTask
DescribeAssetEnvList	DescribeAssetEnvList
DescribeClientException	DescribeClientException
DescribeClsAccountStatus	DescribeClsAccountStatus
DescribeClsLogsets	DescribeClsLogsets
DescribeClsTopics	DescribeClsTopics
DescribeCustomerDetail	DescribeCustomerDetail
DescribeGeneralStat	DescribeGeneralStat
DescribeLogClsDeliverInfo	DescribeLogClsDeliverInfo
DescribeLogStorageConfig	DescribeLogStorageConfig

Interface name	Interface function
DescribeLogStorageRecord	DescribeLogStorageRecord
DescribeLoginPermission	DescribeLoginPermission
DescribeMachineInfoByHashKey	DescribeMachineInfoByHashKey
DescribeMachineLoginType	DescribeMachineLoginType
DescribeMachineLoginTypeStatus	DescribeMachineLoginTypeStatus
DescribeOrderList	DescribeOrderList
DescribeOverviewStatistics	DescribeOverviewStatistics
DescribeProVersionInfo	DescribeProVersionInfo
DescribeProVersionStatus	DescribeProVersionStatus
DescribeRecommendedProtectCpu	DescribeRecommendedProtectCpu
DescribeScanState	DescribeScanState
DescribeScanTaskDetails	DescribeScanTaskDetails
DescribeSecurityDynamics	DescribeSecurityDynamics
DescribeSecurityEventStat	DescribeSecurityEventStat
DescribeSecurityEventsCnt	DescribeSecurityEventsCnt
DescribeSecurityTrends	DescribeSecurityTrends
DescribeTaskDuration	DescribeTaskDuration
DescribeTrialReport	DescribeTrialReport
DescribeUsersConfig	DescribeUsersConfig
DescribeVersionStatistics	DescribeVersionStatistics
DescribeVulTrend	DescribeVulTrend
ExportScanTaskDetails	ExportScanTaskDetails
ExportSecurityTrends	ExportSecurityTrends
ExportTasks	ExportTasks
ModifyEventAttackStatus	ModifyEventAttackStatus

Interface name	Interface function
ModifyLogClsDeliverInfo	ModifyLogClsDeliverInfo
ModifyLogClsDeliverSwitch	ModifyLogClsDeliverSwitch
ModifyLogStorageConfig	ModifyLogStorageConfig
ModifyMachineLoginType	ModifyMachineLoginType
ModifyOrder	ModifyOrder
ModifyUsersConfig	ModifyUsersConfig
ModifyVulDefenceSwitch	ModifyVulDefenceSwitch

Security Operations APIs

Interface name	Interface function
CreateSearchLog	CreateSearchLog
CreateSearchTemplate	CreateSearchTemplate
DeleteSearchTemplate	DeleteSearchTemplate
DescribeESAggregations	DescribeESAggregations
DescribeHistoryService	DescribeHistoryService
DescribeIndexList	DescribeIndexList
DescribeLogStorageStatistic	DescribeLogStorageStatistic
DescribeSearchExportList	DescribeSearchExportList
DescribeSearchLogs	DescribeSearchLogs
DescribeSearchTemplates	DescribeSearchTemplates

Settings Center APIs

Interface name	Interface function
CreateAgentInstallTask	CreateAgentInstallTask

Interface name	Interface function
CreateLicenseOrder	CreateLicenseOrder
DeleteLicenseRecord	DeleteLicenseRecord
DescribeAgentInstallResult	DescribeAgentInstallResult
DescribeAgentInstallTaskResult	DescribeAgentInstallTaskResult
DescribeChangingAssetInfo	DescribeChangingAssetInfo
DescribeLicenseBindList	DescribeLicenseBindList
DescribeLicenseBindSchedule	DescribeLicenseBindSchedule
DescribeLicenseGeneral	DescribeLicenseGeneral
DescribeLicenseList	DescribeLicenseList
DescribeSaveOrUpdateWarnings	DescribeSaveOrUpdateWarnings
DescribeWarningList	DescribeWarningList
DescribeWarningServiceIPList	DescribeWarningServiceIPList
DestroyOrder	DestroyOrder
ExportLicenseDetail	ExportLicenseDetail
ModifyAssetsProtectionStatus	ModifyAssetsProtectionStatus
ModifyAutoOpenProVersionConfig	ModifyAutoOpenProVersionConfig
ModifyLicenseBinds	ModifyLicenseBinds
ModifyLicenseOrder	ModifyLicenseOrder
ModifyLicenseUnBinds	ModifyLicenseUnBinds
ModifyOrderAttribute	ModifyOrderAttribute
ModifyWarningSetting	ModifyWarningSetting

Vulnerability Management APIs

Interface name	Interface function

Interface name	Interface function
CancelIgnoreVul	CancelIgnoreVul
CreateEmergencyVulScan	CreateEmergencyVulScan
DescribeEmergencyVulList	DescribeEmergencyVulList
DescribeInjectRiskyServiceSwitch	DescribeInjectRiskyServiceSwitch
DescribeScanSchedule	DescribeScanSchedule
DescribeScanVulSetting	DescribeScanVulSetting
DescribeUndoVulCounts	DescribeUndoVulCounts
DescribeVulCountByDates	DescribeVulCountByDates
DescribeVulDefenceOverviewCount	DescribeVulDefenceOverviewCount
DescribeVulDefenceSettingList	DescribeVulDefenceSettingList
DescribeVulEffectHostList	DescribeVulEffectHostList
DescribeVulHostCountScanTime	DescribeVulHostCountScanTime
DescribeVulHostTop	DescribeVulHostTop
DescribeVulInfoCvss	DescribeVulInfoCvss
DescribeVulLevelCount	DescribeVulLevelCount
DescribeVulList	DescribeVulList
DescribeVulTop	DescribeVulTop
ExportVulDetectionExcel	ExportVulDetectionExcel
ExportVulDetectionReport	ExportVulDetectionReport
ExportVulEffectHostList	ExportVulEffectHostList
ExportVulList	ExportVulList
IgnoreImpactedHosts	IgnoreImpactedHosts
ModifyInjectRiskyServiceSwitch	ModifyInjectRiskyServiceSwitch
ScanVul	ScanVul
ScanVulAgain	ScanVulAgain

Interface name	Interface function
ScanVulSetting	ScanVulSetting

CallingMethod signaturev1

Converge Cloud authenticates each access request, i.e. each request needs to include authentication information (Signature) in the common parameters to verify the identity of the requester.
The Signature is generated by the security credentials which include SecretId and SecretKey. If you don't have the security credentials yet, go to the API Key page to apply for them; otherwise, you cannot invoke the API.

1. Applying for Security Credentials

Before using the API for the first time, go to the API Key page to apply for security credentials.
Security credentials consist of SecretId and SecretKey:

- SecretId is used to identify the API requester.
- SecretKey is used to encrypt the signature string and verify it on the server.
- You must keep your security credentials private and avoid disclosure.

You can apply for the security credentials through the following steps:

1. Log in to the Converge Cloud Console.
2. Go to the Cloud API Key page.
3. On the API Key Management page, click Create Key to create a SecretId/SecretKey pair.

Note: Each account can have up to two pairs of SecretId/SecretKey.

2. Generating a Signature

With the SecretId and SecretKey, a signature can be generated. The following describes how to generate a signature:

Assume that the SecretId and SecretKey are:

- SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
- SecretKey: Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

Note: This is just an example. For actual operations, please use your own SecretId and SecretKey.

Take the Cloud Virtual Machine's request to view the instance list (DescribeInstances) as an example. When

you invoke this API, the request parameters may be as follows:

Parameter name	Description	Parameter value
Action	Method name	DescribeInstances
SecretId	Key ID	AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
Timestamp	Current timestamp	1465185768
Nonce	Random positive integer	11886
Region	Region where the instance is located	luzon
InstanceIds.0	ID of the instance to query	ins-09dx96dg
Offset	Offset	0
Limit	Allowed maximum output	20
Version	API version number	2017-03-12

2.1. Sorting Parameters

First, sort all the request parameters in an ascending lexicographical order (ASCII code) by their names. Notes: (1) Parameters are sorted by their names instead of their values; (2) The parameters are sorted based on ASCII code, not in an alphabetical order or by values. For example, InstanceIds.2 should be arranged after InstanceIds.12. You can complete the sorting process using a sorting function in a programming language, such as the ksort function in PHP. The parameters in the example are sorted as follows:

```
{
    'Action' : 'DescribeInstances',
    'InstanceIds.0' : 'ins-09dx96dg',
    'Limit' : 20,
    'Nonce' : 11886,
    'Offset' : 0,
    'Region' : 'luzon',
    'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE',
    'Timestamp' : 1465185768,
    'Version': '2017-03-12',
}
```

When developing in another programming language, you can sort these sample parameters and it will work as long as you obtain the same results.

2.2. Concatenating a Request String

This step generates a request string.
Format the request parameters sorted in the previous step into the form of "parameter name"="parameter value". For example, for the Action parameter, its parameter name is "Action" and its parameter value is "DescribeInstances", so it will become Action=DescribeInstances after formatted.
Note: The "parameter value" is the original value but not the value after URL encoding.

Then, concatenate the formatted parameters with "&". The resulting request string is as follows:

```
Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.3. Concatenating the Signature Original String

This step generates a signature original string.
The signature original string consists of the following parameters:

1. HTTP method: POST and GET modes are supported, and GET is used here for the request. Please note that the method name should be in all capital letters.
2. Request host: the domain name of the request to view the list of instances (DescribeInstances) is cvm.convergecloud.com. The actual request domain name varies by the module to which the API belongs. For more information, see the instructions of the specific API.
3. Request path: The request path in the current version of Cloud API is fixed to / .
4. Request string: the request string generated in the previous step.

The concatenation rule of the signature original string is: Request method + request host + request path + ? + request string

The concatenation result of the example is:

```
GETcvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.4. Generating a Signature String

This step generates a signature string.
First, use the HMAC-SHA1 algorithm to sign thesignature original stringobtained in the previous step, and then encode the generated signature using Base64 to obtain the final signature.

The specific code is as follows with the PHP language being used as an example:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3EXAMPLE';
$srcStr = 'GETcvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit
=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPL
E&Timestamp=1465185768&Version=2017-03-12';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

The final signature is:

```
EliP9YW3pW28FpsEdkXt/+WcGeI=
```

When developing in another programming language, you can sign and verify the original in the example above and it works as long as you get the same results.

3. Encoding a Signature String

The generated signature string cannot be directly used as a request parameter and must be URL encoded.

For example, if the signature string generated in the previous step is EliP9YW3pW28FpsEdkXt/+WcGeI= , the final signature string request parameter (Signature) is EliP9YW3pW28FpsEdkXt%2f%2bWcGeI%3d, which will be used to generate the final request URL.

**Note: If your request method is GET, or the request method is POST and the Content-Type is application/x-www-form-urlencoded, then all the request parameter values need to be URL encoded (except the parameter key and the symbol of =) when sending the request. Non-ASCII characters need to be encoded with UTF-8 before URL encoding. **

Note: The network libraries of some programming languages automatically URL encode all parameters, in which case there is no need to URL encode the signature string; otherwise, two rounds of URL encoding will cause the signature to fail.

Note: Other parameter values also need to be encoded using RFC 3986. Use %XY in percent-encoding for special characters such as Chinese characters, where "X" and "Y" are hexadecimal characters (0-9 and uppercase A-F), and using lowercase will cause an error.

4. Signature Failure

The following situational error codes for signature failure may occur. Please resolve the errors accordingly.

Error code	Error description
AuthFailure.SignatureExpire	The signature is expired

Error code	Error description
AuthFailure.SecretIdNotFound	The key does not exist
AuthFailure.SignatureFailure	Signature error
AuthFailure.TokenFailure	Token error
AuthFailure.InvalidSecretId	Invalid key (not a Cloud API key type)

5. Signature Demo

When calling API 3.0, you are recommended to use the corresponding Converge Cloud SDK 3.0, Swhich encapsulates the signature process, enabling you to focus on only the specific APIs provided by the product when developing. See SDK Center for more information. Currently, the following programming languages are supported:

- Python
- Java
- PHP
- Go
- Node

To further explain the signing process, we will use a programming language to implement the process described above. The request domain name, API and parameter values in the sample are used here. This goal of this example is only to provide additional clarification for the signature process, please see the SDK for actual usage.

The final output URL might be: https://cvm.convergecloud.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=luzon&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Signature=EliP9YW3pW28FpsEdkXt%2F%2BWcGeI%3D&Timestamp=1465185768&Version=2017-03-12

Note: The key in the example is fictitious, and the timestamp is not the current time of the system, so if this URL is opened in the browser or called using commands such as curl, an authentication error will be returned: Signature expired. In order to get a URL that can work properly, you need to replace the SecretId and SecretKey in the example with your real credentials and use the current time of the system as the Timestamp.

Note: In the example below, even if you use the same programming language, the order of the parameters in the URL may be different for each execution. However, the order does not matter, as long as all the parameters are included in the URL and the signature is calculated correctly.

Note: The following code is only applicable to API 3.0. It cannot be directly used in other signature processes. Even with an older API, signature calculation errors may occur due to the differences in details. Please refer to the corresponding documentation.

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.convergecloud.com/?");
        // When signing, the parameters need to be sorted in lexicographical order. TreeMap is used here
to guarantee the correct order.
        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.convergecloud.com/?");
        // There is no requirement for the order of the parameters in the actual request URL.
        for (String k : params.keySet()) {
            // The request string needs to be URL encoded. As the Key is all in English letters, only the valu
e is URL encoded here.
            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 enables automati
c sorting
        // A random number should be used when actually calling, for example: params.put("Nonce", new
Random().nextInt(java.lang.Integer.MAX_VALUE));
        params.put("Nonce", 11886); // Common parameter
        // The current time of the system should be used when actually calling, for example:   params.put
("Timestamp", System.currentTimeMillis() / 1000);
        params.put("Timestamp", 1465185768); // Common parameter
        params.put("SecretId", "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"); // Common parameter
        params.put("Action", "DescribeInstances"); // Common parameter
        params.put("Version", "2017-03-12"); // Common parameter
        params.put("Region", "luzon"); // Common parameter
        params.put("Limit", 20); // Business parameter
        params.put("Offset", 0); // Business parameter
        params.put("InstanceIds.0", "ins-09dx96dg"); // Business parameter
        params.put("Signature", sign(getStringToSign(params), "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE
", "HmacSHA1")); // Common parameter
        System.out.println(getUrl(params));
    }
}
```

Python

Note: If running in a Python 2 environment, the following requests dependency package must be installed first: 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.convergecloud.com"
    data = {
        'Action' : 'DescribeInstances',
        'InstanceIds.0' : 'ins-09dx96dg',
        'Limit' : 20,
        'Nonce' : 11886,
        'Offset' : 0,
        'Region' : 'luzon',
        '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"])
    # n actual invocation would occur here, which may incur fees after success
    # resp = requests.get("https://" + endpoint, params=data)
    # print(resp.url)
```

signaturev3

Converge Cloud The API will authenticate each access request, meaning that each request must include signature information (Signature) in the public request parameters to verify the requester's identity.
The signature information is generated by the security credentials, which include SecretId and SecretKey . If the user does not have security credentials, please apply for them on the Cloud API Key page, otherwise they cannot call the Cloud API interfaces.

1. Apply for security credentials.

Before using the Cloud API for the first time, please go to the Cloud API Key page to apply for a security credential.
Security credentials include SecretId and SecretKey:

- SecretId The security credentials are used to identify the identity of the API caller.
- SecretKey The secret key is used to encrypt and sign the string for server-side verification of the signature.
- Users must strictly protect their security credentials and avoid disclosure them.

The specific steps to apply for security credentials are as follows:

1. Log in to Converge Cloud Administration Center Console
2. Go to the console page for cloud API keys
3. On the Cloud API Key page, click New to create a pair of SecretId/SecretKey

Note: Developer accounts can have up to two pairs SecretId / SecretKey.

2. TC3-HMAC-SHA256 signature method

Note: For GET method, only Content-Type: application/x-www-form-urlencoded protocol format is supported. For POST method, Content-Type: application/json and Content-Type: multipart/form-data are currently supported. By default, all business interfaces are supported in json format. Only specific business interfaces are supported in multipart format. In this case, the interface cannot be called in json format. Refer to the specific business interface document description.

The following takes Cloud Virtual Machine querying Region-1 instance list as an example to introduce the signature calculation process step by step. We only use two parameters for the query instance list: Limit and Offset, called using the GET method.

Assume that the SecretId and SecretKey of the user are AKIDz 8krbsJ 5yKBZQpn 74WFkmLPx 3EXAMPLE and Gu 5t9xGARNpq 86cd 98joQYCN3EXAMPLE, respectively.

2.1. splice specification request string

Concatenate CanonicalRequest strings in the following format:

```
CanonicalRequest =
  HTTPRequestMethod + '\n' +
  CanonicalURI + '\n' +
  CanonicalQueryString + '\n' +
  CanonicalHeaders + '\n' +
  SignedHeaders + '\n' +
  HashedRequestPayload
```

- HTTPRequestMethod: HTTP request methods (GET, POST), GET in this example;
- CanonicalURI: URI parameter, API 3.0 fixed to forward slash (/);
- CanonicalQueryString: Query string in the URL that initiates the HTTP request. For POST requests, it is fixed as an empty string. For GET requests, it is the question mark (?) in the URL. The following string content, this example value is: Limit=10&Offset=0. Note: CanonicalQueryString needs to be URL encoded.
- CanonicalHeaders: The header information of participating signature, at least including host and content-type, can also be added with customized header to improve the uniqueness and security of its own request. Splicing rules: 1) head key and value are uniformly converted to lowercase, and the first and last spaces are removed, and spliced according to the format of key:value\n;2) multiple heads are spliced according to the dictionary sorting of head key (lowercase). In this example: content-type: application/x-www-form-urlencoded\nhost: cvm.convergecloud.com\n
- SignedHeaders: The header information involved in the signature indicates which headers participate in the signature of this request, and the header content contained in CanonicalHeaders is one-to-one corresponding. content-type and host are required headers. constructed as: 1) The head key is uniformly converted to lowercase; 2) Multiple header keys (lowercase) are concatenated according to dictionary sorting and separated by semicolons (;). In this case: content-type;host
- HashedRequestPayload: The hash value of the request body, calculated as Lowercase(HexEncode(Hash.SHA256(RequestPayload))), SHA256 hash the entire payload of the HTTP request body, then hexadecimal encoding, and finally converting the encoding string to lowercase letters. Note: For GET requests, RequestPayload is fixed as an empty string. For POST requests, RequestPayload is the payload of the HTTP request body.

According to the above rules, the resulting canonical request string in the example is as follows (for clarity, \nnewlines are replaced by a new line printed separately):

```
GET
```

```
/
Limit=10&Offset=0
content-type:application/x-www-form-urlencoded
host:cvm.convergecloud.com

content-type;host
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

2.2. Concatenate the string to be signed

Concatenate the string to be signed in the following format:

```
StringToSign =
  Algorithm + \n +
  RequestTimestamp + \n +
  CredentialScope + \n +
  HashedCanonicalRequest
```

- Algorithm: Signature algorithm, currently fixed as TC3-HMAC-SHA256;
- RequestTimestamp: Request timestamp, i.e. the X-TC-Timestamp value of the request header. The request in the example above is 1539084154;
- CredentialScope: Credential range in the format Date/service/tc3_request, containing date, requested service and termination string (tc3_request). **Date is the date of UTC standard time, the value needs to be consistent with UTC standard time converted by common parameter X-TC-Timestamp **;service is the product name, which must be consistent with the product domain name called, such as cvm. The above example request, the value is 2018-10-09/cvm/tc3_request;
- HashedCanonicalRequest: The hash value of the canonical request string obtained by concatenating the above steps is calculated by Lowercase(HexEncode(Hash.SHA256(CanonicalRequest))).

note:

> 1. Date must be calculated from timestamp X-TC-Timestamp and time zone UTC+0. Adding local time zone information to the system, such as East Zone 8, will cause calls to succeed during the day and night, but calls to fail in the early hours of the morning. Assuming the timestamp is 1551113065, the time in the East Eight District is 2019-02-26 00:44:25, but the calculated Date with UTC+0 should be 2019-02-25 instead of 2019-02-26.
> 2. Timestamp must be the current system time and ensure that the system time and standard time are synchronized. If the difference exceeds five minutes, it will fail. If it is not synchronized with the standard time for a long time, it may cause the request to fail after running for a period of time (return signature expiration error).

According to the above rules, the string to be signed in the example is as follows (for clarity,\nnewlines are

replaced by new lines printed):

```
TC3-HMAC-SHA256
1539084154
2018-10-09/cvm/tc3_request
91c9c192c14460df6c1ffc69e34e6c5e90708de2a6d282cccf957dbf1aa7f3a7
```

2.3. calculate the signature

1. Compute the derived signature key, pseudocode as follows

```
SecretKey = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"
SecretDate = HMAC_SHA256("TC3" + SecretKey, Date)
SecretService = HMAC_SHA256(SecretDate, Service)
SecretSigning = HMAC_SHA256(SecretService, "tc3_request")
```

- SecretKey: Original SecretKey;
- Date: That is, the Date field information in Credential, as shown in the example above, is 2018-10-09.;
- Service: That is, the Service field information in Credential, as shown in the example above, is cvm;

2. Calculate the signature, pseudocode as follows

```
Signature = HexEncode(HMAC_SHA256(SecretSigning, StringToSign))
```

- SecretSigning: That is, the derivative signature key calculated above;
- StringToSign: That is, the character string to be signed calculated in step 2;

2.4. Splicing Authorization

Splice as follows Authorization:

```
Authorization =
    Algorithm + ' ' +
    'Credential=' + SecretId + '/' + CredentialScope + ', ' +
    'SignedHeaders=' + SignedHeaders + ', '
    'Signature=' + Signature
```

- Algorithm: Signature method, fixed as TC3-HMAC-SHA256;
- SecretId: SecretId in key pair;
- CredentialScope: See above, Scope of Voucher;
- SignedHeaders: See above, header information for participating signatures;
- Signature: signature value

According to the above rules, the values obtained in the example are:

```
TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
```

The final complete invocation information is as follows:

```
https://cvm.convergecloud.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.convergecloud.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: luzon
```

3. signing failed

According to the actual situation, there are the following signature failure error codes, please handle according to the actual situation

error code	error description
AuthFailure.SignatureExpire	signature expiration
AuthFailure.SecretIdNotFound	key is not present
AuthFailure.SignatureFailure	signature error
AuthFailure.TokenFailure	token error
AuthFailure.InvalidSecretId	Illegal key (not cloud API key type)

4. Signature Demo

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.convergecloud.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.convergecloud.com";
        String region = "luzon";
        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");
        // Pay attention to the time zone, otherwise it is easy to make mistakes.
        sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
        String date = sdf.format(new Date(Long.valueOf(timestamp + "000")));

        // ************* Step 1: Assemble the specification request string *************
```

```
        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);

        // ************* Step 2: Stitching the string to be signed *************
        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);

        // ************* Step 3: Calculate the signature *************
        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);

        // ************* Step 4: Splicing 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

# key parameters
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

service = "cvm"
host = "cvm.convergecloud.com"
endpoint = "https://" + host
region = "luzon"
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}

# ************* Step 1: Assemble the specification request string *************
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)

# ************* Step 2: Stitching the string to be signed *************
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)
```

```
# ************* Step 3: Calculate the signature *************
# Compute signature digest function
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)

# ************* Step 4: Splicing Authorization *************
authorization = (algorithm + " " +
                 "Credential=" + secret_id + "/" + credential_scope + ", " +
                 "SignedHeaders=" + signed_headers + ", " +
                 "Signature=" + signature)
print(authorization)

# Common parameters added to request header
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,
}
```

request

1. Service Address

Region refers to the geographical area of a physical data center. Converge Cloud ensures complete isolation between different regions, providing maximum stability and fault tolerance. To reduce access latency and improve download speed, it is recommended to choose the region closest to your customers.

You can view the complete region list by using the API interface "DescribeRegions".

2. Communications Protocol

All the Converge Cloud APIs communicate via HTTPS, providing highly secure communication tunnels.

3. Request Methods

Supported HTTP request methods:

- POST (recommended)
- GET

PThe Content-Type types supported by POST requests:

- application/json (recommended). The TC3-HMAC-SHA256 signature algorithm must be used.
- application/x-www-form-urlencoded. The HmacSHA1 or HmacSHA256 signature algorithm must be used.
- multipart/form-data (only supported by certain APIs). You must use TC3-HMAC-SHA256 to calculate the signature.

The size of a GET request packet is up to 32 KB. The size of a POST request is up to 1 MB when the HmacSHA1 or HmacSHA256 signature algorithm is used, and up to 10 MB when TC3-HMAC-SHA256 is used.

4. Character Encoding

Only UTF-8 encoding is used.

result

Response for Successful Requests

For example, when calling CAM API (version: 2017-03-12) to view the status of instances (DescribeInstancesStatus), if the request has succeeded, you may see the response as shown below:


```
{
    "Response": {
        "TotalCount": 0,
        "InstanceStatusSet": [],
        "RequestId": "b5b41468-520d-4192-b42f-595cc34b6c1c"
    }
}
```


- The API will return Response, which contains RequestId, as long as it processes the request. It does not matter if the request is successful or not.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.
- Except for the fixed fields, all fields are action-specified. For the definitions of action-specified fields, see the corresponding API documentation. In this example, TotalCount and InstanceStatusSet are the fields specified by the API DescribeInstancesStatus. 0 TotalCount means that the requester owns 0 CVM instance so the InstanceStatusSet is empty.

Response for Failed Requests

If the request has failed, you may see the response as shown below:


```
{
    "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"
    }
}
```


- The presence of the Error field indicates that the request has failed. A response for a failed request will include Error, Code and Message fields.

- Code is the code of the error that helps you identify the cause and solution. There are two types of error codes so you may find the code in either common error codes or API-specified error codes.
- Message explains the cause of the error. Note that the returned messages are subject to service updates. The information the messages provide may not be up-to-date and should not be the only source of reference.
- RequestId is the unique ID of an API request. Contact us with this ID when an exception occurs.

Common Error Codes

If there is an Error field in the response, it means that the API call failed. The Code field in Error indicates the error code. The following table lists the common error codes that all actions can return.

Error Code	Description
AuthFailure.InvalidSecretId	Invalid key (not a API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	The key does not exist.
AuthFailure.SignatureExpire	Signature expired.
AuthFailure.SignatureFailure	Signature error.
AuthFailure.TokenFailure	Token error.
AuthFailure.UnauthorizedOperation	The request does not have CAM authorization.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
LimitExceeded	Quota limit exceeded.
MissingParameter	A parameter is missing.
NoSuchVersion	The API version does not exist.

Error Code	Description
RequestLimitExceeded	The number of requests exceeds the frequency limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	hHTTPS request method error. Only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

PublicParameter

Common parameters are parameters used to identify users and interface authentication purposes. If not necessary, these parameters are not described in the separate interface document of each interface, but these parameters need to be carried in each request before the request can be normally initiated.

signature method v3

When using TC3-HMAC-SHA256 signature method, the common parameters need to be uniformly placed in the HTTP Header request header, as follows:

parameter name	type	required	described
X-TC-Action	String	Yes	The name of the operation interface. Refer to the description of the public parameter Action in the input parameters of the interface documentation for the value. For example, the value for the query instance list interface of the cloud server is DescribeInstances.
X-TC-Region	String	Yes	region parameters, Data used to identify which region you wish to operate on. The region value accepted by the interface refers to the description of the input parameter common parameter Region in the interface document. Note: Some interfaces do not need to pass this parameter, which is specifically stated in the interface documentation. In this case, even passing this parameter will not take effect.
X-TC-Timestamp	Integer	Yes	The current UNIX timestamp, which records the time when the API request was initiated. for example 1529223702. Note: If the time difference from the server exceeds 5 minutes, it will cause a signature expiration error.
X-TC-Version	String	Yes	Version of API for operation. Refer to the description of the public parameter Version in the interface document for the value. For example, the version of the cloud server. 2017-03-12.
Authorization	String	Yes	HTTP The standard authentication header field is "Authorization". For example: TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=fe5f80f77d5fa3beca038a248ff027d0445342fe2855ddc963176630326f1024 Here, - TC3-HMAC-SHA256: Signature method, currently fixed as this value, - Credential: Credential: Signature credential; AKIDEXAMPLE is the SecretId; Date is a date in UTC time, and this value must match the value of X-TC-Timestamp (a common parameter) in UTC time format; service is the name of the product/service, and is generally a domain name prefix. For example,cvm; - SignedHeaders: The headers that contains the authentication information; content-type and host are the required headers; - Signature: Signature digest.
X-TC-Token	String	No	The token used for temporary certificates needs to be used in conjunction with a temporary key. Temporary keys and tokens need to be obtained by calling the access management service interface. Long-term keys do not require tokens.

signature method v1

When using HmacSHA1 and HmacSHA256 signature methods, common parameters need to be placed uniformly in the request string, as follows

parameter name	type	required	described
Action	String	Yes	The name of the interface to be operated. The value refers to the explanation of the public parameter Action in the interface documentation. For example, for the cloud server's query instance list interface, the value is DescribeInstances .
Region	String	Yes	The region parameter is used to identify which region's data you want to operate on. The region value accepted by the interface is specified in the input parameter of the public parameter Region in the interface documentation. Note: Some interfaces do not require this parameter to be passed, which will be specifically mentioned in the interface documentation. Even if this parameter is passed, it will not take effect in this case.
Timestamp	Integer	Yes	The current UNIX timestamp, which can record the time when the API request is initiated. For example, 1529223702. If the difference between the current time is too large, it will cause a signature expiration error.
Nonce	Integer	Yes	A random positive integer combined with Timestamp is used to prevent replay attacks.
SecretId	String	Yes	The SecretId is an identifier applied for the cloud API key to identify the user's identity. A SecretId corresponds to a unique SecretKey , and the SecretKey is used to generate the request signature Signature .
Signature	String	Yes	Request signature is used to verify the legitimacy of this request. Users need to calculate it based on the actual input parameters. The specific calculation method can be found in the interface authentication documentation.
Version	String	Yes	The version of the API being operated on. The value refers to the description of the public parameter Version in the interface documentation. For example, the version of the cloud server. 2017-03-12.
SignatureMethod	String	No	Signature method, currently supports HmacSHA256 and HmacSHA1. HmacSHA256 algorithm is used to verify signatures only if this parameter is specified as HmacSHA 256, otherwise HmacSHA1 is used to verify signatures.
Token	String	No	Token used for temporary certificate needs to be used together with temporary key. The temporary key and Token need to be obtained from the Access Management service invocation interface. Long-term keys do not require tokens.

zone list

A region (Region) refers to the geographical area of a physical data center. Converge Cloud Translation: To deliver verification that completely isolates different regions, ensuring maximum stability and fault tolerance between regions. In order to reduce access latency and improve download speed, it is recommended that you choose the region closest to your customers.

You can view the complete region list by using the API interface Query Region List.

Advanced Defense APIs CreateMaWorkloadLabel

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to create a micro-alarm workload tag.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateMaWorkloadLabel
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
LabelIds	Yes	No	Array of Int64	List of tag IDs. Example: [1]
WorkloadIds	Yes	No	Array of Int64	Load ID list. Example: [1]

3. Output Parameters

Parameter	Type	Description

name		
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

CreateProtectServer

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for adding website servers for protection

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateProtectServer
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ProtectDir	Yes	No	String	Address of the protection directory. Example: /var/www
ProtectHostConfig	Yes	No	Array of ProtectHostConfig	Information about servers to protect. Example:View

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

DeleteAttackLogs

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for deleting cyberattack log entries

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-10 10:14:54.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteAttackLogs
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	No	No	Array of Uint64	IDs of log entries. You can specify up to 100 log entries in each request. Example: [1]
IsAll	No	No	Bool	Delete All or Not Example: true

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DeleteMaConnEvent

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete the micro-alarm access events.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteMaConnEvent
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
DeleteIds	Yes	No	Array of Uint64	Deleted event ID set. Example: [1]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DeleteMaCustomPolicy

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete the micro-alarm custom allowlist.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteMaCustomPolicy
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
DeleteIds	Yes	No	Array of Uint64	Deleted custom allowlist policy list. Example: [1]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DeleteMaLabel

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete micro-alarm tags.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteMaLabel
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Int64	Tag ID. Example: [1]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DeleteMaSelfLearnPolicy

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete the micro-alarm self-learning sub-policy.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteMaSelfLearnPolicy
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
DeleteUniqueIds	Yes	No	Array of String	Deleted unique ID collection for the self-learning sub-policy. Example: ["32454"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DeleteMaWhitelist

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete the micro-alarm global allowlist.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteMaWhitelist
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
DeleteIds	Yes	No	Array of Uint64	Deleted configuration ID set of the global allowlist. Example: [1]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DeleteProtectDir

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for removing websites from protection

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteProtectDir
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of String	IDs of up to 100 directories to remove. Example: ["/root/","/tmp"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

DeleteWebPageEventLog

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete event records in the web page anti-tampering module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteWebPageEventLog
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	IDs of up to 100 events that you want to delete. Example: [1,2,3,4]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

DescribeAttackEventInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Yunapi Response

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAttackEventInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	Uint64	Event ID. Example: 49754647

3. Output Parameters

Parameter name	Type	Description
NetAttackEventInfo	NetAttackEventInfo	Details of Network Attack Events Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeAttackEvents

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Yunapi Response

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAttackEvents
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Sorting field, which can be Count or MergeTime. Example: MergeTime
Filters	No	No	Array of Filter	Filter criteria. • Type - String Attack Status 0: Attack Attempt 1: Successful Attack - Required or Not: No • Status - String Event Handling Status 0: Pending 1: Handled 2: Allowlisted 3: Ignored 4: Deleted - Required or Not: No • SrcIP - String Source IP - Required or Not: No • Uuids - String Host Security UUID - Required or Not: No • Quuids - String CVM UUID - Required or Not: No • DstPort - String Target Attack Port - Required or Not: No • MachineName - String Host Name - Required or Not: No • InstanceID - String Host Instance ID - Required or Not: No • AttackTimeBegin - String Attack Start Time - Required or Not: No • AttackTimeEnd - String Attack End Time - Required or Not: No • VulSupportDefense - String Vulnerability Defense Support Status 0 Unsupported, 1 Supported - Required or Not: No Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sort method: ASC, DESC. Example: DESC

3. Output Parameters

Parameter name	Type	Description
List	Array of NetAttackEvent	Attack Event List Example:View
TotalCount	Uint64	Total number. Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeAttackLogInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying cyberattack log details

Default interface request rate limit: 20 times per second.

Interface update time: 2022-10-31 15:59:56.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAttackLogInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	Uint64	Log ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
CreatedAt	String	Attack time. Example: 2020-12-12 10:10:00

Parameter name	Type	Description
DstIp	String	Target IP address of the attack. Example: 192.168.0.1
DstPort	Uint64	Target port of the attack. Example: 8080
HttpCgi	String	Attack path. Example: any attack path
HttpContent	String	Attack content. Example: any content
HttpHead	String	Attack header information. Example: POST /was-wsdft/CoofatorPorasdtType ..
HttpHost	String	Target server of the attack. Example: domain.com
HttpMethod	String	Attack method. Example: POST
HttpParam	String	Attack parameter. Example: anyp=anyv
HttpReferer	String	Request referer. Example: http://domian.com/any
HttpUserAgent	String	Browser identifier of the attacker. Example: ie
Id	Uint64	Log ID. Example: 1
Quuid	String	Server ID. Example: 1
SrcIp	String	Source IP address of the attack. Example: 192.168.0.1
SrcPort	Uint64	Source port of the attack. Example: 8080
VulType	String	Threat type. Example: 1

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAttackLogs

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query cyberattack log entries by pages.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAttackLogs
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter conditions. • HttpMethod - String - Required: No - Attack method, which can be POST or GET. • DateRange - String - Required: No - Time range (for storing data of the last 3 months). For example, the time range is ["2019-11-17", "2019-12-17"] for the last month. • VulType - String - Required: No - Threat type. • SrcIp - String - Required: No - Attack source IP address. • SrcPort - String - Required: No - Attack source port. • DstPort - String - Required: No - Attack destination port. Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Quuid	No	No	String	ID of the cloud server. Example: quuid
Uuid	No	No	String	CWP agent ID. Example: uuid

3. Output Parameters

Parameter name	Type	Description
AttackLogs	Array of DefendAttackLog	List of logs. Example:View
TotalCount	Uint64	Total number. Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.

Error Code	Description
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAttackStatistics

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Yunapi Response

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAttackStatistics
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
AttackSrcIpCount	Uint64	Total Number of Attack Source IPs Example: 0
AttackedAssetCount	Uint64	Total Number of Assets Under Attack Example: 0

Parameter name	Type	Description
AttackedPortCount	Uint64	Total Number of Attacked Ports Example: 0
NewAttackSrcIpCount	Uint64	Number of New Attacking Source IPs Today Example: 0
NewAttackedAssetCount	Uint64	Number of New Attacked Assets Today Example: 0
NewAttackedPortCount	Uint64	Number of New Attacked Ports Today Example: 0
PendingAttackCount	Uint64	Total Number of Attacks Example: 0
PendingNewAttackCount	Uint64	Number of New Attacks Today Example: 0
PendingSuccAttackCount	Uint64	Total Number of Successful Attacks Example: 0
PendingTryAttackCount	Uint64	Total Attack Attempts Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeAttackTop

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Yunapi Response

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAttackTop
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter criteria. • BeginTime - String Start time, last 7 days by default - Required or Not: No . Example:View

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
NetAttackTopInfo	NetAttackTopInfo	Top Statistics Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeAttackTrends

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Yunapi Response

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAttackTrends
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter criteria. • BeginTime - String Start time, last 7 days by default - Required or Not: No . Example:View

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
NetAttackTrend	Array of NetAttackTrend	Attack Trend Statistics (Days) Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeAttackVulTypeList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the risk types of cyberattacks

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAttackVulTypeList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
List	Array of String	List of risk types. Example: ["Command injection", "fastjson command execution", "Unusual threat types"]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DescribeMaConnEventList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the micro-alarm access events.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMaConnEventList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Optional sorting columns: [CreateTime and ModifyTime]. Example: CreateTime
Filters	No	No	Array of Filter	• Type - int64 - Required: Yes - Access type • WorkloadName - string - Required: No - Workload name • SrcWorkloadName - string - Required: No - Source workload name • DestWorkloadName - string - Required: No - Target workload name • SrcIP - string - Required: No - Source IP • DestIP - string - Required: No - Target IP • StartTime string - Required: No - Start time • EndTime string - Required: No - End time • TimeMode int - Required: Yes - Time selection [0: Today; 1: This week; 2: Last week; 3: The week before last; 4: Past half year] Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
List	Array of	Access event set.

Parameter name	Type	Description
	MaConnEvent	Example:View
TotalCount	Int64	Total number. Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMaCustomPolicyList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the micro-alarm custom allowlist.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMaCustomPolicyList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Optional sorting columns: [CreateTime and ModifyTime]. Example: CreateTime
Filters	No	No	Array of Filter	• SrcLabelId - string - Required: No - Source tag ID • SrcLabelKey - string - Required: No - Source tag key • SrcLabelValue - string - Required: No - Source tag value • DestLabelId - string - Required: No - Target tag ID • DestLabelKey - string - Required: No - Target tag key • DestLabelValue - string - Required: No - Target tag value • SrcIP - string - Required: No - Source IP • DestIP - string - Required: No - Target IP • Enable - int64 - Required: No - Enabled or not • Updater - string - Required: No - Creator/Updater • Name - string - Required: No - Custom allowlist name Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
List	Array of MaCustomPolicy	Custom allowlist policy set. Example:View
TotalCount	Int64	Total number. Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMaGlobalConf

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the micro-alarm global configuration.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMaGlobalConf
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
Data	MaGlobalConf	Global Configuration Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMaHostList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the micro-alarm server list.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMaHostList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: [CreateTime] Example: CreateTime
Filters	No	No	Array of Filter	• Name - string - Required: No - Server name • Id - string - Required: No - Server ID • InstanceId - string - Required: No - Instance ID • Ip - string - Required: No - IP address • OsType - string - Required: No - Operating system • VpcId - string - Required: No - Corresponding network • Region - string - Required: No - Region • Label - string - Required: No - Associated tag • IsEnable - string - Required: No - Monitoring status Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
List	Array of MaHost	Server list Example:View
TotalCount	Int64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMaLabel

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the micro-alarm tag information.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMaLabel
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	Int64	Tag ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
Label	MaLabel	Tag Example:View

Parameter name	Type	Description
WorkloadIds	Array of Int64	Tag-associated workload ID list. Example: [1]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMaLabelList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the micro-alarm tag list.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMaLabelList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	• Source - string - Required: No - Tag source • Id - string - Required: No - Tag ID • Label - string - Required: No - Tag key or value Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
List	Array of MaLabel	Tag List Example:View
TotalCount	Int64	Total number. Example: 10

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMaLabelSourceList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the micro-alarm tag source list.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMaLabelSourceList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
List	Array of String	Tag source list. Example: ["any-source"]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMaPodList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the micro-alarm pod list.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMaPodList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: [CreateTime] Example: CreateTime
Filters	No	No	Array of Filters	• Name - string - Required: No - Pod name • Id - string - Required: No - Pod ID • Ip - string - Required: No - IP address • Status - string - Required: No - Pod status • ClusterId - string - Required: No - Cluster ID • ClusterName - string - Required: No - Cluster name • Label - string - Required: No - Associated tag • IsEnabled - string - Required: No - Monitoring status Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
List	Array of MaPod	Pod List Example:View
TotalCount	Int64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMaSelfLearnConfig

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the micro-alarm self-learning policy.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMaSelfLearnConfig
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
Enable	Uint64	Whether self-learning is enabled. • 0: Not enabled • 1: Enabled Example: 1

Parameter name	Type	Description
HostCount	Uint64	Number of server workloads with learning enabled. Example: 1
LearnConfID	Uint64	Self-learning configuration ID. Example: 1
LearnEndDate	String	End time of learning. Example: 2023-10-11
LearnStartDate	String	Start time of learning. Example: 2023-10-10
PodCount	Uint64	Number of pod workloads with learning enabled. Example: 1
RemainingDay	Float	Remaining days of learning. Example: 1.0
Status	Uint64	Self-learning status. • 0: Learning • 1: Learning completed Example: 1
SubPolicyCount	Uint64	Number of sub-policies for self-learning. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.

Error Code	Description
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMaSelfLearnPolicyList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the micro-alarm self-learning sub-policy list.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMaSelfLearnPolicyList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Optional sorting columns: [CreateTime and ModifyTime]. Example: CreateTime
Filters	No	No	Array of Filter	• SrcLabelId - string - Required: No - Source tag ID • SrcLabelKey - string - Required: No - Source tag key • SrcLabelValue - string - Required: No - Source tag value • DestLabelId - string - Required: No - Target tag id • DestLabelKey - string - Required: No - Target tag key • DestLabelValue - string - Required: No - Target tag value • SrcIP - string - Required: No - Source IP • DestIP - string - Required: No - Target IP • UniqueId - string - Required: No - Unique ID for the self-learning sub-policy Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
List	Array of MaSelfLearnPolicy	Self-learning sub-policy set. Example:View
TotalCount	Int64	Total number. Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMaSummary

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the micro-alarm overall summary.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMaSummary
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
CustomPolicyCount	Uint64	Number of custom allowlist policies deprecated. Example: 1
EnableCustomPolicyCount	Uint64	Total number of custom allowlist policies enabled. Example: 0
EnableHostWorkloadCount	Uint64	Number of server workloads with monitoring enabled. Example: 1

Parameter name	Type	Description
EnablePodWorkloadCount	Uint64	Number of pod workloads with monitoring enabled. Example: 1
EnableWorkloadCount	Uint64	Number of workloads with monitoring enabled. Example: 1
GlobalWhitelistEnable	Uint64	Whether the global allowlist is enabled. • 0: Disabled • 1: Enabled Example: 1
HostWorkloadCount	Uint64	Number of server workloads. Example: 1
MonitorEnable	Uint64	Whether the monitoring switch is enabled. • 0: Disabled • 1: Enabled Example: 1
PodWorkloadCount	Uint64	Number of pod workloads. Example: 1
SelfLearnEnable	Uint64	Whether self-learning is enabled. • 0: Disabled • 1: Enabled Example: 1
TodayNewAlarmEventCount	Uint64	Number of new alarm events today. Example: 0
TotalCustomPolicyCount	Uint64	Total number of custom allowlist policies enabled and disabled. Example: 1
WhitelistCount	Uint64	Number of global allowlists. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMaWhitelist

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the micro-alarm global allowlist.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMaWhitelist
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Optional sorting columns: [CreateTime and ModifyTime]. Example: CreateTime
Filters	No	No	Array of Filter	• From - string - Required: No - Allowlist source • Enable - int64 - Required: No - Enabled or not • Updater - string - Required: No - Creator • Name - string - Required: No - Allowlist name Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
Enable	Int64	Whether it is enabled entirely. • 0: Not enabled • 1: Enabled Example: 1
List	Array of MaWhitelist	Configuration set of the global allowlist. Example:View
TotalCount	Int64	Total number. Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMaWorkloadLabel

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the micro-alarm workload tag.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMaWorkloadLabel
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	Int64	Workload ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
List	Array of MaLabel	Tag List Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMaWorkloadList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the micro-alarm workload list.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMaWorkloadList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	• Name - string - Required: No - Workload name • Type - string - Required: No - Workload type [0: Server; 1: Pod] • Id - string - Required: No - Workload ID • Ip - string - Required: No - IP address • IpRange - string - Required: No - IP range [10.1.1.1-10.2.2.2
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
List	Array of MaWorkload	List Example:View
TotalCount	Int64	Total number. Example: 10

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMachineList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the servers in a region for the web page anti-tampering feature.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMachineList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of AssetFilters	Filter condition. • Keywords - String - Required: no - query keywords. • Status - String - Required: No - Connection status of the agent. OFFLINE: disconnected. ONLINE: connected. UNINSTALLED: not installed. • Version - String Required: no - current protection version (PRO_VERSION: professional
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
MachineRegion	Yes	No	String	Region of a server. Example: ap-region1
MachineType	Yes	No	String	Cloud host type. • CVM: cloud virtual machine. • BM: BM. • ECM: Edge Computing Machine • LH: Lighthouse instance • Other: hybrid cloud server Example: CVM
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
Machines	Array of Machine	Server list Example:View
TotalCount	Uint64	Number of hosts. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
FailedOperation.APIServerFail	Failed to call the API service.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeNetAttackSetting

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Yunapi Response

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeNetAttackSetting
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]

3. Output Parameters

Parameter name	Type	Description
AutoInclude	Uint64	New assets automatically include: 0 - Do not include, 1 - include Example: 1
ExcludeInstanceIds	Array of String	Custom Hosts to Exclude Example: ["d92d7"]
InstanceIds	Array of String	Specified servers Example: ["ins-d92d72"]
NetAttackAlarmStatus	Uint64	0: New warning events pending processing by default, 1: New warning events processed by default, 3: New warning events ignored by default. Example: 1
NetAttackEnable	Uint64	0 - Disable Network Attack Detection; 1 - Enable Network Attack Detection. Example: 1
Scope	Uint64	1 - All Premium Edition Hosts, 0 - Hosts in InstanceIds List Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeProtectDirList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the protected directory list in the web page anti-tampering module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeProtectDirList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Sorting field. Valid values: ProtectServerNum, NoProtectServerNum, LatestProtectTime, and RelatedServerNum. Example: ProtectServerNum
Filters	No	No	Array of AssetFilters	DirName: website name. DirPath: protected website directory. Example:View
Limit	Yes	No	Uint64	Maximum number of entries to return on each page. Maximum value: 100. Example: 10
Offset	Yes	No	Uint64	Offset. Example: 1
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc

3. Output Parameters

Parameter name	Type	Description
List	Array of ProtectDirInfo	Information about protected directories. Example:View
TotalCount	Uint64	Total number. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.

Error Code	Description
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeProtectDirRelatedServer

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the servers associated with a protected directory.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeProtectDirRelatedServer
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Example: LatestProtectTime
Filters	No	No	Array of Filter	Filtering parameter. Valid value: ProtectStatus. Example:View
Id	Yes	No	String	Unique ID. Example: 1
Limit	Yes	No	Uint64	Maximum number of entries to return on each page. Maximum value: 100. Example: 10
Offset	Yes	No	Uint64	Offset. Example: 0
Order	No	No	String	Sorting method. Example: asc

3. Output Parameters

Parameter name	Type	Description
List	Array of ProtectDirRelatedServer	Information about servers associated with the website. Example:View
ProtectServerCount	Uint64	Total number of protected servers. Example: 12
TotalCount	Uint64	Total number. Example: 12
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeServerRelatedDirInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the details of directories associated with a server.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeServerRelatedDirInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	Uint64	Unique ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
HostIp	String	Server IP. Example: 10.0.0.1

Parameter name	Type	Description
HostName	String	Server name. Example: redis_node_cvm
ProtectDirNum	Uint64	Number of protected directories. Example: 1
ProtectFileNum	Uint64	Number of protected files. Example: 1
ProtectLinkNum	Uint64	Number of protected soft links. Example: 1
ProtectTamperNum	Uint64	Number of web pages protected by anti-tampering. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeWebPageEventList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying tampering events

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeWebPageEventList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: CreateTime and RestoreTime. Default value: CreateTime. Example: CreateTime
Filters	No	No	Array of AssetFilters	Filter condition. • IpOrAlias - String - Required: no - host IP or alias filter. • EventType - String - Required: No - Event type. • EventStatus - String - Required: No - Event status. Example:View
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	Uint64	Sorting order. 0: descending order. 1: ascending order. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
List	Array of ProtectEventLists	List of protection events. Example:View
TotalCount	Uint64	Total number. Example: 1

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeWebPageGeneralize

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the overview information about web page anti-tampering.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeWebPageGeneralize
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
ProtectDirNum	Uint64	Number of protected directories. Example: 1
ProtectFileNum	Uint64	Number of protected files. Example: 1
ProtectHostNum	Uint64	Number of protected servers. Example: 1

Parameter name	Type	Description
ProtectMonitor	Uint64	Status of protection and monitoring. 0: not enabled. 1: enabled. 2: abnormal. Example: 1
ProtectToday	Uint64	Number of protected items on the current day. Example: 1
TamperFileNum	Uint64	Number of files that have been tampered with. Example: 1
TamperNum	Uint64	Number of tampering attacks. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DescribeWebPageProtectStat

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the dynamic protection information in the web page anti-tampering module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeWebPageProtectStat
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
FileTamperNum	Array of ProtectStat	File tampering information. Example:View
ProtectFileType	Array of ProtectStat	Information about protected file types. Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DescribeWebPageServiceInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the purchase information about the web page anti-tampering service and the relevant server information.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeWebPageServiceInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
AllAuthorizedMachines	Array of ProtectMachineInfo	Information about all licensed servers. Example:View
BuyNum	Uint64	Number of purchased licenses. Example: 1
ExpireAuthorizedMachines	Array of ProtectMachine	Information about servers with licenses that are about to expire. Example:View
ExpireNum	Uint64	Number of licenses that is about to expire. Example: 1
ExpiredNum	Uint64	Number of expired licenses. Example: 1

Parameter name	Type	Description
ProtectDirNum	Uint64	Number of protected directories. Example: 1
ResidueNum	Uint64	Number of available licenses. Example: 1
Status	Bool	Indicates whether the service is purchased. true: yes. false: no. Example: true
UsedNum	Uint64	Number of used licenses. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DisableSelfLearn

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to disable micro-alarm self-learning.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DisableSelfLearn
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
CloseMonitor	Yes	No	Uint64	Whether to synchronously turn off the monitoring switch. • 0 - Don't turn off • 1 - Turn off Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ExportAttackEvents

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Yunapi Response

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportAttackEvents
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid value: CreateTime. Example: CreateTime
Filters	No	No	Array of Filters	Filter criteria. • Type - String Attack Status 0: Attack Attempt 1: Successful Attack - Required or Not: No • Status - String Event Handling Status 0: Pending 1: Handled 2: Allowlisted 3: Ignored 4: Deleted - Required or Not: No • SrcIP - String Source IP - Required or Not: No • Uuids - String Host Security UUID - Required or Not: No • Quuids - String CVM UUID - Required or Not: No • DstPort - String Target Attack Port - Required or Not: No • MachineName - String Host Name - Required or Not: No • InstanceID - String Host Instance ID - Required or Not: No • AttackTimeBegin - String Attack Start Time - Required or Not: No • AttackTimeEnd - String Attack End Time - Required or Not: No • VulSupportDefense - String Vulnerability Defense Support Status 0 Unsupported, 1 Supported - Required or Not: No Example:View
Order	No	No	String	Sorting order. Valid values: ASC and DESC. Example: ASC

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ExportAttackLogs

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting cyberattack logs

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:34.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportAttackLogs
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter conditions. • HttpMethod - String - Required: No - Attack method, which can be POST or GET. • DateRange - String - Required: No - Time range (for storing data of the last 3 months). For example, the time range is ["2019-11-17", "2019-12-17"] for the last month. • VulType - String - Required: No - Threat type. • SrcIp - String - Required: No - Attack source IP address. • SrcPort - String - Required: No - Attack source port. • DstPort - String - Required: No - Attack destination port. Example:View
Quuid	No	No	String	ID of the cloud server. Example: 5a540076-d38a-4078-aa98-qwert371d322
Uuid	No	No	String	CWP agent ID. Example: 5a540076-d38a-4078-aa98-qwert371d322

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	Deprecated parameter. Example: http://domain.com/anypath/x
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 101
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
FailedOperation.Export	Failed to export.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ExportMaConnEventList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export the micro-alarm access events.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportMaConnEventList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Optional sorting columns: [CreateTime, ModifyTime and MatchCount]. Example: CreateTime
Filters	No	No	Array of Filter	• Type - int64 - Required: Yes - Access type • WorkloadName - string - Required: No - Workload name • SrcWorkloadName - string - Required: No - Source workload name • DestWorkloadName - string - Required: No - Target workload name • SrcIP - string - Required: No - Source IP • DestIP - string - Required: No - Target IP • StartTime string - Required: No - Start time • EndTime string - Required: No - End time • TimeMode int - Required: Yes - Time selection [0: Today; 1: This week; 2: Last week; 3: The week before last; 4: Past half year] Example:View
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 101
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ExportMaCustomPolicyList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export the micro-alarm custom allowlist.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportMaCustomPolicyList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Optional sorting columns: [CreateTime and ModifyTime]. Example: CreateTime
Filters	No	No	Array of Filter	• SrcLabelId - string - Required: No - Source tag ID • SrcLabelKey - string - Required: No - Source tag key • SrcLabelValue - string - Required: No - Source tag value • DestLabelId - string - Required: No - Target tag ID • DestLabelKey - string - Required: No - Target tag key • DestLabelValue - string - Required: No - Target tag value • SrcIP - string - Required: No - Source IP • DestIP - string - Required: No - Target IP • Enable - int64 - Required: No - Enabled or not • Updater - string - Required: No - Creator/Updater • Name - string - Required: No - Custom allowlist name Example:View
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 101
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ExportMaHostList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export the micro-alarm server list.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportMaHostList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	• Name - string - Required: No - Server name • Id - string - Required: No - Server ID • InstanceId - string - Required: No - Instance ID • Ip - string - Required: No - IP address • OsType - string - Required: No - Operating system • VpcId - string - Required: No - Corresponding network • Region - string - Required: No - Region • Label - string - Required: No - Associated tag • IsEnable - string - Required: No - Monitoring status

Parameter name	Required	Allow NULL	Type	Description
				Example:View

3. Output Parameters

Parameter name	Type	Description
TaskId	Int64	ID of the export task. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ExportMaPodList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export the micro-alarm pod list.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportMaPodList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	• Name - string - Required: No - Pod name • Id - string - Required: No - Pod ID • Ip - string - Required: No - IP address • Status - string - Required: No - Pod status • ClusterId - string - Required: No - Cluster ID • ClusterName - string - Required: No - Cluster name • Label - string - Required: No - Associated tag • IsEnabled - string - Required: No - Monitoring status Example:View

3. Output Parameters

Parameter name	Type	Description
TaskId	Int64	ID of the export task. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ExportMaSelfLearnPolicyList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Export Micro Alert Self-learning Sub-policy

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportMaSelfLearnPolicyList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Optional sorting columns: [CreateTime and ModifyTime]. Example: CreateTime
Filters	No	No	Array of Filter	• SrcLabelId - string - Required: No - Source tag ID • SrcLabelKey - string - Required: No - Source tag key • SrcLabelValue - string - Required: No - Source tag value • DestLabelId - string - Required: No - Target tag id • DestLabelKey - string - Required: No - Target tag key • DestLabelValue - string - Required: No - Target tag value • SrcIP - string - Required: No - Source IP • DestIP - string - Required: No - Target IP • UniqueId - string - Required: No - Unique ID for the self-learning sub-policy Example:View
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 101
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ExportMaWhitelist

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export the micro-alarm global allowlist.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportMaWhitelist
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Optional sorting columns: [CreateTime and ModifyTime]. Example: CreateTime
Filters	No	No	Array of Filter	• From - string - Required: No - Allowlist source • Enable - int64 - Required: No - Enabled or not • Updater - string - Required: No - Creator • Name - string - Required: No - Allowlist name Example:View
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 101

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ExportProtectDirList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export protected directories in the web page anti-tampering module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportProtectDirList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Sorting field. Valid values: ProtectServerNum, NoProtectServerNum, LatestProtectTime, and RelatedServerNum. Example: ProtectServerNum
Filters	No	No	Array of AssetFilters	DirName: website name. DirPath: protected website directory. Example:View
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ExportWebPageEventList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting tampering events

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportWebPageEventList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: CreateTime and RestoreTime. Default value: CreateTime. Example: CreateTime
Filters	No	No	Array of AssetFilters	Filter condition. • IpOrAlias - String - Required: no - host IP or alias filter. • EventType - String - Required: No - Event type. • EventStatus - String - Required: No - Event status. Example:View
Order	No	No	Uint64	Sorting order. 0: descending order. 1: ascending order. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID. You can call the ExportTasks API to download the exported data based on this ID. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ModifyMaConnEventType

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the micro-alarm access event type.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyMaConnEventType
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ModifyEventIds	Yes	No	Array of Uint64	Changed event ID. Example: [1]
Type	Yes	No	Uint64	Event type. • 0: Normal • 1: Exception Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyMaCustomPolicy

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to create or modify the micro-alarm custom allowlist.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyMaCustomPolicy
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Policy	Yes	No	MaCustomPolicy	Custom whitelist policy Example:View

3. Output Parameters

Parameter name	Type	Description
Id	Uint64	Created custom allowlist ID. Example: 1

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyMaCustomPolicyStatus

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the micro-alarm custom allowlist status.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyMaCustomPolicyStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	Custom allowlist rule ID set. Example: [1]
Status	Yes	No	Uint64	Custom allowlist status. • 0: Disabled • 1: Enabled Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyMaGlobalConf

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the micro-alarm global configuration.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyMaGlobalConf
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Data	Yes	No	MaGlobalConf	Global monitoring configuration. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyMaLabel

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to add or modify the tag information.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyMaLabel
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Label	Yes	No	MaLabel	Tag Example:View
WorkloadIds	No	No	Array of Int64	Tag-associated workload ID list. Example: [1]
WorkloadScope	No	No	Int64	Workload range [0: All; 1: Partial]. Example: 1

3. Output Parameters

Parameter name	Type	Description
Id	Int64	Tag ID Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyMaSelfLearnConfig

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to configure the self-learning policy.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyMaSelfLearnConfig
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
LearnEndDate	Yes	No	String	End time of learning. Example: 2023-10-11
LearnStartDate	Yes	No	String	Start time of learning. Example: 2023-10-10

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyMaWhitelist

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the micro-alarm global allowlist.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyMaWhitelist
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Whitelist	Yes	No	MaWhitelist	Allowlist Configuration Example:View

3. Output Parameters

Parameter name	Type	Description
Id	Uint64	ID of the created allowlist. Example: 1

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyMaWhitelistStatus

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the status of the micro-alarm global allowlist.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyMaWhitelistStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
All	Yes	No	Uint64	Whether it is All. • 0: Partial • 1: All Example: 0
Ids	No	No	Array of Uint64	ID collection for the selected global allowlist configuration in case of not All. Only the outermost switch is operated in case of All. Example: [1]
Status	Yes	No	Uint64	Status. • 0: Disabled • 1: Enabled Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyMaWorkloadLabel

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the micro-alarm workload tag.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyMaWorkloadLabel
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
LabelIds	Yes	No	Array of Int64	Tag List Example: [1]
WorkloadId	Yes	No	Int64	Workload ID. Example: 1

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyMaWorkloadMonitor

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the micro-alarm workload monitoring.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyMaWorkloadMonitor
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
EndTime	No	No	Datetime_iso	End date of self-learning. Example: 2023-12-10 23:59:59
Ids	Yes	No	Array of Int64	Load ID list. Example: [1]
IsEnabled	Yes	No	Int64	Whether monitoring is enabled [1: Enabled; 0: Disabled]. Example: 1
StartTime	No	No	Datetime_iso	Start date of self-learning. Example: 2023-10-10 00:00:00

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyMemShellRules

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to edit or create Java Webshell allowlist rules.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyMemShellRules
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
AnnotationsRegexp	No	No	String	Based64-encoded annotations (regular expression). If this parameter is left blank, matching is not performed. Example: cmVkaXMuY2Zn
ClassNameRegexp	No	No	String	Based64-encoded class name (regular expression). If this parameter is left blank, matching is not performed. Example: LW5vcmcuYXBhY2hlLmNhdGFsaW5hLnN0YXJ0dXAuQm9vdHN0cmFwCg==
GroupID	No	No	String	Batch ID. Example: 85c909fe-c87c-11e9-a100-5cb90191ae78
GroupName	No	No	String	Policy name Example: groupname
HandleHistory	No	No	Uint64	Whether to process historical events. 0: no, 1: yes. Example: 1
Id	No	No	Uint64	Rule auto-increment ID (leave this parameter empty for rule addition). Example: 1302396215
InterfacesRegexp	No	No	String	Based64-encoded names of inherited APIs (regular expression). If this parameter is left blank, matching is not performed. Example: LW5vcmcuYXBhY2hlLmNhdGFsaW5hLnN0YXJ0dXAuQm9vdHN0cmFwCg==
IsGlobal	No	No	Uint64	Whether it is a global rule. (Whether it is effective for all hosts under appid. 0: single UUID, 1: global. The default value is no.) Example: 1
LoaderClassNameRegexp	No	No	String	Based64-encoded class loader name (regular expression). If this parameter is left blank, matching is not performed. Example: LW5vcmcuYXBhY2hlLmNhdGFsaW5hLnN0YXJ0dXAuQm9vdHN0cmFwCg
LogicalSymbol	No	No	Uint64	Logical operator. 0: 5 valid regular expression logical ANDs, 1: logical OR. Example: 0
MemshellListID	No	No	Uint64	ID of the event, which must be passed in when you add the event to the allowlist. If you create a rule, leave this parameter empty. Example: 12
SuperClassNameRegexp	No	No	String	Based64-encoded parent class name (regular expression). If this parameter is left blank, matching is not performed. Example: LW5vcmcuYXBhY2hlLmNhdGFsaW5hLnN0YXJ0dXAuQm9vdHN0cmFwCg
Uuids	No	No	Array of String	Agent IDs. Example: ["0039803a-ca13-40cc-8b39-bd3b103765ec"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.

Error Code	Description
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyNetAttackSetting

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Yunapi Response

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyNetAttackSetting
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
AutoInclude	No	No	Uint64	New assets automatically include: 0 - Do not include, 1 - include. Example: 1
ExcludeInstanceIds	No	No	Array of String	Manually Excluded Hosts Example: ["inst-d92d"]
InstanceIds	No	No	Array of String	Specified servers Example: ["inst-d92d"]
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
NetAttackAlarmStatus	Yes	No	Uint64	0: New warning events pending processing by default, 1: New warning events processed by default, 3: New warning events ignored by default Example: 1
NetAttackEnable	Yes	No	Uint64	0 - Disable Network Attack Detection, 1 - Enable Network Attack Detection. Example: 1
Scope	No	No	Uint64	1: all servers with CWP Ultimate. 0: selected servers. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyWebPageProtectDir

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to create or modify a protected directory.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyWebPageProtectDir
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
HostConfig	Yes	No	Array of ProtectHostConfig	Protected server information. Example:View
ProtectDirAddr	Yes	No	String	URL of the protected directory. Example: /var/www
ProtectDirName	Yes	No	String	Name of the protected directory. Example: Web protection
ProtectFileType	Yes	No	String	Protected file types, separated with semicolons (:). Example: .html;.php

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
FailedOperation.AgentOffline	The agent is offline.
FailedOperation.APIServerFail	Failed to call the API service.
FailedOperation.LicenseExceeded	The number of available licenses is insufficient, and one more license is required. Please purchase a new license.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.
FailedOperation.ProtectStartFail	Failed to enable protection.

ModifyWebPageProtectSetting

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for modifying website protection settings

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyWebPageProtectSetting
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	String	Protected path. Example: var
ModifyType	Yes	No	Uint64	Type of the setting that you want to modify. 1: directory name. 2: protected file type. Example: 1
Value	Yes	No	String	Value. Example: redis_node_protect

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

Error Code	Description
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

ModifyWebPageProtectSwitch

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the protection switches in the web page anti-tampering module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyWebPageProtectSwitch
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of String	Websites for which you want to operate the switch. You can specify a maximum of 100 websites in each request. Example: ["101"]
Status	No	No	Uint64	1: enable. 2: disable. This parameter is required when SwitchType is set to 1 or 2. Example: 1
SwitchType	Yes	No	Uint64	Switch type. 1: protection. 2: automatic recovery. 3: removal from protection. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
FailedOperation.AgentOffline	The agent is offline.
FailedOperation.APIServerFail	Failed to call the API service.
FailedOperation.LicenseExceeded	The number of available licenses is insufficient, and one more license is required. Please purchase a new license.
InvalidParameter	Invalid parameter.
LimitExceeded	The quota limit has been reached.

Error Code	Description
OperationDenied	Operation denied.
FailedOperation	Operation failed.

Asset Management APIs CreateIncidentBacktracking

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to trigger event investigation backtracking.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateIncidentBacktracking
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Quuid	Yes	No	String	CWPP QUuid. Example: c973997a-36ad-4374-860a-fa462281ayay

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request

Parameter name	Type	Description
		needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DeleteCloudVendorAccountAK

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete an AK record.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteCloudVendorAccountAK
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	Int64	Record ID Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DeleteMachine

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to uninstall the CWP agent.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-26 17:06:53.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteMachine
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
Uuid	Yes	No	String	CWP client UUID. Example: 97d7cec6-0f2a-b636-e340-43f212dbb33c

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
FailedOperation.MachineDelete	The server was uninstalled.
InternalError.MainDBFail	Failed to operate data.
FailedOperation.APIServerFail	Failed to call the API service.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

DeleteMachineTag

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to remove a tag from a server.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteMachineTag
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Rid	Yes	No	Uint64	ID of the tag that you want to remove. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

DeleteTags

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete tags.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteTags
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	IDs of up to 100 tags. Example: [16500]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
FailedOperation	Operation failed.

DescribeAccountStatistics

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to get the account statistics list.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAccountStatistics
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter condition. • Username - String - Required: No - Username of the account. Example:View
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
AccountStatistics	Array of AccountStatistics	Account statistics. Example:View
TotalCount	Uint64	Total number of records in the account statistics list. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetAppList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the application list

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetAppList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: FirstTime and ProcessCount. Example: FirstTime
Filters	No	No	Array of AssetFilters	Filter conditions. • AppName - String - Required: No - Application name for search. • IP - String - Required: No - Host IP address. • MachineName - String - Required: No - Host name. • InstanceID - String - Required: No - Instance ID. • Type - Int - Required: No - Type. Only Linux applications are supported. 0: all 1: Ops 2: database 3: security 4: suspicious application 5: system architecture 6: system application 7: web service 99: others • OsType - String - Required: No - Windows or Linux. • OsName - String - Required: No - Operating system name (Value returned by the DescribeMachineOsList API). Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 1
Offset	No	No	Uint64	Offset. Default value: 0. Example: 1
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc

Parameter name	Required	Allow NULL	Type	Description
Quuid	No	No	String	QUUID of the server. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter name	Type	Description
Apps	Array of AssetAppBaseInfo	Application list API Example:View
Total	Uint64	Total number. Example: 1021
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetAppProcessList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for getting a list of software-associated processes

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetAppProcessList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 1
Name	Yes	No	String	Name of the application. Example: mysql
Offset	No	No	Uint64	Offset. Default value: 0. Example: 1
Quuid	Yes	No	String	Host QUUID. Example: 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	Yes	No	String	Host UUID. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter name	Type	Description
Process	Array of AssetAppProcessInfo	Process list. Example:View
Total	Uint64	Total number of partitions. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetCoreModuleInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for getting kernel module details

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetCoreModuleInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	String	ID of the kernel module. Example: 1001
Quuid	Yes	No	String	QUUID of the server. Example: 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	Yes	No	String	Server UUID. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter name	Type	Description
Module	AssetCoreModuleDetail	Details of the kernel module. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetCoreModuleList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying kernel modules for asset management

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetCoreModuleList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: Size, FirstTime, ProcessCount, and ModuleCount. Example: Size
Filters	No	No	Array of AssetFilters	Filter conditions. • IP - String - Required: No - Host IP address. • MachineName - String - Required: No - Host name. • InstanceID - String - Required: No - Instance ID. • Name - String - Required: No - Package name. Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc
Quuid	No	No	String	QUUID of the server. Example: 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	No	No	String	Server UUID. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
Modules	Array of AssetCoreModuleBaseInfo	List Example:View
Total	Uint64	Total number. Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetDatabaseInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying database details in the asset management module

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetDatabaseInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	String	Database ID. Example: 1
Quuid	Yes	No	String	QUUID of the server. Example: 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	Yes	No	String	Server UUID. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter name	Type	Description
Database	AssetDatabaseDetail	Database details. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetDatabaseList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the database list in the asset management module

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetDatabaseList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid value: FirstTime. Example: FirstTime
Filters	No	No	Array of AssetFilters	Filter conditions. • MachineName - String - Required: No - Host alias for filtering. • IP - String - Required: No - Host IP address for filtering. • InstanceID - String - Required: No - Host instance ID for filtering. • User - String - Required: No - corresponding user. • Port - Int - Required: No - Port. • Name - Int - Required: No - Database name. 0: all 1: MySQL 2: Redis 3: Oracle 4: MongoDB 5: MemCache 6: PostgreSQL 7: HBase 8: DB2 9: Sybase 10: TiDB • Proto - String - Required: No - Protocol. 1: TCP; 2: UDP; 3: unknown. • OsType - String - Required: No - Operating system type, which can be Linux or Windows. • OsName - String - Required: No - Operating system name (value returned by the DescribeMachineOsList API). Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 1

Parameter name	Required	Allow NULL	Type	Description
Offset	No	No	Uint64	Offset. Default value: 0. Example: 1
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: desc
Quuid	No	No	String	QUUID of the server. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter name	Type	Description
Databases	Array of AssetDatabaseBaseInfo	List Example:View
Total	Uint64	Total number. Example: 21
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetHostTotalCount

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the quantity statistics about all resources on a server

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetHostTotalCount
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Quuid	Yes	No	String	Host QUUID. Example: ed12c76b-2f65-4d44-a001-8f60cce9ayay
Uuid	Yes	No	String	Host UUID. Example: ed12c76b-2f65-4d44-a001-8f60cce9ayay

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
Types	Array of AssetKeyVal	Number of resources of each type. system: resource monitoring. account: account. port: port. process: process. app: application software. database: database. webapp: web application. webframe: web framework. webservice: web service. weblocation: website. systempackage: system installation package. jar: JAR package. initservice: initialization service. env: The environment variables. coremodule: kernel module. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the numbers of the following resources: servers, accounts, ports, processes, software applications, databases, web applications, web frameworks, web services, and websites.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:54:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
AccountCount	Uint64	Number of accounts. Example: 1
AccountNewCount	Int64	Number of accounts added on the current day. Example: 1

Parameter name	Type	Description
DatabaseCount	Uint64	Number of databases. Example: 1
DatabaseNewCount	Int64	Number of databases added on the current day. Example: 1
MachineCount	Uint64	Number of servers. Example: 1
MachineNewCount	Int64	Number of servers added on the current day. Example: 1
PortCount	Uint64	Number of ports. Example: 1
PortNewCount	Int64	Number of ports added on the current day. Example: 1
ProcessCount	Uint64	Number of processes. Example: 1
ProcessNewCount	Int64	Number of processes added on the current day. Example: 1
SoftwareCount	Uint64	Number of software applications. Example: 1
SoftwareNewCount	Int64	Number of software applications added on the current day. Example: 1
WebAppCount	Uint64	Number of web applications. Example: 1
WebAppNewCount	Int64	Number of web applications added on the current day. Example: 1
WebFrameCount	Uint64	Number of web frameworks. Example: 1
WebFrameNewCount	Int64	Number of web frameworks added on the current day. Example: 1
WebLocationCount	Uint64	Number of websites. Example: 1
WebLocationNewCount	Int64	Number of websites added on the current day. Example: 1

Parameter name	Type	Description
WebServiceCount	Uint64	Number of web services. Example: 1
WebServiceNewCount	Int64	Number of web services added on the current day. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetInitServiceList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the list of asset management startup services

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetInitServiceList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid value: FirstTime. Example: FirstTime
Filters	No	No	Array of AssetFilters	Filtering conditions. • IP - String - required: no - host IP address. • MachineName - String - required: no - host name. • InstanceID - String - required: no - instance ID. • Name - String - required: no - package name. • User - String - required: no - user. • IsAutoRun - String - required: no - whether it starts at boot: 0: no; 1: yes. • Status - String - required: no - default enabling status: 0: not enabled; 1: enabled (Linux only). • Type- String - required: no - type: type (Windows only). 1: encoder. 2: IE plugin. 3: network provider. 4: image hijacking. 5: LSA provider. 6: KnownDLLs. 7: start execution. 8: WMI. 9: scheduled task. 10: Winsock provider. 11: printing monitor. 12: resource manager. 13: driving service. 14: login. Example:View

Parameter name	Required	Allow NULL	Type	Description
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 1
Offset	No	No	Uint64	Offset. Default value: 0. Example: 11
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: desc
Quuid	No	No	String	QUUID of the server. Example: 1
Uuid	No	No	String	Server UUID. Example: 1

3. Output Parameters

Parameter name	Type	Description
Services	Array of AssetInitServiceBaseInfo	List Example:View
Total	Uint64	Total number. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
ResourceNotFound	The resource does not exist.

DescribeAssetJarInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the details of a JAR package

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetJarInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	String	ID of the JAR package. Example: 1
Quuid	Yes	No	String	QUUID of the server. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Uuid	Yes	No	String	Server UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

3. Output Parameters

Parameter name	Type	Description
Jar	AssetJarDetail	Details of the JAR package. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist.
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetJarList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying JAR packages

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetJarList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid value: FirstTime. Example: FirstTime
Filters	No	No	Array of AssetFilters	Filtering conditions. • IP - String - required: no - host IP address. • MachineName - String - required: no - host name. • InstanceID - String - required: no - instance ID. • Name - String - required: no - package name. • Type - Uint - required: no - type: 1: application. 2: system library. 3: Web service built-in library. 4: other dependency packages. • Status - String - required: no - whether executable: 0: no; 1: yes. Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 1
Offset	No	No	Uint64	Offset. Default value: 0. Example: 1
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: desc
Quuid	No	No	String	QUUID of the server. Example: 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	No	No	String	Server UUID. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter name	Type	Description
Jars	Array of AssetJarBaseInfo	Application list API Example:View
Total	Uint64	Total number. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetMachineDetail

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for getting the resource details of the asset management host

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetMachineDetail
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Quuid	Yes	No	String	QUUID of the server. Example: de92dec8-d312-49c5-b3e4-505584eeayay
Uuid	Yes	No	String	Server UUID. Example: de92dec8-d312-49c5-b3e4-505584eeayay

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
MachineDetail	AssetMachineDetail	Server details. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetMachineList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the resource monitoring list on the asset fingerprint page.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetMachineList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: FirstTime and PartitionCount. Example: FirstTime
Filters	No	No	Array of Filter	Filter conditions. • MachineName: Host name. • InstanceID: Instance ID. • IP: Private IP address or public IP address. • OsType - String - Required: No - Windows or Linux. • CpuLoad - Int - Required: No - 0: unknown; 1: low load; 2: medium load; 3: high load. • DiskLoad - Int - Required: No - 0: 0% or unknown; 1: 0%–20%; 2: 20%–50%; 3: 50%–80%; 4: 80%–100%. • MemLoad - Int - Required: No - 0: 0% or unknown; 1: 0%–20%; 2: 20%–50%; 3: 50%–80%; 4: 80%–100%. • Quuid: Host QUUID. • OsName - String - Required: No - Operating system name (value returned by the DescribeMachineOsList API). Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

Parameter name	Required	Allow NULL	Type	Description
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc

3. Output Parameters

Parameter name	Type	Description
Machines	Array of AssetMachineBaseInfo	List of records. Example:View
Total	Uint64	Total number. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetPlanTaskList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying scheduled tasks in the asset management module

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetPlanTaskList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid value: FirstTime. Example: FirstTime
Filters	No	No	Array of AssetFilters	Filtering conditions. • IP - String - required: no - host IP address. • MachineName - String - required: no - host name. • InstanceID - String - required: no - instance ID. • User - String - required: no - user. • Status - int - required: no - default enabling status: 0: not enabled; 1: enabled. Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 1
Offset	No	No	Uint64	Offset. Default value: 0. Example: 1
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: desc
Quuid	No	No	String	QUUID of the server. Example: 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	No	No	String	Server UUID. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter	Type	Description

name		
Tasks	Array of AssetPlanTask	List Example:View
Total	Uint64	Total number. Example: 12
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetPortInfoList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the port list in the asset management module

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetPortInfoList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: FirstTime and StartTime. Example: FirstTime
Filters	No	No	Array of Filter	Filter conditions. • Port - uint64 - Required: No - Port. • IP - String - Required: No - Host IP address. • MachineName - String - Required: No - Host name. • InstanceID - String - Required: No - Instance ID. • ProcessName - String - Required: No - Listening process. • Pid - uint64 - Required: No - PID. • User - String - Required: No - Corresponding user. • Group - String - Required: No - User group. • Ppid - uint64 - Required: No - PPID. • Proto - String - Required: No - Port protocol: TCP/UDP/unknown. • OsType - String - Required: No - Windows or Linux. • RunTimeStart - String - Required: No - Running start time. • RunTimeEnd - String - Required: No - Running end time. • BindIp - String - Required: No - Bound IP address. • OsName - String - Required: No - Operating system (value returned by the DescribeMachineOsList API). Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 1

Parameter name	Required	Allow NULL	Type	Description
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc
Quuid	No	No	String	QUUID of the server. Example: 37b6df34-68f1-4ab8-a3d8-7b89de604c82

3. Output Parameters

Parameter name	Type	Description
Ports	Array of AssetPortBaseInfo	List Example:View
Total	Uint64	Total number of records. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetProcessInfoList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying processes in the asset management module

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetProcessInfoList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: FirstTime and StartTime. Example: FirstTime
Filters	No	No	Array of Filter	Filter conditions. • IP - String - Required: No - Host IP address. • MachineName - String - Required: No - Host name. • InstanceID - String - Required: No - Instance ID. • Name - String - Required: No - Process name. • User - String - Required: No - Process user. • Group - String - Required: No - Process user group. • Pid - UInt64 - Required: No - Process ID. • Ppid - UInt64 - Required: No - Parent process ID. • OsType - String - Required: No - Windows or Linux. • Status - String - Required: No - Process status. 1: executable (R) 2: interruptible (S) 3: uninterruptible (D) 4: paused or traced (T) 5: zombie (Z) 6: to be terminated (X). • RunTimeStart - String - Required: No - Running start time. • RunTimeEnd - String - Required: No - Running end time. • InstallByPackage - UInt64 - Required: No - Whether a package is used for installation. 0: no; 1: yes. • OsName - String - Required: No - Operating system name (value returned by the DescribeMachineOsList API). Example:View

Parameter name	Required	Allow NULL	Type	Description
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 12
Offset	No	No	Uint64	Offset. Default value: 0. Example: 100
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc
Quuid	No	No	String	QUUID of the server. Example: 392f05bd-bf86-4911-8cf9-b8c2ac0f62ab

3. Output Parameters

Parameter name	Type	Description
Process	Array of AssetProcessBaseInfo	List Example:View
Total	Uint64	Total number of records. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetRecentMachineInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the most recent server trend.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetRecentMachineInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
BeginDate	Yes	No	Date	Start time, such as 2020-09-22. Example: 2020-10-10
EndDate	Yes	No	Date	End time, such as 2020-09-22. Example: 2020-10-10

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
LiveList	Array of AssetKeyVal	List of online servers. Example:View
OfflineList	Array of AssetKeyVal	List of offline servers. Example:View
RiskList	Array of AssetKeyVal	List of servers at risk. Example:View
TotalList	Array of AssetKeyVal	List of total servers. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter.DateRange	The time range format is incorrect.
UnknownParameter	Unknown parameter error.

DescribeAssetSystemPackageList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying system installation packages in the asset management module

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetSystemPackageList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: FirstTime and InstallTime. Example: FistTime
Filters	No	No	Array of Filter	Filter conditions. • IP - String - Required: No - Host IP address. • MachineName - String - Required: No - Host name. • InstanceID - String - Required: No - Instance ID. • Name - String - Required: No - Package name. • StartTime - String - Required: No - Installation start time. • EndTime - String - Required: No - Installation end time. • Type - int - Required: No - Installation package type. 1: RPM 2: dpkg 3: Java 4: system Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 1
Offset	No	No	Uint64	Offset. Default value: 0. Example: 11
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Default value: desc. Example: asc
Quuid	Yes	No	String	Host QUUID. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

Parameter name	Required	Allow NULL	Type	Description
Uuid	Yes	No	String	Host UUID. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter name	Type	Description
Packages	Array of AssetSystemPackageInfo	List Example:View
Total	Uint64	Total number of records. Example: 12
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetUserInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the details of a server account

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetUserInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Name	Yes	No	String	Account name. Example: any_user
Quuid	Yes	No	String	UUID of the cloud server. Example: 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	Yes	No	String	UUID of the CWP agent. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter name	Type	Description
User	AssetUserDetail	User details. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
InternalError.MainDBFail	Failed to operate data.

DescribeAssetUserList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for getting the account list

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetUserList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Optional sorting method: [FirstTime
Filters	No	No	Array of Filter	Filter conditions. • IP - String - Required: No - Host IP address. • MachineName - String - Required: No - Host name. • InstanceID - String - Required: No - Instance ID. • Name - String - Required: No - Account name (fuzzy match). • NameStrict - String - Required: No - Account name (exact match). • Uid - UInt64 - Required: No - Uid. • Gid - UInt64 - Required: No - GID. • LoginTimeStart - String - Required: No - Start time. For example, 2021-01-11. • LoginTimeEnd - String - Required: No - End time. For example, 2021-01-11. • LoginType - UInt64 - Required: No - 0: login not supported; 1: key-based login only; 2: password-based login only; 3: key-based and password-based login (Linux only). • OsType - String - Required: No - Windows or Linux. • Status - UInt64 - Required: No - Account status. 0: disabled; 1: enabled. • UserType - UInt64 - Required: No - Account type. 0: guest user; 1: standard user; 2: admin user (Windows only). • IsDomain - UInt64 - Required: No - Whether the account is a domain account. 0: no; 1: yes (Windows only). • IsRoot - UInt64 - Required: No - Whether the permission is root permission. 0: no; 1: yes (Linux only). • IsSudo - UInt64 - Required: No - Whether the permission is Sudo permission. 0: no; 1: yes (Linux only). • IsSshLogin -UInt64 - Required: No - Whether SSH login is used. 0: no; 1: yes (Linux only). • ShellLoginStatus - UInt64 - Required: No - Whether shell login is used. 0: no; 1: yes (Linux only). • PasswordStatus - UInt64 - Required: No -

Parameter name	Required	Allow NULL	Type	Description
				Password status. 1: normal; 2: about to expire; 3: expired; 4: locked (Linux only). • OsName - String - Required: No - Operating system name (value returned by the DescribeMachineOsList API). Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 1
Offset	No	No	Uint64	Offset. Default value: 0. Example: 1
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc
Quuid	No	No	String	QUUID of the server. Example: 1

3. Output Parameters

Parameter name	Type	Description
Total	Uint64	Total number of records. Example: 1
Users	Array of AssetUserBaseInfo	Account list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.DateRange	The time range format is incorrect.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetWebAppList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying web applications in the asset management module

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetWebAppList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: FirstTime and PluginCount. Example: FirstTime
Filters	No	No	Array of Filter	Filter conditions. • IP - String - Required: No - Host IP address. • MachineName - String - Required: No - Host name. • InstanceID - String - Required: No - Instance ID. • Name - String - Required: No - Application name. • Domain - String - Required: No - Site domain name. • Type - Int - Required: No - Service type. 0: all 1: Tomcat 2: Apache 3: Nginx 4: WebLogic 5: Websphere 6: JBoss 7: Jetty 8: IHS 9: Tengine • OsType - String - Required: No - Windows or Linux. • OsName - String - Required: No - Operating system name (value returned by the DescribeMachineOsList API). Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 10

Parameter name	Required	Allow NULL	Type	Description
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc
Quuid	No	No	String	QUUID of the server. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter name	Type	Description
Total	Uint64	Total number of records. Example: 12
WebApps	Array of AssetWebAppBaseInfo	List Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetWebAppPluginList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying web application plug-ins in the asset management module

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetWebAppPluginList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	String	ID of the web application. Example: 23210436
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 1
Offset	No	No	Uint64	Offset. Default value: 0. Example: 1
Quuid	Yes	No	String	Host QUUID. Example: 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	Yes	No	String	Host UUID. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter name	Type	Description
Plugins	Array of AssetWebAppPluginInfo	List Example:View
Total	Uint64	Total number of partitions. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist.
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetWebFrameList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the web frameworks in the asset management module

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetWebFrameList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: FirstTime and JarCount. Example: FirstTime
Filters	No	No	Array of Filter	Filter conditions. • IP - String - Required: No - Host IP address. • MachineName - String - Required: No - Host name. • InstanceID - String - Required: No - Instance ID. • Name - String - Required: No - Framework name. • NameStrict - String - Required: No - Framework name (strict match). • Lang - String - Required: No - Framework language, which can be Java or Python. • Type - String - Required: No - Service type. 0: all 1: Tomcat 2: Apache 3: Nginx 4: WebLogic 5: Websphere 6: JBoss 7: WildFly 8: Jetty 9: IHS 10: Tengine • OsType - String - Required: No - Windows or Linux. • OsName - String - Required: No - Operating system name (value returned by the DescribeMachineOsList API). Example:View

Parameter name	Required	Allow NULL	Type	Description
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc
Quuid	No	No	String	QUUID of the server. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter name	Type	Description
Total	Uint64	Total number of records. Example: 12
WebFrames	Array of AssetWebFrameBaseInfo	List Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetWebLocationInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for getting web site details

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetWebLocationInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	String	Website ID. Example: 1
Quuid	Yes	No	String	QUUID of the server. Example: 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	Yes	No	String	Server UUID. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter name	Type	Description
WebLocation	AssetWebLocationInfo	Website information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetWebLocationList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for getting the list of web sites

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetWebLocationList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: FirstTime and PathCount. Example: PathCount
Filters	No	No	Array of Filter	Filter conditions. • IP - String - Required: No - Host IP address. • MachineName - String - Required: No - Host name. • InstanceID - String - Required: No - Instance ID. • Name - String - Required: No - Domain name. • User - String - Required: No - Corresponding user. • Port - UInt64 - Required: No - Site port. • Proto - UInt64 - Required: No - Site protocol. 1: HTTP; 2: HTTPS. • ServiceType - UInt64 - Required: No - Service type. 1: Tomcat 2: Apache 3: Nginx 4: WebLogic 5: Websphere 6: JBoss 7: WildFly 8: Jetty 9: IHS 10: Tengine • OsType - String - Required: No - Windows or Linux. • OsName - String - Required: No - Operating system name (value returned by the DescribeMachineOsList API). Example:View

Parameter name	Required	Allow NULL	Type	Description
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 12
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc
Quuid	No	No	String	QUUID of the server. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

3. Output Parameters

Parameter name	Type	Description
Locations	Array of AssetWebLocationBaseInfo	List of websites. Example:View
Total	Uint64	Total number of records. Example: 12
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetWebServiceInfoList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the list of asset management web services

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetWebServiceInfoList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: FirstTime and ProcessCount. Example: FirstTime
Filters	No	No	Array of AssetFilters	Filter conditions. • IP - String - Required: No - Host IP address. • MachineName - String - Required: No - Host name. • InstanceID - String - Required: No - Instance ID. • User - String - Required: No - Corresponding user. • Name - String - Required: No - Web service name. Valid values: 1: Tomcat 2: Apache 3: Nginx 4: WebLogic 5: Websphere 6: JBoss 7: WildFly 8: Jetty 9: IHS 10: Tengine • OsType - String - Required: No - Windows or Linux. • OsName - String - Required: No - Operating system name (value returned by the DescribeMachineOsList API). Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. • IpOrAlias - String - Required: no - host IP or alias filter. Example: 0

Parameter name	Required	Allow NULL	Type	Description
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc
Quuid	No	No	String	QUUID of the server. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter name	Type	Description
Total	Uint64	Total number. Example: 1
WebServices	Array of AssetWebServiceBaseInfo	List Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeAssetWebServiceProcessList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for getting the list of web service associated processes

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetWebServiceProcessList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	String	ID of the web service. Example: 12869
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Quuid	Yes	No	String	Host QUUID. Example: 24c9be55-c743-4a75-a5c7-2a2936843684
Uuid	Yes	No	String	Host UUID. Example: 24c9be55-c743-4a75-a5c7-2a2936843684

3. Output Parameters

Parameter name	Type	Description
Process	Array of AssetAppProcessInfo	Process list. Example:View
Total	Uint64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeCloudVendorAccountAKList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the list of cloud vendor AKs added by a user.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeCloudVendorAccountAKList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
CloudVendorAccountAKs	Array of CloudVendorAccountAK	AK list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeComponentStatistics

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to get the component statistics list.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeComponentStatistics
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter condition. ComponentName - String - Required: No - Component name. Example:View
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
ComponentStatistics	Array of ComponentStatistics	Component statistics. Example:View
TotalCount	Uint64	Total number of records in the component statistics list. Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeComponents

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the list of components.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeComponents
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ComponentId	No	No	Uint64	Component ID. You must specify either Uuid or ComponentId. If you configure the ComponentId parameter, the information about the specified component will be queried. Example: 1
Filters	No	No	Array of Filter	Filter condition. • ComponentVersion - String - Required: No - Version number of the component. • MachineIp - String - Required: No - Private IP of the server. Example:View
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Uuid	No	No	String	Unique UUID of the CWP client. You must specify either Uuid or ComponentId. If you configure the Uuid parameter, the information about the components on the specified server will be queried. Example: 5a540076-d38a-4078-aa98-qwert371d322

3. Output Parameters

Parameter name	Type	Description
Components	Array of Component	Component list data. Example:View
TotalCount	Uint64	Total number of records in the component list. Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeExportMachines

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the servers in a region.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:00:52.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeExportMachines
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter condition. • Keywords - String - Required: no - query keywords. • Status - String - Required: No - Connection status of the agent. OFFLINE: disconnected. ONLINE: connected. UNINSTALLED: not installed. • Version - String Required: no - current protection version (PRO_VERSION: professional
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
MachineRegion	Yes	No	String	Region of a server. Example: ap-region1
MachineType	Yes	No	String	Cloud host type. • CVM: cloud virtual machine. • BM: BM. Example: CVM
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
ProjectIds	No	No	Array of Uint64	List of business IDs to which the machine belongs. Example: [1002,1003]

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 12
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeHistoryAccounts

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to get the account change history list.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeHistoryAccounts
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter condition. • Username - String - Required: No - Account name. Example:View
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Uuid	Yes	No	String	Unique UUID of the CWP client. Example: 5a540076-d38a-4078-aa98-qwert371d322

3. Output Parameters

Parameter name	Type	Description
HistoryAccounts	Array of HistoryAccount	Account change history data. Example:View
TotalCount	Uint64	Total number of records in the account change history list. Example: 100

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeImportMachineInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying information about servers that are batch imported

Default interface request rate limit: 20 times per second.

Interface update time: 2022-06-16 12:16:37.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeImportMachineInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter conditions. • Version - String - Required: No - Protection edition. PRO_VERSION: Professional Edition. BASIC_VERSION: Basic Edition. Flagship: Ultimate Edition. ProtectedMachines: Professional Edition and Ultimate Edition. BASIC_PROPOST_GENERAL_DISCOUNT: General Edition, Professional Edition (pay-as-you-go), and Basic Edition.
ImportType	Yes	No	String	Type of the data that is batch imported. Valid values: Ip, Name, and Id. Example: Ip
IsQueryProMachine	No	No	Bool	Deprecated parameter. Example: true
MachineList	Yes	No	Array of String	Up to 1,000 server private IP addresses (default), server names, or server IDs. Example: ["192.168.0.204"]

3. Output Parameters

Parameter name	Type	Description
EffectiveMachineInfoList	Array of EffectiveMachineInfo	Valid server information, including server name, public or private IP address of the server, and server tags. Example:View
InvalidMachineList	Array of String	Servers that have failed to be imported at a time, such as servers that do not exist. Example: [""a9fe0359-04d9-417f-ab6d-ayay""]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMachineInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to get server details.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMachineInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Quuid	No	No	String	QUUID. You must specify at least one of the Quuid and Uuid parameters. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
Uuid	No	No	String	CWP client UUID. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0

3. Output Parameters

Parameter name	Type	Description
AgentVersion	String	Agent version number. Example: 10
FreeMalwaresLeft	Uint64	Number of free trojan detections remaining. Example: 1
FreeVulsLeft	Uint64	Number of free vulnerability detections remaining. Example: 1
HasAssetScan	Uint64	Whether there is an asset scan record. 0: no. 1: yes. Example: 1

Parameter name	Type	Description
InstanceId	String	Unique identifier of the CVM or BM host. Example: CVM
IsProVersion	Bool	Whether to enable the professional version. • true: yes. • false: no. Example: false
MachineIp	String	Machine IP. Example: 10.0.0.0
MachineName	String	Host name. Example: redis_node_cvm
MachineOs	String	Operating system. Example: Windows Server 2022
MachineRegion	String	Region of a server. Example: ap-region1
MachineStatus	String	Status. • ONLINE: online. • OFFLINE: Offline. Example: OFFLINE
MachineType	String	CVM type. • CVM: CVM. • BM: Bare Metal Service. • ECM: Edge Computing Machine. • LH: Cloud Platform Lighthouse. • Other: Hybrid cloud machines. Example: CVM
MachineWanIp	String	Public IP of the host. Example: 10.0.0.0
PayMode	String	Host status. • POSTPAY: postpaid mode, that is, pay-as-you-go. • PREPAY: prepaid mode, that is, monthly subscription. Example: PREPAY
ProVersionDeadline	String	Expiration time of the professional version (only valid for prepaid mode). Example: 2025-10-17 20:08:03
ProVersionOpenDate	String	Time when the professional version was enabled. Example: 2024-10-17 20:08:03
ProtectDays	Uint64	Protection duration in days by CWP. Example: 1

Parameter name	Type	Description
ProtectType	String	Protection edition: BASIC_VERSION - Basic Edition; PRO_VERSION - Pro Edition; Flagship - Ultimate Edition; GENERAL_DISCOUNT - General Edition. Example: BASIC_VERSION
Quuid	String	Unique UUID of the CVM or BM host. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
Uuid	String	CWP client UUID. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
ResourceNotFound	The resource does not exist.
InvalidParameterValue	The parameter value is invalid.

DescribeMachineOsList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query operating systems.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMachineOsList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
List	Array of OsName	List of operating systems. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DescribeMachineRegionList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the list of host regions.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMachineRegionList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
RegionList	Array of RegionListDetail	CVM type region list Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMachineRegions

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for getting the list of machine regions

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMachineRegions
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
ALL	Array of RegionInfo	Regions of all types. Example:View
BM	Array of RegionInfo	BM region list. Example:View

Parameter name	Type	Description
CVM	Array of RegionInfo	CVM region list. Example:View
ECM	Array of RegionInfo	ECM region list. Example:View
LH	Array of RegionInfo	LH region list. Example:View
Other	Array of RegionInfo	Other hybrid cloud region list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeMachines

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to get the list of servers in a specified region.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-10-18 17:27:47.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMachines
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filtering conditions. • Ips - String - required: no - query by IP address. • Names - String - required: no - query by instance name. • InstanceIds - String - required: no - query by instance ID. • Status - String - required: no - client status (OFFLINE: offline/shut down
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
MachineRegion	Yes	No	String	Region of a server. Example: ap-region1
MachineType	Yes	No	String	Zone type of the server. CVM: CVM zone BM: BM zone ECM: ECM zone LH: Lighthouse zone Other: hybrid cloud zone. Example: CVM
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
ProjectIds	No	No	Array of Uint64	List of business IDs to which the machine belongs. Example: [1]

3. Output Parameters

Parameter name	Type	Description
Machines	Array of Machine	Server list Example:View
TotalCount	Uint64	Number of hosts. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeOpenPortStatistics

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to get the statistics on port usage

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeOpenPortStatistics
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter condition. • Port - Uint64 - Required: No - Port number. Example:View
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
OpenPortStatistics	Array of OpenPortStatistics	Port statistics. Example:View
TotalCount	Uint64	Total number of records in the port statistics list. Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeProcessStatistics

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to get the process statistics list.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-07-28 23:46:05.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeProcessStatistics
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter condition. • ProcessName - String - Required: No - Process name. Example:View
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
ProcessStatistics	Array of ProcessStatistics	Data in the process statistics list. Example:View
TotalCount	Uint64	Total number of records in the process statistics list Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameterValue	The parameter value is invalid.

DescribeTagMachines

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to get the information of servers associated with a specified tag.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeTagMachines
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	Uint64	Tag ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
List	Array of TagMachine	The custom attributes. Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeTags

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to get all server tags.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-12-29 09:47:48.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeTags
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter conditions. • AddedOnTheFifteen - String - Required: No - Whether the tags are created within the last 15 days. If there is any value, it means yes. Example:View
MachineRegion	No	No	String	Region of a server. Example: ap-region1
MachineType	No	No	String	Cloud host type. • CVM: Cloud Virtual Machine • BM: BM. • ECM: Edge Computing Machine • LH: Lighthouse instance • Other: hybrid cloud server Example: CVM

3. Output Parameters

Parameter name	Type	Description
List	Array of Tag	The service information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

EditTags

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to add or edit tags.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: EditTags
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	No	No	Uint64	Tag ID. Example: 1
Name	Yes	No	String	Tag name. Example: tag-name
Quuids	No	No	Array of String	Quuid Example: ["dd90a245-ca7a-4268-9051-1fce4291ayay"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
MissingParameter	Missing parameter.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
ResourceNotFound	The resource does not exist.
InvalidParameterValue.TagNameLengthLimit	The tag name cannot contain more than 15 characters.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ExportAssetCoreModuleList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting the asset management kernel module list

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportAssetCoreModuleList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: FirstTime, Size, ProcessCount, and ModuleCount. Example: FirstTime
Filters	No	No	Array of AssetFilters	Filter conditions. • IP - String - Required: No - Host IP address. • MachineName - String - Required: No - Host name. • InstanceID - String - Required: No - Instance ID. • Name - String - Required: No - Package name. Example:View
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc
Quuid	No	No	String	QUUID of the server. Example: 1ce68339-8828-457f-b358-d5b1b34e4fe9
Uuid	No	No	String	Server UUID. Example: 1ce68339-8828-457f-b358-d5b1b34e4fe9

3. Output Parameters

Parameter name	Type	Description
TaskId	String	ID of the async download task. This value needs to be used together with the ExportTasks API.

Parameter name	Type	Description
		Example: 10001
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ExportAssetWebServiceInfoList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting the list of asset management web services

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportAssetWebServiceInfoList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: FirstTime and ProcessCount. Example: FirstTime
Filters	No	No	Array of AssetFilters	Filter conditions. • IP - String - Required: No - Host IP address. • MachineName - String - Required: No - Host name. • InstanceID - String - Required: No - Instance ID. • User - String - Required: No - Corresponding user. • Name - String - Required: No - Web service name. Valid values: 1: Tomcat 2: Apache 3: Nginx 4: WebLogic 5: Websphere 6: JBoss 7: WildFly 8: Jetty 9: IHS 10: Tengine • OsType - String - Required: No - Windows or Linux. • OsName - String - Required: No - Operating system name (value returned by the DescribeMachineOsList API). Example:View

Parameter name	Required	Allow NULL	Type	Description
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc
Quuid	No	No	String	QUUID of the server. Example: 1

3. Output Parameters

Parameter name	Type	Description
TaskId	String	ID of the async download task. This value needs to be used together with the ExportTasks API. Example: 10001
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameterValue	The parameter value is invalid.

ModifyMachineRemark

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Modify Host Remark Information

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-15 10:32:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyMachineRemark
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Quuid	Yes	No	String	Host QUUID. Example: 5a540076-d38a-4078-aa98-e7c86371d322
Remark	No	No	String	Remark Example: mark redis cvm

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ScanAsset

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for starting to scan asset fingerprints

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ScanAsset
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
AssetTypeIds	No	No	Array of Uint64	IDs of the asset fingerprint types. Example: [102]
Quuids	No	No	Array of String	List of QUUIDs. Example: ["5a540076-d38a-4078-aa98-q45rt371d322"]

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
TaskId	Uint64	Task ID. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InternalError.MainDBFail	Failed to operate data.
FailedOperation.NoProfessionHost	No servers with CWP Pro exist.
OperationDenied	Operation denied.
FailedOperation	Operation failed.

SyncAssetScan

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for synchronizing asset scan information

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: SyncAssetScan
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Sync	Yes	No	Bool	Specifies whether to enable synchronization. Valid values: true and false. Default value: false. Example: true

3. Output Parameters

Parameter name	Type	Description
LatestEndTime	String	Latest synchronization end time. Example: 2021-01-01 11:22:11
LatestStartTime	String	Latest synchronization start time. Example: 2021-01-01 11:22:11
State	String	The enumeration values are (uppercase): NOTASK (no synchronization task), SYNCING (synchronization in progress), FINISHED (synchronization completed). Example: NOTASK
TaskId	Uint64	The task ID. Example: 88
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InternalError.MainDBFail	Failed to operate data.
FailedOperation.APIServerFail	Failed to call the API service.
FailedOperation	Operation failed.

UpdateMachineTags

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for attaching tags to a server

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UpdateMachineTags
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MachineArea	Yes	No	String	Server type. Valid values: CVM, BM, ECM, and Other. Example: CVM
MachineRegion	Yes	No	String	Server region. Example: ap-region1
Quuid	Yes	No	String	QUUID of the server. Example: 24c9be55-c743-4a75-a5c7-2a2936843684
TagIds	No	No	Array of Uint64	Tag IDs. This operation will overwrite the original tags. Example: [115]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

Baseline Management APIs ChangeRuleEventsIgnoreStatus

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to batch change the ignoring status of events based on check item IDs or event IDs.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ChangeRuleEventsIgnoreStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
EventIdList	No	No	Array of Uint64	Event IDs. Example: [1,2]
IgnoreStatus	Yes	No	Uint64	Ignore status. 0: canceled from ignoring. 1: ignored. Example: 1
RuleIdList	No	No	Array of Uint64	IDs of the check items. Example: [1,2]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

CreateBaselineStrategy

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to create a baseline policy based on policy information.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateBaselineStrategy
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
CategoryIds	Yes	No	Array of Uint64	Baseline IDs selected for this policy. Example: [1,3,5,7] Example: [1,3,5,7]
IsGlobal	Yes	No	Uint64	Specifies whether all servers will be scanned. 1: yes. 0: no. If you set this parameter to 1, all servers with CWP Pro are scanned. Example: 1
MachineType	Yes	No	String	Cloud server type. Valid values: CVM: Cloud Virtual Machine BM: Bare Metal instance ECM: Edge Computing Machine LH: Lighthouse instance Other: hybrid cloud server Example: CVM
Quuids	No	No	Array of String	Server IDs. Example: ["quuid1","quuid2"] Example: ["657f3c29-4bc9-4c48-a8d6-de5bd14ffc67"]
RegionCode	Yes	No	String	Region Example: ap-region1
ScanAt	Yes	No	String	Scheduled scan time, which specifies the time to deliver a scan task. For example, if you set this parameter to 22:00, the system delivers a scan task at 22:00. Example: 02:00
ScanCycle	Yes	No	Uint64	Scan cycle, which specifies the interval at which scans are performed. For example, if you set this parameter to 2, the system performs a scan every 2 days. Example: 2
StrategyName	Yes	No	String	Policy name Example: Scheduled baseline scan

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
FailedOperation.NoProfessionHost	No servers with CWP Pro exist.
FailedOperation.TooManyStrategy	The maximum number of baseline policies is exceeded.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.

DeleteBaselineStrategy

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete a baseline policy based on a policy ID.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteBaselineStrategy
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
StrategyId	Yes	No	Uint64	ID of the baseline policy. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

DescribeBaselineAnalysisData

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the data overview statistics about a baseline policy based on a policy ID.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineAnalysisData
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
StrategyId	Yes	No	Uint64	ID of the baseline policy. Example: 1

3. Output Parameters

Parameter name	Type	Description
IfFirstScan	Uint64	Indicates whether it is the first scan. 1: yes. 0: no. Example: 1

Parameter name	Type	Description
IsGlobal	Uint64	Indicates whether all servers are selected. 1: yes. 0: no. Example: 1
LatestScanTime	String	Last detection time. Example: 2019-12-25 11:57:15
ScanHostCount	Uint64	Total number of servers. Example: 1
ScanRuleCount	Uint64	Total number of check items. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBaselineBasicInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the basic information about a baseline.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineBasicInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
BaselineName	No	No	String	Baseline name. Example: MySQL weak password detection

3. Output Parameters

Parameter name	Type	Description
BaselineBasicInfoList	Array of BaselineBasicInfo	Baseline basics. Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBaselineDetail

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the details of a baseline based on a baseline ID.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineDetail
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
BaselineId	Yes	No	Uint64	Baseline ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
BaselineDetail	BaselineDetail	Baseline details. Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBaselineEffectHostList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the servers affected by a baseline based on a baseline ID.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-03-28 01:21:07.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineEffectHostList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
BaselineId	Yes	No	Uint64	Baseline ID. Example: 12
Filters	No	No	Array of Filters	Filter condition. • AliasName - String - Server alias. • Status - Uint - 1: passed. 0: not passed. 5: checking. Example:View
Limit	Yes	No	Uint64	Maximum number of entries to return on each page. Maximum value: 100. Example: 10
Offset	Yes	No	Uint64	The number of the page to be returned. Example: 0
StrategyId	No	No	Uint64	Policy ID. Example: 1124
UuidList	No	No	Array of String	Server UUIDs. Example: ["5a540076-d38a-4078-aa98-qwert371d322"]

3. Output Parameters

Parameter name	Type	Description
EffectHostList	Array of BaselineEffectHost	List of affected servers. Example:View
TotalCount	Uint64	Total number of records. Example: 12
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBaselineHostTop

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query Top N servers at risk.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineHostTop
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
StrategyId	Yes	No	Uint64	Policy ID. Example: 1
Top	Yes	No	Uint64	Top N value. Example: 1

3. Output Parameters

Parameter name	Type	Description
BaselineHostTopList	Array of	Top events triggered by the baseline policy on servers.

Parameter name	Type	Description
	BaselineHostTopList	Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
FailedOperation.NoProfessionHost	No servers with CWP Pro exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBaselineList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query a list of baselines.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filtering conditions. • StrategyId - Uint64 - baseline policy ID. • Status - Uint64 - processing status: 1 - passed; 0 - failed. • Level - Uint64[] - threat level. • BaselineName - String - baseline name. • Quuid - String - host QUUID. • Uuid - String - host UUID. Example:View
Limit	Yes	No	Uint64	Maximum number of entries to return on each page. Maximum value: 100. Example: 10
Offset	Yes	No	Uint64	The number of the page to be returned. Example: 0

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
BaselineList	Array of BaselineInfo	Baseline information. Example:View
TotalCount	Uint64	Total number of records returned for the paginated query. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBaselineRule

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the baseline check items based on a baseline ID.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineRule
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
BaselineId	Yes	No	Uint64	Baseline ID. Example: 1
Level	No	No	Array of Uint64	Baseline risk level. 0: low; 1: medium; 2: high; 3: critical. Example: [1,2,3]
Limit	Yes	No	Uint64	Maximum number of entries to return on each page. Maximum value: 100. Example: 10
Offset	Yes	No	Uint64	The number of the page to be returned. Example: 0
Quuid	No	No	String	QUUID of the server. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
Status	No	No	Uint64	State. Example: 0
Uuid	No	No	String	Host UUID. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0

3. Output Parameters

Parameter name	Type	Description
BaselineRuleList	Array of BaselineRuleInfo	List of baseline check items. Example:View
ShowRuleRemark	Bool	Indicates whether to display the Description column. true: yes. false: no. Example: true
TotalCount	Uint64	Total number of records returned for the paginated query. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBaselineScanSchedule

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the baseline check progress based on a task ID.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineScanSchedule
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
TaskId	Yes	No	Uint64	Task ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
Schedule	Uint64	Check progress in percentage. Example: 1

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBaselineStrategyDetail

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the details of a baseline policy based on a policy ID.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineStrategyDetail
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
StrategyId	Yes	No	Uint64	ID of the custom baseline policy. Example: 1

3. Output Parameters

Parameter name	Type	Description
CategoryIds	Array of String	IDs of all baselines associated with this policy. Example: ["10021"]
IfScanned	Uint64	1: scanned. 0: not scanned. Example: 1
IsGlobal	Uint64	Specifies whether all servers will be scanned. 1: yes. 0: no. If you set this parameter to 1, all servers with CWP Pro are scanned. Example: 1
MachineType	String	CVM type. • CVM: CVM. • BM: Bare Metal Service. • ECM: Edge Computing Machine. • LH: Cloud Platform Lighthouse. • Other: Hybrid cloud machines. Example: CVM
PassRate	Uint64	Pass rate of the scans based on the policy. Example: 1
Quuids	Array of String	QUUIDs of all servers associated with this policy. Example: ["0096440e-9a9f-4e80-a82d-0b018637ayay"]
Region	String	Region of the server. Example: ap-bj
ScanAt	String	Time to deliver the regular scan. Example: 00:00:00

Parameter name	Type	Description
ScanCycle	String	Scan cycle. Unit: days. Example: 1
StrategyName	String	Policy name. Example: Weak password
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBaselineStrategyList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the custom baseline policy information.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineStrategyList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Enabled	Yes	No	Uint64	Enabling status of the rule. 1: enabled. 0: disabled. 2: all. Example: 1
Limit	Yes	No	Uint64	Maximum number of entries to return on each page. Maximum value: 100. Example: 10
Offset	Yes	No	Uint64	The number of the page to be returned. Example: 0

3. Output Parameters

Parameter name	Type	Description
StrategyList	Array of Strategy	Custom policy information. Example:View
TotalCount	Uint64	Total number of records returned for the paginated query. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBaselineTop

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query top baseline check items based on a policy ID.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineTop
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
StrategyId	Yes	No	Uint64	Policy ID. Example: 1
Top	Yes	No	Uint64	Top N value. Example: 5

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RuleTopList	Array of BaselineRuleTopInfo	Top check items. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
FailedOperation.NoProfessionHost	No servers with CWP Pro exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeIgnoreBaselineRule

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the information about ignored check items.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeIgnoreBaselineRule
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Limit	Yes	No	Uint64	Maximum number of entries to return on each page. Maximum value: 100. Example: 10
Offset	Yes	No	Uint64	The number of the page to be returned. Example: 0
RuleName	No	No	String	Detection item name. Example: rulename

3. Output Parameters

Parameter name	Type	Description
IgnoreBaselineRuleList	Array of IgnoreBaselineRule	List of ignored baseline check items. Example:View
TotalCount	Uint64	Total number of records returned for the paginated query. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeIgnoreRuleEffectHostList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query servers affected by ignored check items based on check item IDs and filter conditions.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeIgnoreRuleEffectHostList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter condition. • AliasName - String - Server alias. Example:View
Limit	Yes	No	Uint64	Maximum number of entries to return on each page. Maximum value: 100. Example: 10
Offset	Yes	No	Uint64	The number of the page to be returned. Example: 0
RuleId	Yes	No	Uint64	ID of the check item. Example: 1
TagNames	No	No	Array of String	Server tag names. Example: ["tag1"]

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
IgnoreRuleEffectHostList	Array of IgnoreRuleEffectHostInfo	Servers affected by the ignored check items. Example:View
TotalCount	Uint64	Total number of records returned for the paginated query. Example: 12
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeStrategyExist

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying whether a policy exists by policy name

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:34.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeStrategyExist
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
StrategyName	Yes	No	String	Policy name. Example: sname

3. Output Parameters

Parameter name	Type	Description
IfExist	Uint64	Indicates whether the policy exists. 1: yes. 0: no. Example: 1

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ExportBaselineEffectHostList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export servers affected by a baseline.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportBaselineEffectHostList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
BaselineId	Yes	No	Uint64	Baseline ID. Example: 1
BaselineName	No	No	String	Obsolete Example: check_redis_cvm
Filters	No	No	Array of Filters	Filter condition. • AliasName - String - Server alias. • Status - Uint - 1: passed. 0: not passed. 5: checking. Example:View
StrategyId	No	No	Uint64	Policy ID. Example: 2
UuidList	No	No	Array of String	Server UUIDs. Example: ["1ce68339-8828-457f-b358-d5b1b34e4fe9"]

3. Output Parameters

Parameter	Type	Description

name		
DownloadUrl	String	This parameter has been deprecated. Example: http://domain.com/anypath/x
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ExportBaselineList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting baselines

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportBaselineList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filtering conditions. • StrategyId - Uint64 - baseline policy ID. • Status - Uint64 - processing status: 1 - passed; 0 - failed. • Level - Uint64[] - threat level. • BaselineName - String - baseline name. • Quuid - String - host QUUID. • Uuid - String - host UUID. Example:View
IfDetail	No	No	Uint64	Deprecated parameter. Example: 1

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	Download URL of the exported file. This parameter has been deprecated. Example: http://www.ay.com/ay

Parameter name	Type	Description
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ExportIgnoreBaselineRule

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export information about ignored baseline check items.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportIgnoreBaselineRule
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
RuleName	No	No	String	Detection item name. Example: Redis baseline compliance check

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	This parameter has been deprecated. Example: http://www.ay.com/ay
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ExportIgnoreRuleEffectHostList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export servers affected by ignored check items based on check item IDs.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportIgnoreRuleEffectHostList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter condition. • AliasName - String - Server alias. Example:View
RuleId	Yes	No	Uint64	ID of the check item. Example: 1

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	This parameter has been deprecated. Example: http://domain.com/anypath/x
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

UpdateBaselineStrategy

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to update a baseline policy based on a policy ID.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UpdateBaselineStrategy
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
CategoryIds	Yes	No	Array of String	Baseline IDs selected for the specified policy. Example: ["1002"]
IsGlobal	Yes	No	Uint64	Specifies whether all servers will be scanned. 1: yes. 0: no. If you set this parameter to 1, all servers with CWP Pro are scanned. Example: 1
MachineType	Yes	No	String	Cloud host type. CVM: CVM instance BM: BMS instance ECM: ECM instance LH: Lighthouse instance OTHER: hybrid cloud instance. Example: CVM
Quuids	Yes	No	Array of String	Server IDs. Example: ["5a540076-d38a-4078-aa98-e7c86371d322"]
RegionCode	Yes	No	String	Region Example: ap-region1
ScanAt	Yes	No	String	Regular scan time at which a scan task is delivered. Example: 00:00:00
ScanCycle	Yes	No	Uint64	Scan cycle. Example: 1
StrategyId	Yes	No	Uint64	Policy ID. Example: 1
StrategyName	Yes	No	String	Policy name Example: redis_node_check

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

Error Code	Description
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
FailedOperation.NoProfessionHost	No servers with CWP Pro exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

Baseline Management APIs (New) DeleteBaselinePolicy

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for deleting baseline policies

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 12:02:51.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteBaselinePolicy
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
PolicyIds	Yes	No	Array of Int64	Policy ID. Example: [309052]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request

Parameter name	Type	Description
		needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DeleteBaselineRule

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for deleting a baseline rule

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 12:02:34.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteBaselineRule
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
RuleId	Yes	No	Int64	Rule ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
FailedOperation	Operation failed.

DeleteBaselineRuleIgnore

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for deleting a baseline ignoring rule

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 11:59:19.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteBaselineRuleIgnore
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
RuleIds	Yes	No	Array of Int64	Rule ID. Example: [44106]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

DeleteBaselineWeakPassword

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for deleting baseline weak passwords

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:32:04.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteBaselineWeakPassword
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
PasswordIds	Yes	No	Array of Int64	IDs of weak passwords. Example: [1002]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

DescribeBaselineDetectList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the baseline check details

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:34:39.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineDetectList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: [HostCount
Filters	No	No	Array of Filter	• PolicyName - string - Required: No - Policy name. • PolicyDetectStatus - int - Required: No - 1: checking. 2: check completed. • FirstTime - string - Required: No - Start time. • LastTime - string - Required: No - End time. Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
List	Array of BaselinePolicyDetect	Data returned. Example:View
Total	Int64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
FailedOperation	Operation failed.

DescribeBaselineDetectOverview

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the baseline check overview information

Default interface request rate limit: 20 times per second.

Interface update time: 2022-10-25 10:23:03.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineDetectOverview
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
PolicyId	No	No	Int64	Policy ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
HostCount	Int64	Number of servers on which baseline checks are performed. Example: 0

Parameter name	Type	Description
ItemCount	Int64	Number of check items. Example: 0
LatestNotPassCount	Int64	Number of Recent Detections Not Passed Example: 1
LatestPassCount	Int64	Number of Passed Tasks in the Most Recent Detection Example: 1
PassRate	Int64	Pass rate in percentage. Example: 100
PolicyCount	Int64	Number of policies. Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
FailedOperation	Operation failed.

DescribeBaselineDownloadList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the baseline download list

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 12:08:32.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineDownloadList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: [StartTime
Filters	No	No	Array of Filter	• Status - int - Required: No - 0: exporting. 1: completed. • StartTime - string - Required: No - Start time. • EndTime - string - Required: No - End time. • TaskName - string - Required: No - Task name. Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: DESC

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
List	Array of BaselineDownload	Data returned. Example:View
Total	Int64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidParameter	Invalid parameter.

DescribeBaselineFixList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the baseline fixing list

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 12:08:20.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineFixList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: [CreateTime
Filters	No	No	Array of Filter	• ItemName- string - Required or Not: No - Item Name Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
List	Array of BaselineFix	Data returned. Example:View
Total	Int64	Total number. Example: 10

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

DescribeBaselineHostDetectList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the servers configured with baseline checks

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:36:16.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineHostDetectList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: [LastTime
Filters	No	No	Array of Filter	• PolicyId - int64 - required: no - policy ID. • HostName - String - required: no - host name. • HostIp - String - required: no - host IP address. • ItemId - int64 - required: no - item ID. • RuleId - int64 - required: no - rule ID. • DetectStatus - int - required: no - detection status. • Level - int - required: no - risk level. • StartTime - String - required: no - start time. • EndTime - String - required: no - end time. Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10

Parameter name	Required	Allow NULL	Type	Description
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: DESC

3. Output Parameters

Parameter name	Type	Description
List	Array of BaselineHostDetect	Data returned. Example:View
Total	Int64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
FailedOperation	Operation failed.

DescribeBaselineHostIgnoreList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the servers on which the ignoring rule takes effect

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:28:44.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineHostIgnoreList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
RuleID	Yes	No	Int64	Rule ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
List	Array of BaselineHost	Data returned. Example:View
Total	Int64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidParameter	Invalid parameter.

DescribeBaselineHostRiskTop

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying top 5 baseline risks on servers

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 11:55:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineHostRiskTop
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
PolicyId	No	No	Int64	Policy ID. Example: 861027

3. Output Parameters

Parameter name	Type	Description
HostRiskTop5	Array of HostRiskLevelCount	Top 5 servers at risk. Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
FailedOperation	Operation failed.

DescribeBaselineItemDetectList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying baseline check items

Default interface request rate limit: 20 times per second.

Interface update time: 2022-10-13 10:14:09.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineItemDetectList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: [HostCount
Filters	No	No	Array of Filter	• HostId - string - Required or Not: No - Host Id • RuleId - int64 - Required or Not: No - Rule Id • PolicyId - int64 - Required or Not: No - Rule Id • ItemName - string - Required or Not: No - Item Name • DetectStatus - int - Required or Not: No - Detection Status • Level - int - Required or Not: No - Risk Level • StartTime - string - Required or Not: No - Start Time • EndTime - string - Required or Not: No - End Time Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: DESC

3. Output Parameters

Parameter name	Type	Description
List	Array of BaselineItemDetect	Data returned. Example:View
Total	Int64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
FailedOperation	Operation failed.

DescribeBaselineItemIgnoreList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the items in an ignoring rule

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 12:03:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineItemIgnoreList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid value: ID. Example: ID
Filters	No	No	Array of Filter	• CategoryId - int64 - Required or Not: No - Rule ID Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. Valid values: ASC (ascending order) and DESC (descending order). Example: ASC
RuleID	Yes	No	Int64	ID of the ignoring rule. Example: 1

3. Output Parameters

Parameter name	Type	Description
List	Array of	Data returned.

Parameter name	Type	Description
	BaselineItemInfo	Example:View
Total	Int64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

DescribeBaselineItemInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the information about baseline check items

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:38:03.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineItemInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Sorting column. Valid values: FirstTime and LastTime. Example: FirstTime
Filters	No	No	Array of Filter	• ItemId - int64 - required: no - item ID. • Level - int - required: no - risk level. • ItemName - String - required: no - detection item name. • RuleId - int - required: no - rule ID. Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 1
Offset	No	No	Int64	Offset. Default value: 0. Example: 1
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
CategoryList	Array of BaselineItemsCategory	Baseline category list. Example:View
List	Array of BaselineItemInfo	The rules. Example:View
Total	Int64	The number of entries. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

DescribeBaselineItemList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the baseline check results

Default interface request rate limit: 20 times per second.

Interface update time: 2022-10-13 10:13:14.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineItemList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Example: LastTime
Filters	No	No	Array of Filter	• PolicyId - int64 - Required or Not: No - Policy ID • RuleId - int64 - Required or Not: No - Rule ID • HostId - string - Required or Not: No - Host ID • HostName - string - Required or Not: No - Host Name • HostIp - string - Required or Not: No - Host IP • ItemId - String - Required or Not: No - Detection Item ID • ItemName - String - Required or Not: No - Item Name • DetectStatus - int - Required or Not: No - Detection Status [0: Failed
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: DESC

3. Output Parameters

Parameter	Type	Description

name		
List	Array of BaselineItem	Data returned. Example:View
Total	Int64	Total number. Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

DescribeBaselineItemRiskTop

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying top 5 baseline check items

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:35:07.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineItemRiskTop
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
PolicyId	No	No	Int64	Policy ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
RiskItemTop5	Array of BaselineRiskItem	Data returned. Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
FailedOperation	Operation failed.

DescribeBaselinePolicyList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying baseline policies

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 12:03:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselinePolicyList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: [RuleCount
Filters	No	No	Array of Filter	• PolicyName - String - Required: No - Policy name. Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 20
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
List	Array of BaselinePolicy	Data returned. Example:View
Total	Int64	Total number. Example: 19

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

DescribeBaselineRuleCategoryList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying baseline categories

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:22:40.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineRuleCategoryList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
List	Array of BaselineCategory	Data returned. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DescribeBaselineRuleDetectList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the baseline rule-based check list

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:35:47.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineRuleDetectList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: [HostCount
Filters	No	No	Array of Filter	• PolicyId - int64 - Required: No - Policy ID. • ItemId - int64 - Required: No - Item ID. • RuleName - string - Required: No - Rule name. • DetectStatus - int - Required: No - Check status. • StartTime - string - Required: No - Start time. • EndTime - string - Required: No - End time. Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: DESC

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
List	Array of BaselineRuleDetect	Data returned. Example:View
Total	Int64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

DescribeBaselineRuleIgnoreList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the baseline ignoring rule list

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-24 13:37:14.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineRuleIgnoreList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: [HostCount] Example: HostCount
Filters	No	No	Array of Filter	• RuleName - String - Required: No - Rule name. • ItemId- int - Required: No - ID of the check item. Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: DESC

3. Output Parameters

Parameter name	Type	Description
List	Array of BaselineRule	List Example:View

Parameter name	Type	Description
Total	Int64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

DescribeBaselineRuleList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying baseline rules

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 12:03:09.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineRuleList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Example: ID
Filters	No	No	Array of Filter	• RuleName - String - Required: No - Rule name. • CategoryId - int64 - Required: No - Rule category. -1: custom rule. • RuleType - int - Required: No - Rule type. 0: system rule. 1: custom rule. Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
List	Array of BaselineRule	Data returned. Example:View
Total	Int64	Total number. Example: 98
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

DescribeBaselineWeakPasswordList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying baseline weak passwords

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:29:50.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBaselineWeakPasswordList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: CreateTime and ModifyTime. Example: CreateTime
Filters	No	No	Array of Filter	• WeakPassword - string - Required: No - Weak password. Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. Valid values: ASC (ascending order) and DESC (descending order). Example: ASC

3. Output Parameters

Parameter name	Type	Description
List	Array of BaselineWeakPassword	List Example:View

Parameter name	Type	Description
Total	Int64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

DescribeHotVulTop

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Obtain Network-wide Hot Spot Vulnerabilities

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeHotVulTop
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
List	Array of VulStoreListInfo	Vulnerability information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeIgnoreHostAndItemConfig

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying information about check items and servers affected by the quick ignore feature

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 12:05:46.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeIgnoreHostAndItemConfig
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	• ItemId - int64 - required: no - item ID. • RuleId - int64 - required: no - rule ID. • HostId - String - required: no - host ID. Example:View

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
HostSet	Array of BaselineHost	Affected servers. Example:View
ItemSet	Array of BaselineItemInfo	Affected check items. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

DescribeVulStoreList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Obtain Vulnerability Database List

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVulStoreList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Optional sorting columns: [PublishDate]. Example: PublishDate
Filters	No	No	Array of Filter	• VulName- string - Required or Not: No - Vulnerability Name • CveId- string - Required or Not: No - CVEID • VulCategory- string - Required or Not: No - Vulnerability Classification 1 Web - CMS Vulnerabilities, 2 Application Vulnerabilities, 4 Linux Software Vulnerabilities, 5 Windows System Vulnerabilities • Method- string - Required or Not: No - Detection Method 0 Edition Comparison, 1 POC Detection • SupportDefense- string - Required or Not: No - Is Defense Supported 0 Not Supported, 1 Supported • FixSwitch- string - Required or Not: No - Is Auto-repair Supported 0 Not Supported, 1 Supported . Example:View
Limit	No	No	Int64	Maximum number of entries to return. Default value: 10. Maximum number: 100. Example: 10
Offset	No	No	Int64	Offset. Default value: 0. Example: 10
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
FreeSearchTimes	Uint64	Free Search Count Example: 102
List	Array of VulStoreListInfo	Vulnerability information. Example:View
Remaining	Uint64	Remaining Searches for Today Example: 10
TotalCount	Uint64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ExportBaselineFixList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting the fix list

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 12:29:02.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportBaselineFixList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ExportAll	No	No	Int64	0: exports only filtered results. 1: exports all results. Example: 1
Filters	No	No	Array of Filter	• ItemName- string - Required or Not: No - Item Name Example:View

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

ExportBaselineHostDetectList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting baseline checks on servers

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:36:37.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportBaselineHostDetectList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ExportAll	No	No	Int64	0: exports only filtered results. 1: exports all results. Example: 1
Filters	No	No	Array of Filter	• PolicyId - int64 - required: no - policy ID. • HostName - String - required: no - host name. • HostIp - String - required: no - host IP address. • ItemId - int64 - required: no - item ID. • RuleId - int64 - required: no - rule ID. • DetectStatus - int - required: no - detection status.

Parameter name	Required	Allow NULL	Type	Description
				• Level - int - required: no - risk level. • StartTime - String - required: no - start time. • EndTime - String - required: no - end time. Example:View
IsExportDetail	No	No	Int64	0: show the export interface; 1: export all result events Example: 0

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

ExportBaselineItemDetectList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting baseline check items

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:37:19.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportBaselineItemDetectList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ExportAll	No	No	Int64	0: exports only filtered results. 1: exports all results. Example: 1
Filters	No	No	Array of Filter	• HostId - string - Required or Not: No - Host Id • RuleId - int64 - Required or Not: No - Rule Id • PolicyId - int64 - Required or Not: No - Rule Id • ItemName - string - Required or Not: No - Item Name • DetectStatus - int - Required or Not: No - Detection Status • Level - int - Required or Not: No - Risk Level • StartTime - string - Required or Not: No - Start Time • EndTime - string - Required or Not: No - End Time Example:View

Parameter name	Required	Allow NULL	Type	Description
IsExportDetail	No	No	Int64	0: show the export interface; 1: export all result events Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

ExportBaselineItemList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting results of check items

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:38:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportBaselineItemList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ExportAll	No	No	Int64	0: exports only filtered results. 1: exports all results. Example: 1
Filters	No	No	Array of Filter	• PolicyId - int64 - Required or Not: No - Policy ID • RuleId - int64 - Required or Not: No - Rule ID • HostId - string - Required or Not: No - Host ID • HostName - string - Required or Not: No - Host Name • HostIp - string - Required or Not: No - Host IP • ItemId - String - Required or Not: No - Detection Item ID • ItemName - String - Required or Not: No - Item Name • DetectStatus - int - Required or Not: No - Detection Status [0: Failed

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

ExportBaselineRuleDetectList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting baseline check rules

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:36:56.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportBaselineRuleDetectList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ExportAll	No	No	Int64	0: exports only filtered results. 1: exports all results. Example: 1
Filters	No	No	Array of Filter	• PolicyId - int64 - Required: No - Policy ID. • ItemId - int64 - Required: No - Item ID. • RuleName - string - Required: No - Rule name. • DetectStatus - int - Required: No - Check status. • StartTime - string - Required: No - Start time. • EndTime - string - Required: No - End time. Example:View
IsExportDetail	No	No	Int64	0: show the export interface; 1: export all result events Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

ExportBaselineWeakPasswordList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting weak password configurations

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 12:05:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportBaselineWeakPasswordList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ExportAll	No	No	Int64	0: exports only filtered results. 1: exports all results. Example: 0
Filters	No	No	Array of Filter	• WeakPassword - string - Required: No - Weak password. Example:View

3. Output Parameters

Parameter	Type	Description

name		
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

FixBaselineDetect

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for fixing risks based on baseline checks

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 12:05:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: FixBaselineDetect
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Data	No	No	Array of String	Fix content. Example: ["1ce68339-8828-457f-b358-d5b1b34e4fe9"]
HostId	Yes	No	String	Server ID. Example: 1ce68339-8828-457f-b358-d5b1b34e4fe9
ItemId	Yes	No	Int64	Item ID. Example: 10001

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
FailedOperation	Operation failed.

ModifyBaselinePolicy

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for modifying the baseline policy settings

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 12:07:43.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyBaselinePolicy
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Data	Yes	No	BaselinePolicy	Data content Example:View
Filters	No	No	Array of Filter	• RuleName - String - Required: No - Rule name. • CategoryId - int64 - Required: No - Rule category. -1: custom rule. • RuleType - int - Required: No - Rule type. 0: system rule. 1: custom rule. Example:View
SelectAll	No	No	Int64	Specifies whether to select all. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
FailedOperation	Operation failed.

ModifyBaselinePolicyState

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for changing the status of a baseline policy

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-17 16:05:09.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyBaselinePolicyState
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
IsEnabled	Yes	No	Int64	Enabling status: [1: Enabled
PolicyId	Yes	No	Int64	Policy ID. Example: 638392

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request

Parameter name	Type	Description
		needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

ModifyBaselineRule

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for modifying baseline check rules

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 12:06:12.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyBaselineRule
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
CategoryIds	No	No	Array of Uint64	Selected detection item category. Example: [100,101]
Data	Yes	No	BaselineRule	Data content Example:View
ExcludeIds	No	No	Array of Uint64	ID of the detection item to be excluded. Example: [142]
Filters	No	No	Array of Filter	• ItemName - string - Required: No - Item name. Example:View

Parameter name	Required	Allow NULL	Type	Description
IdType	No	No	Uint64	0: detection item, 1: detection item category. Example: 0
SelectAll	No	No	Int64	Specifies whether to select all. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
FailedOperation	Operation failed.

ModifyBaselineRuleIgnore

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for modifying baseline ignoring rules

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 12:06:22.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyBaselineRuleIgnore
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
AssetType	Yes	No	Int64	Asset type. 0: all servers with CWP Pro and all servers with CWP Ultimate. 1: server ID. 2: server IP address. Example: 0
Filters	No	No	Array of Filter	• ItemName - string - Required: No - Item name. Example:View
HostIds	No	No	Array of String	Server ID. Example: ["4c4c4544-0053-4d10-8052-c4c04f53ayay"]
HostIps	No	No	Array of String	IP address of the server. Example: ["172.10.0.0"]
ItemIds	No	No	Array of Int64	Associated item IDs. Example: [1000]
RuleId	No	No	Int64	Rule ID. Example: 100
RuleName	Yes	No	String	Rule Name Example: Redis Check
SelectAll	No	No	Int64	Specifies whether to select all. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
FailedOperation	Operation failed.

ModifyBaselineWeakPassword

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for modifying or creating a weak password

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:30:52.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyBaselineWeakPassword
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Data	Yes	No	Array of BaselineWeakPassword	Data content Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request

Parameter name	Type	Description
		needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

StartBaselineDetect

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for starting a baseline check

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:33:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: StartBaselineDetect
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Param	Yes	No	BaselineDetectParam	Baseline check parameter. Example:View

3. Output Parameters

Parameter name	Type	Description
TaskId	Int64	ID of the scan task. Example: 1

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
FailedOperation	Operation failed.

StopBaselineDetect

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for stopping baseline checks

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:33:39.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: StopBaselineDetect
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
TaskIds	Yes	No	Array of Int64	IDs of the tasks that you want to stop. Example: [1106788]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.

SyncBaselineDetectSummary

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for synchronizing the summary information about the baseline check progress

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-23 15:34:11.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: SyncBaselineDetectSummary
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
TaskIds	No	No	Array of Uint64	IDs for calculating the progress of ongoing check tasks. Generally, this parameter is not required. Example: [1024]

3. Output Parameters

Parameter name	Type	Description
DetectingTaskIds	Array of Int64	IDs of the running check tasks. Example: [1002]
EndTime	String	End time. Example: 2020-11-21 15:16:00
HostCount	Int64	Total number of hosts. Example: 0
LeftMins	Int64	Remaining time for the scan. Unit: minutes. Example: 1
NotPassPolicyCount	Int64	Total number of policies against which the check failed. Example: 0
ProgressRate	Int64	Handling progress. Example: 70
StartTime	String	Start time. Example: 2020-11-21 15:16:00
WillFirstScan	Int64	1: about to perform the first scan. 0: has been scanned. Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
FailedOperation	Operation failed.

Expert Service APIs DescribeEmergencyResponseList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the emergency response list in the expert service module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeEmergencyResponseList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: StartTime and EndTime. Example: StartTime
Filters	No	No	Array of Filters	Filter conditions. • Keyword - String - Required: No - Keyword for filtering. • Status - String - Required: No - Status. Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10
Offset	No	No	Uint64	Offset. Example: 0

Parameter name	Required	Allow NULL	Type	Description
Order	No	No	String	Sorting order. Example: desc

3. Output Parameters

Parameter name	Type	Description
List	Array of EmergencyResponseInfo	API for querying the emergency response list Example:View
TotalCount	Uint64	Total number. Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeMonthInspectionReport

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the monthly inspection reports provided by the security manager service in the expert service module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMonthInspectionReport
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Limit	Yes	No	Uint64	Page size. Example: 10
Offset	Yes	No	Uint64	Offset of the paginated query results. Example: 10

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
List	Array of MonthInspectionReport	List of inspection reports. Example:View
TotalCount	Uint64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
ResourceInsufficient	Insufficient resource.
LimitExceeded	The quota limit has been reached.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

Intrusion Detection - APIs of Logins from Unusual Locations DeleteLoginWhiteList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete a login allowlist rule.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteLoginWhiteList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	IDs of allowlist entries. You can specify up to 100 IDs in each request. Example: [36040272]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DeleteNonlocalLoginPlaces

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete unusual login location records.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteNonlocalLoginPlaces
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
DelType	No	No	String	Method to delete login events from unusual locations. Valid values: Ids, Ip, and All. Default value: Ids. Example: Ip
Ids	No	No	Array of Uint64	IDs of login events from unusual locations. This parameter is required when the DelType parameter is set to Ids or left empty. Example: [202417010656750]
Ip	No	No	Array of String	IP address of the login event from an unusual location. This parameter is required when the DelType parameter is set to Ip. Example: ["1.1.1.1"]
Uuid	No	No	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeHostLoginList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying login audits

Default interface request rate limit: 20 times per second.

Interface update time: 2022-06-06 17:19:32.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeHostLoginList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. LoginTime: occurrence time. Example: LoginTime
Filters	No	No	Array of Filter	Filtering conditions. • Quuid - String - required: no - CVM UUID. • Uuid - String - required: no - CWP unique UUID. • MachineName - String - required: no - host alias. • Ip - String - required: no - host IP address. • InstanceID - String - required: no - host instance ID. • SrcIp - String - required: no - filter by source IP address. • UserName - String - required: no - filter by username. • Status - String - required: no - filter by status: 1: logged in normally; 5: allowlisted; 14: processed; 15: ignored. • LoginTimeBegin - String - required: no - filter by modification time; start time. • LoginTimeEnd - String - required: no - filter by modification time; end time. • RiskLevel - String - required: no - filter by risk level: 0: high; 1: suspicious.

Parameter name	Required	Allow NULL	Type	Description
				Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 1
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc

3. Output Parameters

Parameter name	Type	Description
HostLoginList	Array of HostLoginList	List of login audits. Example:View
TotalCount	Uint64	Total number. Example: 12
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter.DateRange	The time range format is incorrect.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeLoginWhiteCombinedList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the login allowlist after merging

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-15 10:50:58.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLoginWhiteCombinedList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filtering conditions. • IpOrAlias - String - required: no - filter by host IP address or alias. • UserName - String - required: no - filter by username. • SrcIP - String - required: no - filter by source IP address. • Location - String - required: no - filter by login location. • ModifyBeginTime - String - required: no - filter by modification time; start time. • ModifyEndTime - String - required: no - filter by modification time; end time. Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
LoginWhiteCombinedInfos	Array of LoginWhiteCombinedInfo	Allowlist entries after merging. Example:View

Parameter name	Type	Description
TotalCount	Uint64	Total number. Example: 12
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeLoginWhiteList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to get the list of login allowlist entries.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLoginWhiteList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter condition. • IpOrAlias - String - Required: No - Query keyword. • UserName - String - Required: No - Username. • ModifyBeginTime - String - Required: No - Beginning of the modification time range. • ModifyEndTime - String - Required: No - End of the modification time range. Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
LoginWhiteLists	Array of LoginWhiteLists	Entries in the login allowlist. Example:View
TotalCount	Uint64	Total number of records. Example: 12
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeUsualLoginPlaces

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query usual login locations.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeUsualLoginPlaces
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Uuid	Yes	No	String	CWP client UUID. Example: d1245804-b922-4c3b-8499-f95dce26b33c

3. Output Parameters

Parameter name	Type	Description
UsualLoginPlaces	Array of UsualPlace	Usual login locations. Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ExportNonlocalLoginPlaces

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export unusual login location events into a CSV file.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportNonlocalLoginPlaces
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filtering conditions. • Quuid - String - required: no - CVM UUID. • Uuid - String - required: no - CWP unique UUID. • MachineName - String - required: no - host alias. • Ip - String - required: no - host IP address. • InstanceID - String - required: no - host instance ID. • SrcIp - String - required: no - filter by source IP address. • UserName - String - required: no - filter by username. • Status - String - required: no - filter by status: 1: logged in normally; 5: allowlisted; 14: processed; 15: ignored. • LoginTimeBegin - String - required: no - filter by modification time; start time. • LoginTimeEnd - String - required: no - filter by modification time; end time. • RiskLevel - String - required: no - filter by risk level: 0: high; 1: suspicious. Example:View

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	This parameter has been deprecated. Example: http://www.ay.com/ay
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
FailedOperation.Export	Failed to export.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

Intrusion Detection - File Scanning and Cleaning APIs
CreateNetAttackWhiteList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Yunapi Response

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateNetAttackWhiteList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
DealOldEvents	No	No	Uint64	Whether to allowlist all alarms that match this rule: 1: Yes, 0: No. Example: 1
Description	No	No	String	Description Example: any create description
EventId	No	No	Uint64	Event ID. Example: 1
QuuidList	No	No	Array of String	List of QUUIDs. Example: ["5a540076-d38a-4078-aa98-qwert371d322"]
Scope	Yes	No	Uint64	Specifies whether to take effect on all servers. 0: no. 1: yes. Example: 1
SrcIp	Yes	No	Array of String	Source IP. Single IP: 1.1.1.1, IP Range: 1.1.1.1-1.1.2.1, IP Range: 1.1.1.0/24 Example: ["1.1.1.1"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

CreateScanMalwareSetting

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to configure the file scanning and cleaning settings in the intrusion detection module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-03 19:52:53.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateScanMalwareSetting
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
EnableMemShellScan	No	No	Int64	Whether to enable malicious process killing [0: Not Enabled; 1: Enabled]. Example: 1
EngineType	No	No	Uint64	1: standard mode (only critical and high-risk issues are reported). 2: enhanced mode (critical, high-risk, and medium-risk issues are reported). 3: strict mode (critical, high-risk, medium-risk, low-risk, and informational issues are reported). Example: 2
HostType	Yes	No	Int64	Server type. 1: server with CWP Pro. 2: selected server. Example: 1
QuuidList	No	No	Array of String	QUUIDs of servers. This parameter takes effect if the HostType parameter is set to 2 (selected server). Example: ["a15a2cac-0bea-478d-a5d0-f54be8ayayay""]
ScanPattern	Yes	No	Uint64	Scan mode. 0: full-disk scan. 1: quick scan. Example: 1
TimeoutPeriod	No	No	Uint64	Timeout period. Unit: seconds. Default value: 3600. Example: 1

3. Output Parameters

Parameter name	Type	Description
TaskId	Uint64	Task ID. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

Error Code	Description
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter.DateRange	The time range format is incorrect.
FailedOperation.APIServerFail	Failed to call the API service.
FailedOperation.NoProfessionHost	No servers with CWP Pro exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

DeleteMalwareScanTask

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for stopping a trojan scan task in the intrusion management module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteMalwareScanTask
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
FailedOperation.APIServerFail	Failed to call the API service.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

DeleteMalwares

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete trojan records.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteMalwares
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	IDs of trojan records. You can specify up to 100 IDs in each request. Example: [1]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameterValue	The parameter value is invalid.

DeleteNetAttackWhiteList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Yunapi Response

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteNetAttackWhiteList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	Array of IDs. You can specify up to 100 IDs in each request. Example: [1]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeJavaMemShellList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying Java memory trojan events

Default interface request rate limit: 20 times per second.

Interface update time: 2022-04-22 09:49:39.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeJavaMemShellList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filtering conditions: InstanceID (instance ID for query), IP (IP address for query), MachineName (host name for fuzzy query), Type (host type for query), Status (status for exact match), CreateBeginTime (start time of query creation), and CreateEndTime (end time of query creation). Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
List	Array of JavaMemShellInfo	Event list. Example:View
TotalCount	Uint64	Total number. Example: 12
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeMalWareList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the trojan list in the intrusion detection module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-02-22 18:20:24.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMalWareList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid value: CreateTime. Example: CreateTime
Filters	No	No	Array of Filter	Filter conditions. • IpOrAlias - String - Required: No - Host IP address or alias for filtering. • FilePath - String - Required: No - Path for filtering. • VirusName - String - Required: No - Virus name for filtering. • CreateBeginTime - String - Required: No - Creation start time for filtering. • CreateEndTime - String - Required: No - Creation end time for filtering. • Status - String - Required: No - Status for filtering. 4: to be handled; 5: trusted; 6: isolated; 10: isolating; 11: canceling isolation; 14: handled. Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sort method: ASC, DESC. Example: ASC

3. Output Parameters

Parameter name	Type	Description
MalWareList	Array of MalWareList	List of trojans. Example:View
TotalCount	Uint64	Total number. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeMalwareFile

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the download URL of a trojan file

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMalwareFile
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	Uint64	ID of the trojan record. Example: 1

3. Output Parameters

Parameter name	Type	Description
FileName	String	Saved filename. Example: tmp

Parameter name	Type	Description
FileUrl	String	Download URL of the trojan file. Example: www.domain.com/1.txt
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeMalwareInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the details of a malicious file

Default interface request rate limit: 20 times per second.

Interface update time: 2021-12-09 20:22:45.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMalwareInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	Int64	Unique ID. Example: 1023290

3. Output Parameters

Parameter name	Type	Description
MalwareInfo	MalwareInfo	Details of the malicious file. Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
FailedOperation.APIServerFail	Failed to call the API service.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeMalwareRiskWarning

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query whether alarms are generated for detected malicious files in the intrusion detection module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-03 19:53:29.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMalwareRiskWarning
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
IsCheckRisk	Bool	Indicates whether automatic scanning is enabled. true: enabled. false: not enabled. Example: true
IsPop	Bool	Indicates whether the system displays pop-up messages. true: displays pop-up messages. false: does not display pop-up messages. Example: true
List	Array of MalwareRisk	List of files at risk. Example:View
ProcessList	Array of MalwareRisk	Information on Abnormal Process List Example:View

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DescribeMalwareTimingScanSetting

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the scheduled scan configuration

Default interface request rate limit: 20 times per second.

Interface update time: 2022-10-25 19:31:47.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMalwareTimingScanSetting
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
AutoIsolation	Uint64	Indicates whether auto-quarantine is enabled. 1: enabled. 0: not enabled. Example: 1
CheckPattern	Uint64	Scan mode. 0: full-disk scan. 1: quick scan. Example: 1
ClickTimeout	Uint64	Timeout period for the quick scan, such as 1800 seconds. Example: 60
Cycle	Uint64	Scan cycle. 1: every day. Example: 1
EnableInspiredEngine	Uint64	Heuristic Engine: 0 - OFF, 1 - ON Example: 1
EnableMemShellScan	Uint64	Whether to enable malicious process killing [0: Not Enabled; 1: Enabled] Example: 1
EnableScan	Int64	Indicates whether scheduled scanning is enabled. 0: disabled. 1: enabled. Example: 1
EndTime	String	End time of the scan. Example: 18:00
EngineType	Uint64	1: standard mode (only critical and high-risk issues are reported). 2: enhanced mode (critical, high-risk, and medium-risk issues are reported). 3: strict mode (critical, high-risk, medium-risk, low-risk, and informational issues are reported). Example: 1
Id	Int64	Unique ID. Example: 1
IsGlobal	Uint64	Specifies whether to specify all servers. 1: all servers. 2: selected servers. Example: 1
KillProcess	Uint64	Indicates whether to kill the process. 1: kills the process. 0: does not kill the process. This parameter takes effect only when the AutoIsolation parameter is set to 1. Example: 1
MonitoringPattern	Uint64	Monitoring mode. 0: standard mode. 1: deep mode. Example: 1
ProtectFileScope	Uint64	Scope of detection: 0: malicious files other than scripts; 1: all malicious files Example: 0
ProtectMode	Uint64	Protection mode: 0 - standard; 1 - enhanced Example: 0
QuuidList	Array of String	QUUIDs of servers. This parameter is required if you set IsGlobal to 2. Example: ["972290ce-2e07-4689-8f92-f617239bbf82"]
RealTimeMonitoring	Int64	Indicates whether real-time monitoring is enabled. 0: disabled. 1: enabled. Example: 1
StartTime	String	Start time of the scan. Example: 00:00
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DescribeNetAttackWhiteList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Yunapi Response

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeNetAttackWhiteList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: [CreateTime] Example: CreateTime
Filters	No	No	Array of Filter	Filter criteria. • IP - String - Required or Not: No - Host IP Query • SrcIP- String - Required or Not: No - Allowlist IP Query . Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Total number of records. Example: 4
WhiteList	Array of NetAttackWhiteRule	Allowlist list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeScanMalwareSchedule

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the trojan scan progress

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeScanMalwareSchedule
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
IsSchedule	Bool	Indicates whether it is being scanned. Example: true
RiskFileNumber	Int64	Number of files at risk. This value is returned when the progress reaches 100%. Example: 1
ScanStatus	Uint64	0: never scanned. 1: scanning. 2: scan completed. 3: stopping. 4: stopped. Example: 1

Parameter name	Type	Description
Schedule	Int64	Scan progress in percentage. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeServersAndRiskAndFirstInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the number of pending files at risk, the number of affected servers, and the last scan time.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeServersAndRiskAndFirstInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
AddRiskFileCount	Uint64	Number of newly added files at risk on the current day. Example: 1
IsFirstCheck	Bool	Indicates whether it is the first scan. true: yes. false: no. Example: true

Parameter name	Type	Description
RiskFileCount	Uint64	Number of files at risk. Example: 1
ScanTime	String	Last trojan scan time. Example: 2024-10-28 20:23:23
ServersCount	Uint64	Number of affected servers. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

ExportMalwares

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export trojan records into a CSV file.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportMalwares
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Sorting field. Valid values: CreateTime and LatestScanTime. Example: CreateTime
Filters	No	No	Array of Filters	Filter parameters. • MachineName - String - Required: No - Host name. • FilePath - String - Required: No - Path for filtering. • VirusName - String - Required: No - Virus name for filtering. • CreateBeginTime - String - Required: No - Creation start time for filtering. • CreateEndTime - String - Required: No - Creation end time for filtering. • Status - String - Required: No - Status for filtering. 4: to be handled; 5: file trusted; 6: isolated; 8: file deleted; 10: isolating; 11: canceling isolation; 14: handled. Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Default value: 10. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. Valid values: ASC and DESC. Example: ASC

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	This parameter has been deprecated. Example: http://www.ay.com/ay
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.

Error Code	Description
ResourceNotFound	The resource does not exist.
FailedOperation.Export	Failed to export.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

ModifyMalwareTimingScanSettings

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for setting scheduled scans

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-03 19:52:01.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyMalwareTimingScanSettings
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
AutoIsolation	No	No	Uint64	Specifies whether to enable the auto-quarantine feature. 1: enables the feature. 2: disables the feature. Example: 1
CheckPattern	Yes	No	Uint64	Scan mode. 0: full-disk scan. 1: quick scan. Example: 1
Cycle	Yes	No	Uint64	Scan cycle. By default, the system performs scans once every day. Example: 1
DoClean	No	No	Uint64	1: Clean. 0: Do not clean. • This operation will repair tampered system commands, scheduled tasks, and other system files. Ensure yum/apt is available during the operation. Example: 1
EnableInspiredEngine	No	No	Uint64	Heuristic Engine Switch: 0 OFF, 1 ON. Example: 1
EnableMemShellScan	No	No	Uint64	Whether to enable malicious process killing [0: Not Enabled; 1: Enabled]. Example: 1
EnableScan	Yes	No	Uint64	Specifies whether to enable the scheduled scan feature. 0: disables the feature. 1: enables the feature. Example: 1
EndTime	Yes	No	String	End time of the scan, such as 04:00:00. Example: 02:00:00
EngineType	No	No	Uint64	1: standard mode (only critical and high-risk issues are reported). 2: enhanced mode (critical, high-risk, and medium-risk issues are reported). 3: strict mode (critical, high-risk, medium-risk, low-risk, and informational issues are reported). Example: 1
IsGlobal	Yes	No	Uint64	Specifies whether to specify all servers. 1: all servers. 2: selected servers. Example: 1
KillProcess	No	No	Uint64	Specifies whether to kill the process. 1: kills the process. 0: does not kill the process. Example: 1
MonitoringPattern	Yes	No	Uint64	Monitoring mode. 0: standard mode. 1: deep mode. Example: 1
ProtectFileScope	No	No	Uint64	Scope of detection: 0: malicious files other than scripts; 1: all malicious files Example: 0
ProtectMode	No	No	Uint64	Protection mode: 0: standard; 1: important period guarantee Example: 0

Parameter name	Required	Allow NULL	Type	Description
QuuidList	No	No	Array of String	QUUIDs of servers. This parameter is required if you set IsGlobal to 2. Example: ["5a540076-d38a-4078-aa98-q45rt371d322"]
RealTimeMonitoring	Yes	No	Uint64	Specifies whether to enable real-time monitoring. 0: disables real-time monitoring. 1: enables real-time monitoring. Example: 1
StartTime	Yes	No	String	Start time of the scan, such as 02:00:00. Example: 00:00:00

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter.DateRange	The time range format is incorrect.
FailedOperation.APIServerFail	Failed to call the API service.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

ModifyNetAttackWhiteList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Yunapi Response

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyNetAttackWhiteList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
DealOldEvents	Yes	No	Uint64	Whether to allowlist all alarms that match this rule: 1: Yes, 0: No. Example: 1
Description	No	No	String	Rule description Example: from redis node check
Id	Yes	No	Uint64	Rule ID. Example: 1
QuuidList	No	No	Array of String	List of QUUIDs. Example: ["1c26308c-5493-4eaf-a817-112ec25f499e"]
Scope	Yes	No	Uint64	Specifies whether to take effect on all servers. 0: no. 1: yes. Example: 1
SrcIp	Yes	No	Array of String	Source IP. Single IP: 1.1.1.1, IP Range: 1.1.1.1-1.1.2.1, IP Range: 1.1.1.0/24 Example: ["1.1.1.1"]

3. Output Parameters

Parameter	Type	Description

name		
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

RecoverMalwares

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to recover isolated trojan files in a batch.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: RecoverMalwares
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	Up to 100 trojan IDs. Example: [1002,1003]

3. Output Parameters

Parameter name	Type	Description
FailedIds	Array of Uint64	IDs of trojan files that failed to be recovered. If no trojan files failed to be recovered, this parameter returns an empty string. Example: [1003]
SuccessIds	Array of Uint64	IDs of trojan files that are successfully recovered. If no trojan files are successfully recovered, this parameter returns an empty string. Example: [1002]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
FailedOperation.Recover	Failed to recover the trojan.
InvalidParameter	Invalid parameter.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

SeparateMalwares

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to isolate trojans.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: SeparateMalwares
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	IDs of trojan events. You can specify a maximum of 100 IDs. Example: [300005850594]
KillProcess	No	No	Bool	Specifies whether to kill the process. Example: true

3. Output Parameters

Parameter name	Type	Description
FailedIds	Array of Uint64	Unsuccessfully isolated arrays of IDs; if none, an empty array is returned. Example: [300005850595]
SuccessIds	Array of Uint64	Successfully isolated arrays of IDs; if no array is successfully isolated, an empty array is returned. Example: [300005850594]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
FailedOperation.PartSeparate	Failed to isolate all or part of servers.
FailedOperation.SingleSeparate	Failed to isolate a single server.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

TrustMalwares

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to trust an identified trojan file.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: TrustMalwares
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	Up to 100 trojan IDs. Example: [300005556389]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

UntrustMalwares

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to untrust a trojan file.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: UntrustMalwares
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	Up to 100 trojan IDs. Example: [300005556389]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

Intrusion Detection - High-Risk Command APIs CheckBashRuleParams

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to check the parameters that you use to create or modify a custom anti-high-risk command rule.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CheckBashRuleParams
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
CheckField	Yes	No	String	Name or rule of the check content. If both need to be checked, separate them with commas (,). Example: Name,Rule
EventId	No	No	Uint64	ID of the event required for adding allowlist entries in the event list. Example: 10003
Id	No	No	Uint64	Rule ID required for the modification. Example: 3680
Name	No	No	String	Rule name. Example: Rule 1
Rule	No	No	String	Regular expression, which must match the command corresponding to the specified event ID. Example: rm -rf /tmp/tmp

3. Output Parameters

Parameter name	Type	Description
ErrCode	Uint64	0: the check is passed. 1: the rule name has failed the check. 2: failed to pass the regular expression check. Example: 2
ErrMsg	String	Error message. Example: OK
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
InvalidParameter	Invalid parameter.

DeleteBashEvents

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete high-risk command events based on IDs.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteBashEvents
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	ID array. Up to 1,000 items are allowed. Example: [1002]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DeleteBashRules

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for deleting anti-high-risk command rules

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteBashRules
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	Array of IDs. You can specify up to 100 IDs in each request. Example: [1,23,100]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter.DateRange	The time range format is incorrect.
InvalidParameter.RegexRuleError	The format of the regular expression parameter is invalid.

DescribeBashEvents

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying high-risk commands

Default interface request rate limit: 20 times per second.

Interface update time: 2022-06-06 14:53:54.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBashEvents
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. CreateTime: occurrence time. ModifyTime: processing time. Example: CreateTime
Filters	No	No	Array of Filter	Filtering conditions. • HostName - String - required: no - host name. • Hostip - String - required: no - host's private IP address. • RuleCategory - Int - required: no - policy type (all types or a single type): 0: system; 1: user. • RuleName - String - required: no - policy name. • RuleLevel - Int - required: no - threat level (multiple levels supported). • Status - Int - required: no - processing status (multiple statuses supported): 0: pending; 1: processed; 2: allowlisted; 3: ignored; 4: deleted; 5: blocked. • DetectBy - Int - required: no - data source (multiple sources supported): 0: bash logs; 1: real-time monitoring. • StartTime - String - required: no - start time. • EndTime - String - required: no - end time. Example:View
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc

3. Output Parameters

Parameter name	Type	Description
List	Array of BashEvent	List of high-risk command events. Example:View
TotalCount	Uint64	Total number. Example: 1021

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBashEventsNew

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying high-risk commands (new)

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-19 20:56:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBashEventsNew
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. CreateTime: occurrence time. ModifyTime: processing time. Example: CreateTime
Filters	No	No	Array of Filter	Filter condition. • HostName - String - Required: No - Server name. • Hostip - String - Required: No - Private IP of the server. • HostIp - String - Required: No - Private IP of the server. • RuleCategory - Int - Required: No - Policy type. You can specify one type or all types. 0: system rule. 1: custom rule. • RuleName - String - Required: No - Rule name. • RuleLevel - Int - Required: No - One or more risk severity levels. • Status - Int - Required: No - One or more handling statuses. 0: pending. 1: handled. 2: added to the allowlist. 3: ignored. 4: deleted. 5: blocked. • DetectBy - Int - Required: No - One or more data sources. 0: bash log. 1: real-time monitoring. • StartTime - String - Required: No - Start time. • EndTime - String - Required: No - End time. Example:View
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc

3. Output Parameters

Parameter name	Type	Description
List	Array of BashEventNew	List of high-risk command events. Example:View
TotalCount	Uint64	Total number. Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

DescribeBashRules

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying anti-high-risk command rules

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBashRules
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filtering conditions. • Name - String - required: no - rule name. • Rule - String - required: no - rule content. • Level - Int - required: no - threat level. • White - Int - required: no - allowlist type. • RuleCategory - Int - required: no - policy type. • BashAction - Int - required: no - operation action. • Status - Int - required: no - effective status. Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

Parameter name	Required	Allow NULL	Type	Description
Type	Yes	No	Uint64	0: system rule. 1: custom rule. Example: 1

3. Output Parameters

Parameter name	Type	Description
List	Array of BashRule	The entries returned. Example:View
TotalCount	Uint64	Total number. Example: 12
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

EditBashRules

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for creating or modifying an anti-high-risk command rule

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: EditBashRules
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
DealOldEvents	No	No	Uint64	Whether to add previous events to the allowlist. 0: no. 1: yes. Example: 1
EventId	No	No	Uint64	ID of the event, which must be passed in when you add the event to the allowlist. Example: 10023
HostIp	No	No	String	Server IP address. Example: 1.1.1.1
Id	No	No	Uint64	Rule ID. If you want to create a rule, leave this parameter empty. Example: 1
IsGlobal	No	No	Uint64	Specifies whether it is a global rule. 1: yes. 2: no. Default value: 0. Example: 1
Level	No	No	Uint64	Risk severity. 0: no risk. 1: high. 2: medium. 3: low. Example: 1
Name	No	No	String	Rule name. If you want to modify a rule, the rule name cannot be changed. Example: Rule name
Rule	No	No	String	This API is deprecated. Use the ModifyBashPolicy API instead. Example: sh cmdline
Uuids	No	No	Array of String	Agent IDs. Example: ["05f0bcab-726c-4ea4-8109-bcd03d5598f7"]
White	No	No	Uint64	0: blocklist. 1: allowlist. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.RegexRuleError	The format of the regular expression parameter is invalid.
InvalidParameter.RuleHostipErr	Incorrect server IP address for a rule API.
InvalidParameter.IpNoValid	Invalid IP address format.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ExportBashEvents

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting high-risk command events

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportBashEvents
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filtering conditions. • HostName - String - required: no - host name. • Hostip - String - required: no - host's private IP address. • RuleCategory - Int - required: no - policy type (all types or a single type): 0: system; 1: user. • RuleName - String - required: no - policy name. • RuleLevel - Int - required: no - threat level (multiple levels supported). • Status - Int - required: no - processing status (multiple statuses supported): 0: pending; 1: processed; 2: allowlisted; 3: ignored; 4: deleted; 5: blocked. • DetectBy - Int - required: no - data source (multiple sources supported): 0: bash logs; 1: real-time monitoring. • StartTime - String - required: no - start time. • EndTime - String - required: no - end time. Example:View

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	Download URL of the exported file. Example: http://www.ay.com/ay
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description

Error Code	Description
InternalError	Internal error.
FailedOperation.Export	Failed to export.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

SetBashEventsStatus

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for setting the status of high-risk command events

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: SetBashEventsStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	Array of IDs. You can specify up to 100 IDs in each request. Example: [1,2]
Status	Yes	No	Uint64	New status. 0: to be handled. 1: high risk. 2: normal. Example: 1

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameterValue	The parameter value is invalid.

SwitchBashRules

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for changing the status of anti-high-risk command rules

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: SwitchBashRules
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Disabled	Yes	No	Uint64	Whether to disable the rule. Example: 1
Id	Yes	No	Uint64	Rule ID. Example: 1

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter.DateRange	The time range format is incorrect.
InvalidParameter.RegexRuleError	The format of the regular expression parameter is invalid.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

Intrusion Detection - Local Privilege Escalation APIs DeletePrivilegeEvents

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete local privilege escalation events based on IDs.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeletePrivilegeEvents
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	Array of up to 100 IDs. Example: [1,2,3]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DeletePrivilegeRules

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for deleting anti-local privilege escalation rules

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeletePrivilegeRules
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	Array of IDs. You can specify up to 100 IDs in each request. Example: [1,2]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter.DateRange	The time range format is incorrect.
InvalidParameter.RegexRuleError	The format of the regular expression parameter is invalid.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribePrivilegeEvents

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying local privilege escalation events

Default interface request rate limit: 20 times per second.

Interface update time: 2022-06-06 15:33:40.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribePrivilegeEvents
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. CreateTime: occurrence time. Example: CreateTime
Filters	No	No	Array of Filter	Filter conditions. • CreateBeginTime - String - Required: No - Creation start time. • CreateEndTime - String - Required: No - Creation end time. • Status - String - Required: No - Handling status. 0: to be handled; 2: allowlisted; 3: handled; 4: ignored; 5: deleted. • ParentProcName - String - Required: No - Parent process. • InstanceID - String - Required: No - Host instance ID. • IP - String - Required: No - Host IP address. • MachineName - String - Required: No - Host name. Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: desc

3. Output Parameters

Parameter name	Type	Description
List	Array of PrivilegeEscalationProcess	Data returned. Example:View
TotalCount	Uint64	Total number. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribePrivilegeRules

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying anti-local privilege escalation rules

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribePrivilegeRules
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter conditions. • Keywords - String - Required: No - Keyword (process name). • SMode - String - Required: No - Whether the process is an S-privilege process. 1: yes; 0: no. Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
List	Array of PrivilegeRule	The entries returned. Example:View
TotalCount	Uint64	Total number. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ExportPrivilegeEvents

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting local privilege escalation events

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportPrivilegeEvents
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter conditions. • CreateBeginTime - String - Required: No - Creation start time. • CreateEndTime - String - Required: No - Creation end time. • Status - String - Required: No - Handling status. 0: to be handled; 2: allowlisted; 3: handled; 4: ignored; 5: deleted. • ParentProcName - String - Required: No - Parent process. • InstanceID - String - Required: No - Host instance ID. • IP - String - Required: No - Host IP address. • MachineName - String - Required: No - Host name. Example:View

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	This parameter has been deprecated. Example: http://www.ay.com/ay
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 1596595610
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
FailedOperation.Export	Failed to export.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

Intrusion Detection - Malicious Request APIs DeleteMaliciousRequests

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete malicious request records.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteMaliciousRequests
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	IDs of malicious request records. You can specify up to 100 IDs in each request. Example: [1002]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

Error Code	Description
InvalidParameter.ParsingError	Parameter parsing error.
MissingParameter	Missing parameter.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeMaliciousRequestWhiteList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the allowlist of the Anti-Malicious Requests feature

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMaliciousRequestWhiteList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Sorting field. Valid values: CreateTime and LatestScanTime. Example: CreateTime
Filters	No	No	Array of Filters	Filter conditions. • Domain - String - Base64-encoded domain name. Example:View
Limit	Yes	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	Yes	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting Method: [ASC: Ascending Order, DESC: Descending Order] Example: ASC

3. Output Parameters

Parameter name	Type	Description
List	Array of MaliciousRequestWhiteListInfo	Allowlist information. Example:View

Parameter name	Type	Description
TotalCount	Uint64	Total number of records returned for the paginated query. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeRiskDnsList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the malicious request list in the intrusion detection module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-06-06 14:42:23.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeRiskDnsList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. AccessCount: number of requests. MergeTime: most recent access time. Example: AccessCount
Filters	No	No	Array of Filter	Filter condition. • IpOrAlias - String - Required: no - host IP or alias filter. • Url - String - Required: No - URL. • Status - String - Required: No - Status. 0: to be handled. 2: trusted. 3: untrusted. • MergeBeginTime - String - Required: No - Beginning of the most recent access time range. • MergeEndTime - String - Required: No - End of the most recent access time range. Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RiskDnsList	Array of RiskDnsList	List of malicious requests. Example:View
TotalCount	Uint64	Total number. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ExportMaliciousRequests

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export the malicious request file into a CSV file for download.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportMaliciousRequests
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter conditions. • IpOrAlias - String - Required: No - Host IP address or alias for filtering. • Url - String - Required: No - Access domain name for filtering. • Status - String - Required: No - Status for filtering. 1: deleted; 0: to be handled; 2: allowlisted; 3: removed from the allowlist; 4: marked as handled; 5: ignored. • MergeBeginTime - String - Required: No - Creation start time for filtering. • MergeEndTime - String - Required: No - Creation end time for filtering. Example:View

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	This parameter has been deprecated. Example: http://www.ay.com/ay
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameterValue	The parameter value is invalid.

Intrusion Detection - Password Cracking APIs DeleteBruteAttacks

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete brute force attack records.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteBruteAttacks
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	IDs of brute force attack events. You can specify up to 100 IDs in each request. Example: [1,2]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

Error Code	Description
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBanMode

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the blocking mode for brute-force attacks

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBanMode
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
Mode	String	Blocking mode. Valid values: STANDARD_MODE and DEEP_MODE. Example: STANDARD_MODE
StandardModeConfig	StandardModeConfig	Standard blocking configuration. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBanRegions

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying blocked regions

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBanRegions
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Mode	Yes	No	String	Blocking mode. Valid values: STANDARD_MODE and DEEP_MODE. Example: STANDARD_MODE

3. Output Parameters

Parameter name	Type	Description
RegionSet	Array of RegionSet	Region information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBanStatus

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the blocking status

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBanStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
OpenSmartMode	Bool	Whether to enable intelligent over-allowing mode Example: true
ShowTips	Bool	Indicates whether to display a pop-up message. false: does not display a pop-up message. true: displays a pop-up message. Example: false
Status	Uint64	Blocking switch status: 0 - off. 1 - advanced blocking. 2 - basic blocking (only blocklisted IP addresses in the intelligence database will be blocked). Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBanWhiteList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying a blocklist

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBanWhiteList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter condition. • Keywords - String - Required: no - query keywords. Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter	Type	Description

name		
TotalCount	Uint64	Total number of records. Example: 4
WhiteList	Array of BanWhiteListDetail	Allowlist list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBruteAttackList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying password cracking events

Default interface request rate limit: 20 times per second.

Interface update time: 2022-06-06 18:35:50.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBruteAttackList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. CreateTime: first attack time. Example: CreateTime
Filters	No	No	Array of Filter	Filter conditions. • MachineName - String - Required: No - Host alias for filtering. • InstanceID - String - Required: No - Instance ID. • Quuid - String - Required: No - CVM instance UUID. • Status - String - Required: No - Status for filtering. FAILED: failed; SUCCESS: successful. • UserName - String - Required: No - Username for filtering. • SrcIp - String - Required: No - Source IP address for filtering. • CreateBeginTime - String - Required: No - First attack start time for filtering. • CreateEndTime - String - Required: No - First attack end time for filtering. • ModifyBeginTime - String - Required: No - Last attack start time for filtering. • ModifyEndTime - String - Required: No - Last attack end time for filtering. • Banned - String - Required: No - Blocking status for filtering. Separate multiple values by commas (,). 0: not blocked (global ZooKeeper switch off); 82: not blocked (non-Pro Edition); 83: not blocked (allowlisted); 1: blocking successful (completed); 2: not blocked (program error); 3: not blocked (private network attack blocking not supported); 4: not blocked (blocking not supported for Anping); 10: blocking successful (effective). • DataFrom - Int - Hit rule. 0: login rule; 1: intelligence rule. • EventType - String - Required: No - Cracking status for filtering. 200: cracking failed (incorrect password); 300: cracking successful; 400: cracking failed (account does not exist). Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 1
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: asc

3. Output Parameters

Parameter name	Type	Description
BruteAttackList	Array of BruteAttackInfo	Password cracking list API Example:View
TotalCount	Uint64	Total number. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.DateRange	The time range format is incorrect.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeBruteAttackRules

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying anti-brute-force attack rules

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeBruteAttackRules
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
Rules	Array of BruteAttackRuleList	List of rules for determining a block brute force attack. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

ExportBruteAttacks

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export brute force attack records into a CSV file.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportBruteAttacks
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter conditions. • MachineName - String - Required: No - Host alias for filtering. • InstanceID - String - Required: No - Instance ID. • Quuid - String - Required: No - CVM instance UUID. • Status - String - Required: No - Status for filtering. FAILED: failed; SUCCESS: successful. • UserName - String - Required: No - Username for filtering. • SrcIp - String - Required: No - Source IP address for filtering. • CreateBeginTime - String - Required: No - First attack start time for filtering. • CreateEndTime - String - Required: No - First attack end time for filtering. • ModifyBeginTime - String - Required: No - Last attack start time for filtering. • ModifyEndTime - String - Required: No - Last attack end time for filtering. • Banned - String - Required: No - Blocking status for filtering. Separate multiple values by commas (,). 0: not blocked (global ZooKeeper switch off); 82: not blocked (non-Pro Edition); 83: not blocked (allowlisted); 1: blocking successful (completed); 2: not blocked (program error); 3: not blocked (private network attack blocking not supported); 4: not blocked (blocking not supported for Anping); 10: blocking successful (effective). • DataFrom - Int - Hit rule. 0: login rule; 1: intelligence rule. • EventType - String - Required: No - Cracking status for filtering. 200: cracking failed (incorrect password); 300: cracking successful; 400: cracking failed (account does not exist). Example:View

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	This parameter has been deprecated. Example: http://www.ay.com/ay
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
FailedOperation.Export	Failed to export.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ModifyBanMode

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for modifying the brute-force attack blocking mode

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyBanMode
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Mode	Yes	No	String	Blocking mode. Valid values: STANDARD_MODE and DEEP_MODE. Example: STANDARD_MODE
Ttl	No	No	Uint64	Blocking period. This parameter is used for the standard blocking mode. Example: 2

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ModifyBanStatus

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for setting the blocking switch

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyBanStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
OpenSmartMode	No	No	Bool	Whether to enable intelligent over-allowing mode Example: true
Status	Yes	No	Uint64	Blocking switch status: 0 -- off; 1 -- advanced blocking; 2 -- basic blocking (Only blocklisted IPs in the intelligence database will be blocked.) Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.

Error Code	Description
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameterValue	The parameter value is invalid.

ModifyBruteAttackRules

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for modifying rules for determining a brute force attack

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyBruteAttackRules
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Rules	Yes	No	Array of BruteAttackRule	Rules for determining a brute force attack. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

StopNoticeBanTips

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for disabling notifications for brute force attack blocking

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: StopNoticeBanTips
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

Intrusion Detection - Reverse Shell APIs DeleteMemShellRules

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete Java Webshell allowlist rules.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteMemShellRules
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
GroupIDs	Yes	No	Array of String	Batch ID array (maximum 100 entries). Example: ["1","2"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request

Parameter name	Type	Description
		needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DeleteReverseShellEvents

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete reverse shell events based on IDs.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteReverseShellEvents
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	Array of up to 100 IDs. Example: [232196162]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DeleteReverseShellRules

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for deleting anti-reverse shell rules

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteReverseShellRules
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	Array of up to 100 IDs. Example: [1]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter.DateRange	The time range format is incorrect.
InvalidParameter.RegexRuleError	The format of the regular expression parameter is invalid.
InvalidParameter.ReverShellKeyFieldAllEmpty	The process name, target IP address, and target port cannot be left empty at the same time.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DeleteReverseShellRulesAggregation

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete reverse shell rules for the aggregated version.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteReverseShellRulesAggregation
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
GroupIDs	Yes	No	Array of String	Batch ID array (maximum 100 entries). Example: ["85c909fe-c87c-11e9-a100-5cb90191ae78"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMemShellRules

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the Java Webshell allowlist.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMemShellRules
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Sort field, which currently supports CreateTime and ModifyTime. The default value is ModifyTime. Example: ModifyTime
Filters	No	No	Array of Filter	Filter conditions. • Keywords - String - Required: No - Base64-encoded allowlisted content. Example:View
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting method: DESC, ASC. Example: ASC

3. Output Parameters

Parameter name	Type	Description
List	Array of MemShellRule	The entries returned. Example:View
TotalCount	Uint64	Total number. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeReverseShellEvents

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying reverse shell events

Default interface request rate limit: 20 times per second.

Interface update time: 2022-06-06 15:48:41.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeReverseShellEvents
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. CreateTime: occurrence time. Example: CreateTime
Filters	No	No	Array of Filter	Filter conditions. • MachineName - String - Required: No - Host alias. • Ip - String - Required: No - Host IP address. • InstanceID - String - Required: No - Host instance ID. • CreateBeginTime - String - Required: No - Creation start time. • CreateEndTime - String - Required: No - Creation end time. • Status - String - Required: No - Status. 0: to be handled; 2: allowlisted; 3: handled; 4: ignored; 5: deleted. • DetectBy - String - Required: No - Detection method. 0: behavior analysis; 1: command feature detection. • InnerNetAlarmShow - String - Required: No - Whether to display the private network data. 1: yes; 0: no. • ProcName - String - Required: No - Process name. • Uuid - String - Required: No - Host UUID. • Quuid - String - Required: No - Host QUUID. Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10

Parameter name	Required	Allow NULL	Type	Description
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: desc

3. Output Parameters

Parameter name	Type	Description
List	Array of ReverseShell	The entries returned. Example:View
TotalCount	Uint64	Total number. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeReverseShellRules

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying anti-reverse shell rules

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeReverseShellRules
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter condition. • Keywords - String - Required: No - Process name keywords. Example:View
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
List	Array of ReverseShellRule	The entries returned. Example:View
TotalCount	Uint64	Total number. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter.DateRange	The time range format is incorrect.
InvalidParameter.RegexRuleError	The format of the regular expression parameter is invalid.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeReverseShellRulesAggregation

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the list of reverse shell rules for the aggregated version.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeReverseShellRulesAggregation
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Sort field, which currently supports CreateTime and ModifyTime. The default value is ModifyTime. Example: ModifyTime
Filters	No	No	Array of Filter	Filter conditions. • Keywords - String - Required: No - Keyword (process name). • WhiteType - String - Required: No - Rule type. 1: regular expression; 0: ordinary. Example:View
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting method: DESC, ASC. Example: ASC

3. Output Parameters

Parameter name	Type	Description
List	Array of ReverseShellRuleAggregation	The entries returned. Example:View
TotalCount	Uint64	Total number. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeReverseShellSystemPolicyConfig

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Query the configuration of the reverse shell system policy.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeReverseShellSystemPolicyConfig
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
InnerIPShow	Bool	Private IP Display Example: true
InnerNetAlarmShow	Bool	Private Network Alarm Display Example: true

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeShellPolicyList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the list of reverse shell policies.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeShellPolicyList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Sorting column. Valid values: UpdateTime and CreateTime. Example: CreateTime
Filters	No	No	Array of Filters	Filter parameters. Valid values: Id and IdIn. Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Default value: 10. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. ASC: ascending order. DESC: descending order. Example: ASC

3. Output Parameters

Parameter name	Type	Description
List	Array of ShellPolicyList	The custom attributes. Example:View
TotalCount	Uint64	Total number. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ExportReverseShellEvents

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting reverse shell events

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportReverseShellEvents
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter conditions. • MachineName - String - Required: No - Host alias. • Ip - String - Required: No - Host IP address. • InstanceID - String - Required: No - Host instance ID. • CreateBeginTime - String - Required: No - Creation start time. • CreateEndTime - String - Required: No - Creation end time. • Status - String - Required: No - Status. 0: to be handled; 2: allowlisted; 3: handled; 4: ignored; 5: deleted. • DetectBy - String - Required: No - Detection method. 0: behavior analysis; 1: command feature detection. • InnerNetAlarmShow - String - Required: No - Whether to display the private network data. 1: yes; 0: no. • ProcName - String - Required: No - Process name. • Uuid - String - Required: No - Host UUID. • Quuid - String - Required: No - Host QUUID. Example:View

3. Output Parameters

Parameter	Type	Description

name		
DownloadUrl	String	This parameter has been deprecated. Example: http://www.ay.com/ay
TaskId	String	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
FailedOperation.Export	Failed to export.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ModifyReverseShellRulesAggregation

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to edit reverse shell rules for the aggregated version. (It supports multiple server selection and regular expressions.)

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyReverseShellRulesAggregation
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
DestIp	No	No	String	Target IP address. Example: 172.17.0.2
DestPort	No	No	String	Target port. Example: 80
EventId	No	No	Uint64	ID of the event, which must be passed in when you add the event to the allowlist. If you create a rule, leave this parameter empty. Example: 12
GroupID	No	No	String	Batch ID. Example: 85c909fe-c87c-11e9-a100-5cb90191ae78
HandleHistory	No	No	Uint64	Whether to process historical events. 0: no, 1: yes. Example: 1
HostIp	No	No	String	Server IP address. Example: 172.17.0.2
Id	No	No	Uint64	Rule ID. If you want to create a rule, leave this parameter empty. Example: 1
IsGlobal	No	No	Uint64	Specifies whether it is a global rule. It is not a global rule by default. Example: 1
ProcessName	No	No	String	Process name. Example: nginx
RuleRegexp	No	No	String	Base64-encoded rule (regular expression). Example: c2ggcmVkaXMuc2g=
Uuids	No	No	Array of String	Agent IDs. Example: ["a9fe0359-04d9-417f-ab6d-4941891d6c4b"]
WhiteType	No	No	Uint64	Allowlisting method. 0: regular allowlisting, 1: regular expression allowlisting. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

Error Code	Description
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyReverseShellSystemPolicyConfig

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Modify the configuration of the reverse shell system policy.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyReverseShellSystemPolicyConfig
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
InnerIPShow	Yes	No	Bool	Private IP Display Example: true
InnerNetAlarmShow	Yes	No	Bool	Private Network Alarm Display Example: false

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyShellPolicyStatus

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to edit the reverse shell policy switch.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyShellPolicyStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
IsEnabled	No	No	Uint64	0: enabled, 1: disabled. Example: 0
PolicyId	No	No	Uint64	Policy ID. Example: 2001

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

Other APIs
CreateLoginPermissionPush

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to issue a login license.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateLoginPermissionPush
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
InstanceId	No	No	String	Fill in at least one of the host instance ID and UUID. Example: inst-anyinst
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
NonceData	Yes	No	String	Random login code. Example: 8095

Parameter name	Required	Allow NULL	Type	Description
Uuid	No	No	String	Fill in at least one of the host instance ID and UUID. Example: 5a540076-d38a-4078-aa98-qwert371d322

3. Output Parameters

Parameter name	Type	Description
ResultCode	Int64	0: Successful. 1: Failed: No login permissions. 2: Failed: Agent not installed. 3: Failed: Agent offline. 4: Failed: Sending timed out. Please retry. 5: Failed: Unknown error. Example: 0
ResultMessage	String	Reason for an issuance failure. Example: Exception Information
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DeleteLogClsDeliverInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete the CLS log shipping configuration.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteLogClsDeliverInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
SecurityType	Yes	No	Uint64	Security module type. 1: intrusion detection; 2: vulnerability management; 3: baseline management; 4: advanced defense; 5: client security; 6: asset fingerprint; 7: host list; 8: client reporting. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DeleteScanTask

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to stop scan tasks of a specified type.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteScanTask
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ModuleType	Yes	No	String	Module type. Malware: Trojan; Vul: vulnerability. Example: Vul
QuuidList	No	No	Array of String	QUUIDs of servers. This parameter takes effect if the HostType parameter is set to 2 (selected server). Example: ["17d8ad3a-afbb-44a8-8b9e-99a92160f367"]
TaskId	Yes	No	Uint64	Task ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.

Error Code	Description
InvalidParameter.IllegalRequest	Invalid request.
FailedOperation.APIServerFail	Failed to call the API service.
InvalidParameter	Invalid parameter.
AuthFailure	CAM signature or authentication error.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

DescribeAssetEnvList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying environment variables in the asset management module

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-28 15:55:30.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAssetEnvList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid value: FirstTime. Example: FirstTime
Filters	No	No	Array of AssetFilters	Filter conditions. • MachineName - String - Required: No - Host alias for filtering. • IP - String - Required: No - Host IP address for filtering. • InstanceID - String - Required: No - Host instance ID for filtering. • User - String - Required: No - User. • Name - String - Required: No - Environment variable name. • Type - Int - Required: No - Type. 0: user variable; 1: system variable. Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 1
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: desc
Quuid	No	No	String	QUUID of the server. Example: 1c26308c-5493-4eaf-a817-112ec25f499e
Type	No	No	Uint64	Deprecated parameter, which is replaced with Filters . Example: 1
Uuid	No	No	String	Server UUID. Example: 1c26308c-5493-4eaf-a817-112ec25f499e

3. Output Parameters

Parameter name	Type	Description
Envs	Array of AssetEnvBaseInfo	List Example:View
Total	Uint64	Total number. Example: 1021
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeClientException

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Obtain Client Exception Events

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-16 10:43:36.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeClientException
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
EndTime	No	No	String	End time in the format of 2006-01-02 15:04:05 Example: 2006-01-02 15:04:05
ExceptionType	Yes	No	Int64	Client Exception Type 1: Client Offline, 2: Client Uninstallation Example: 1
Limit	Yes	No	Uint64	Limit per Page, not 0, up to 100 Example: 10
Offset	Yes	No	Uint64	Paging Offset Example: 0
StartTime	No	No	String	Start time in the format of 2006-01-02 15:04:05 Example: 2006-01-02 15:04:05

3. Output Parameters

Parameter name	Type	Description
Records	Array of RecordInfo	Event details. Example:View
TotalCount	Uint64	Total Number of Events Example: 944
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

There is no error code related to business logic for this interface, For other error codes, see public ErrorCode.

DescribeClsAccountStatus

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the CLS account status.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeClsAccountStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
AccountStatus	Uint64	0: not enabled, 1: normal, 2: overdue, 3: terminated. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeClsLogsets

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the list of CLS logsets.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeClsLogsets
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter Criteria Example:View
Limit	No	No	Uint64	The maximum value is 100. Example: 10
LogsetRegion	Yes	No	String	Logset region. Example: ap-region1
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
List	Array of ClsLogsetInfo	List Example:View
TotalCount	Uint64	Total number Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeClsTopics

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the list of CLS log topics.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeClsTopics
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Limit	No	No	Uint64	Maximum Example: 10
LogsetId	No	No	String	Logset ID Example: any data
LogsetRegion	Yes	No	String	Logset region. Example: ap-region1
Offset	No	No	Uint64	Offset. Example: 0

3. Output Parameters

Parameter name	Type	Description
List	Array of ClsTopicInfo	List Example:View
TotalCount	Uint64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeCustomerDetail

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Query customer information.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeCustomerDetail
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
IsEnterprise	Bool	Whether it is an enterprise customer. Example: false
Level	String	Level: HEAD. WAIST.

Parameter name	Type	Description
		TAIL. Example: HEAD
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeGeneralStat

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying server-related statistics

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-19 10:10:24.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeGeneralStat
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter parameter CloudFrom. 0: cloud platform; 1: other; 2: Alibaba Cloud; 3: Huawei Cloud; 4: Amazon; 5: Microsoft; 6: Google; 7: Oracle; 8: DigitalOcean; 9: Baidu. Example:View
MachineRegion	No	No	String	Region of a server. Example: ap-region1
MachineType	No	No	String	Cloud host type. • CVM: Cloud Virtual Machine. • BM: Bare Metal Service. • ECM: Edge Computing Machine. • LH: Cloud Platform Lighthouse. • Other: Hybrid cloud machines. Example: CVM

3. Output Parameters

Parameter name	Type	Description
AddedOnTheFifteen	Uint64	Number of servers that were added within the last 15 days. Example: 12
AgentsAll	Uint64	Total number of CWP agents. Example: 2
AgentsBasic	Uint64	Total number of CWP agents of the Basic Edition. Example: 15
AgentsOffline	Uint64	Total number of offline and shutdown CWP agents. Example: 4
AgentsOnline	Uint64	Total number of online CWP agents. Example: 8
AgentsPro	Uint64	Total number of CWP agents of the Professional Edition. Example: 5
AgentsProExpireWithInSevenDays	Uint64	Total number of prepaid CWP Pro agents that will expire in 7 days. Example: 27
FlagshipMachineCnt	Uint64	Total number of servers with CWP Ultimate. Example: 1
MachinesAll	Uint64	Total number of cloud servers. Example: 100
MachinesUninstalled	Uint64	Total number of cloud servers on which no CWP agent is installed. Example: 3
Offline	Uint64	Total number of offline servers. Example: 0
ProtectDays	Uint64	Protection period. Unit: days. Example: 1
RiskMachine	Uint64	Total number of servers at risk. Example: 6
Shutdown	Uint64	Total number of shutdown servers. Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeLogClsDeliverInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to return the CLS shipping configuration.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLogClsDeliverInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
DeliverTypeDetails	Array of DeliverTypeDetails	Details Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeLogStorageConfig

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the log storage configuration.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLogStorageConfig
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
Period	Int64	Log retention time. The value 3640 indicates that the time is unlimited. Example: 3640
PeriodModifyCount	Int64	Number of modifications made to Period this month. Example: 2

Parameter name	Type	Description
Type	Array of String	Storage type: string array Example: ["malware"]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeLogStorageRecord

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the record of stored log size.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLogStorageRecord
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
Records	Array of LogStorageRecord	Storage record. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeLoginPermission

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the login permissions status of a user's host.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLoginPermission
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
InstanceId	No	No	String	Instance ID (fill in at least one of the instance ID and QUuid). Example: inst-anyinst
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
Quuid	No	No	String	Host QUuid list (fill in at least one of the instance ID and QUuid). Example: 5a540076-d38a-4078-aa98-qwert371d322

3. Output Parameters

Parameter name	Type	Description
HasLoginPermission	Bool	Whether a user has login permissions. Example: true

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMachineInfoByHashKey

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the machine information.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMachineInfoByHashKey
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MachineKey	No	No	String	Host hashkey. Example: 539844622

3. Output Parameters

Parameter name	Type	Description
HostIp	String	Private Network IP Address Example: 10.0.0.11

Parameter name	Type	Description
InstanceId	String	Instance ID Example: ins-dsdbhjqf
InstanceName	String	Instance Name Example: redis_node_cvm
Quuid	String	Host QUUID Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Region	String	Availability zone. Example: ap-region1
Uuid	String	Host UUID Example: acdd5474-6360-4fd4-bfc7-843162cb8116
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMachineLoginType

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the host login method.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMachineLoginType
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
InstanceIds	No	No	Array of String	instance_id Example: ["inst-anyinst"]
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
Quuids	No	No	Array of String	Host Quuid List Example: ["5a540076-d38a-4078-aa98-qwert371d322"]

3. Output Parameters

Parameter name	Type	Description
List	Array of MachineLoginType	Login Method Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeMachineLoginTypeStatus

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the status of the host login method.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeMachineLoginTypeStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
InstanceId	No	No	String	Instance ID (fill in at least one of the instance ID and QUuid). Example: inst-anyinst
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
Quuid	No	No	String	Host QUuid list (fill in at least one of the instance ID and QUuid). Example: 5a540076-d38a-4078-aa98-qwert371d322

3. Output Parameters

Parameter name	Type	Description
LoginType	Uint64	Login method. 0: original method, 1: Scan code for password-free login.

Parameter name	Type	Description
		Example: 1
ReturnCode	Uint64	Reason for failing to scan code for login. 0: Successful (you can scan code for login). 1: Agent not installed. 2: Agent offline. 3: Agent version not supported. 4: Unknown error. Example: 0
ReturnMessage	String	Description of the reason for failing to scan code for login. Example: Agent Offline
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeOrderList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the order list.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeOrderList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	When filtering by multiple conditions, take the intersection. • ProductCode: product code, which starts with p_. • SubProductCode: sub-product code, which starts with sp_. • InquireKey: billable item name, which starts with sv_. • Status: resource status. 1: normal, 2: isolated, 3: terminated. • PayMode: payment mode. 0: pay-as-you-go, 1: monthly subscription. • ResourceId: resource ID. • RenewFlag: auto-renewal flag. 0: Disabled by default (auto-renewal available for key accounts). 1: Automatically renew. 2: Manually set to not automatically renew. • DealNames: sub-order number. Example:View
Limit	No	No	Uint64	Limit Entries, 10 by default, up to 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
ResourceIds	No	No	Array of String	Resource ID. Example: ["32454"]

3. Output Parameters

Parameter name	Type	Description
List	Array of OrderList	Order resource object list. Example:View
TotalCount	Uint64	Total number of orders. Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeOverviewStatistics

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to get the overview statistics of CWP under the current account.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeOverviewStatistics
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
BaseLineNum	Uint64	Number of security baselines. Example: 1
BruteAttackSuccessNum	Uint64	Number of successful brute force attacks. Example: 1

Parameter name	Type	Description
MalwareNum	Uint64	Number of trojan files. Example: 1
NonlocalLoginNum	Uint64	Number of logins from unusual locations. Example: 1
OnlineMachineNum	Uint64	Number of online servers. Example: 1
ProVersionMachineNum	Uint64	Number of servers with CWP Pro. Example: 1
VulNum	Uint64	Number of vulnerabilities. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InternalError.MainDBFail	Failed to operate data.

DescribeProVersionInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to get the CWP Pro information.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeProVersionInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
IsAutoOpenProVersion	Bool	Indicates whether CWP Pro is automatically activated for newly added servers. Example: true
PostPayCost	Uint64	Payment details for [Pro Edition - pay-as-you-go] yesterday (the actual bill prevails). Example: 1
ProVersionNum	Uint64	Number of hosts with Pro Edition. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DescribeProVersionStatus

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query whether CWP Pro is activated on a single server or all servers.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeProVersionStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Uuid	Yes	No	String	CWP client UUID. If the value is all, it indicates all hosts. Example: e8f91530-02c7-3e98-d84d-26df60d981ef

3. Output Parameters

Parameter name	Type	Description
Status	String	Activation status. • UNOPENED: CWP Pro is not activated. • OPENED: CWP Pro is activated.

Parameter name	Type	Description
		Example: OPENED
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeRecommendedProtectCpu

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the recommended number of protection cores for purchase.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeRecommendedProtectCpu
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
Number	Int64	Recommended purchase quantity. Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeScanState

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the status of a scan task that is running in the corresponding module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-12-29 09:49:27.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeScanState
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter parameters; • StrategyId - Baseline strategy ID, required only when ModuleType is Baseline. Example:View
ModuleType	Yes	No	String	Module type. Valid values: Malware (trojan), Vul (vulnerability), and Baseline. Example: Vul

3. Output Parameters

Parameter name	Type	Description
RiskEventCount	Uint64	Number of scanned vulnerabilities. Example: 1
ScanBeginTime	String	Time when the scan starts. Example: 2021-07-09 15:04:01
ScanEndTime	String	Time when the scan ends. Example: 2021-07-09 15:04:01

Parameter name	Type	Description
ScanState	Uint64	0: never scanned. 1: scanning. 2: scan completed. 3: stopping. 4: stopped. Example: 2
Schedule	Uint64	Scan progress. Example: 10
TaskId	Uint64	Task ID. Example: 1
Type	Uint64	0: quick scan .1: scheduled scan. Example: 1
VulId	Array of Uint64	Vulnerability ID in the scan task. Example: [1,2,4]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
AuthFailure	CAM signature or authentication error.
InvalidParameterValue	The parameter value is invalid.

DescribeScanTaskDetails

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the details of a scan task or query the progress of the scan task or whether the scan task is running normally.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-06-14 17:12:25.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeScanTaskDetails
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter conditions. • MachineName - String - Required: No - Host alias. • Ip - String - Required: No - Host IP address. • InstanceID - String - Required: No - Host instance ID. Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10
ModuleType	Yes	No	String	Module type. Valid values: Malware (trojan), Vul (vulnerability), and Baseline. Example: Vul
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
TaskId	Yes	No	Uint64	The task ID. Example: 1

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RiskEventCount	Uint64	Number of risky events. Example: 1
RiskMachineCount	Uint64	Number of servers at risk. Example: 1
ScanBeginTime	String	Start time of the scan. Example: 2024-10-30 10:13:53
ScanContent	Array of String	Scan content. Example: ["0", "1", "2", "4", "5"]
ScanEndTime	String	Time when the scan ends. Example: 2021-02-01 12:00:00
ScanLeftTime	Uint64	Remaining scanning time. Example: 12
ScanMachineCount	Uint64	Total number of scanned servers. Example: 1
ScanProgress	Uint64	Scan progress. Example: 10
ScanTaskDetailList	Array of ScanTaskDetails	Scan task information. Example:View
ScanTime	Uint64	Scan time. Example: 19
StoppingAll	Bool	Indicates whether the task is being stopped. true: yes. Example: true
TotalCount	Uint64	Total number. Example: 1
Type	Uint64	0: quick scan .1: scheduled scan. Example: 1
VulCount	Uint64	Number of vulnerabilities detected in the scan. Example: 0
VulInfo	Array of VulDetailInfo	Vulnerability information. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

Error Code	Description
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
AuthFailure	CAM signature or authentication error.
InvalidParameterValue	The parameter value is invalid.

DescribeSecurityDynamics

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to get the security event message data.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSecurityDynamics
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
SecurityDynamics	Array of SecurityDynamic	Security event messages. Example:View

Parameter name	Type	Description
TotalCount	Uint64	The number of entries returned. Example: 100
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
InvalidParameter.IllegalRequest	Invalid request.

DescribeSecurityEventStat

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying security event statistics

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-08 16:30:42.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSecurityEventStat
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	This API does not support filter conditions. Example:View

3. Output Parameters

Parameter name	Type	Description
AttackLogsStat	EventStat	Statistics about cyberattack events. Example:View
BaseLineTotalAffectNum	Uint64	Total number of servers on which pending baseline security events exist. Example: 1
BaselineHighStat	EventStat	Statistics about high-risk baseline vulnerability events. Example:View
BaselineLowStat	EventStat	Statistics about low-risk baseline vulnerability events. Example:View

Parameter name	Type	Description
BaselineNormalStat	EventStat	Statistics about medium-risk baseline vulnerability events. Example:View
BaselineRiskStat	EventStat	Statistics about critical baseline vulnerability events. Example:View
BruteAttackStat	EventStat	Statistics about brute force attacks. Example:View
CyberAttackTotalAffectNum	Uint64	Total number of servers on which pending cyberattack events exist. Example: 1
HighRiskBashStat	EventStat	Statistics about high-risk command events. Example:View
HostLoginStat	EventStat	Statistics about logins from unusual locations. Example:View
InvasionTotalAffectNum	Uint64	Total number of servers on which pending intrusion events exist. Example: 1
MachineTotalAffectNum	Uint64	Total number of servers on which pending security events exist. Example: 1
MaliciousRequestStat	EventStat	Statistics about malicious request events. Example:View
MalwareStat	EventStat	Statistics about trojan events. Example:View
PrivilegeStat	EventStat	Statistics about local privilege escalation events. Example:View
ReverseShellStat	EventStat	Statistics about reverse shell events. Example:View
Score	Uint64	Security score. Example: 20
VulHighStat	EventStat	Statistics about high-risk vulnerability events. Example:View
VulLowStat	EventStat	Statistics about low-risk vulnerability events. Example:View
VulNormalStat	EventStat	Statistics about medium-risk vulnerability events. Example:View
VulRiskStat	EventStat	Statistics about critical vulnerability events. Example:View
VulStat	EventStat	Vulnerability count statistics. Example:View

Parameter name	Type	Description
VulTotalAffectNum	Uint64	Total number of servers on which pending vulnerability events exist. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
ResourceNotFound	The resource does not exist.

DescribeSecurityEventsCnt

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the event statistics related to security overview.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-11-08 16:30:42.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSecurityEventsCnt
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
AttackLogs	SecurityEventInfo	Risk events related to attack detection. Example:View
BaseLine	SecurityEventInfo	Risk events related to security baselines. Example:View

Parameter name	Type	Description
Bash	SecurityEventInfo	Risk events related to high-risk commands. Example:View
BruteAttack	SecurityEventInfo	Risk events related to password cracking. Example:View
EffectMachineCount	Uint64	Number of affected servers. Example: 1
EmergencyVul	SecurityEventInfo	Risk events related to emergency vulnerabilities. Example:View
EventsCount	Uint64	Total number of all events. Example: 1
HostLogin	SecurityEventInfo	Risk events related to login audits. Example:View
LinuxVul	SecurityEventInfo	Total number of Linux system vulnerability events. Example:View
Malware	SecurityEventInfo	Risk events related to trojan files. Example:View
PrivilegeRules	SecurityEventInfo	Risk events related to local privilege escalation. Example:View
ReverseShell	SecurityEventInfo	Risk events related to reverse shells. Example:View
RiskDns	SecurityEventInfo	Risk events related to malicious requests. Example:View
SysVul	SecurityEventInfo	Risk events related to application vulnerabilities. Example:View
WebVul	SecurityEventInfo	Risk events related to web application vulnerabilities. Example:View
WindowVul	SecurityEventInfo	Total number of Windows system vulnerability events. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
ResourceNotFound	The resource does not exist.
InternalError.MainDBFail	Failed to operate data.
InvalidParameter	Invalid parameter.

DescribeSecurityTrends

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to get the security event statistics.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSecurityTrends
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
BeginDate	Yes	No	Date	Start time, such as 2021-07-10. Example: 2021-07-10
EndDate	Yes	No	Date	End time, such as 2021-07-10. Example: 2021-09-10

3. Output Parameters

Parameter name	Type	Description
BaseLines	Array of	Statistics about baseline vulnerabilities.

Parameter name	Type	Description
	SecurityTrend	Example:View
BruteAttacks	Array of SecurityTrend	Statistics about password cracking events. Example:View
CyberAttacks	Array of SecurityTrend	Statistics about cyberattacks. Example:View
HighRiskBashs	Array of SecurityTrend	Statistics about high-risk commands. Example:View
MaliciousRequests	Array of SecurityTrend	Statistics about malicious requests. Example:View
Malwares	Array of SecurityTrend	Statistics about trojan events. Example:View
NonLocalLoginPlaces	Array of SecurityTrend	Statistics about logins from unusual locations. Example:View
PrivilegeEscalations	Array of SecurityTrend	Statistics about local privilege escalation. Example:View
ReverseShells	Array of SecurityTrend	Statistics about reverse shells. Example:View
Vuls	Array of SecurityTrend	Statistics about vulnerabilities. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.

Error Code	Description
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter.DateRange	The time range format is incorrect.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeTaskDuration

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Obtain Task Distribution Duration

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeTaskDuration
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
TimingScan	No	No	Bool	Whether to perform a scheduled scan Example: true
UuidCnt	Yes	No	Uint64	Number of Hosts that Require Performing Tasks Example: 100

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
Duration	Uint64	Time Required for Task Deployment, in Minutes Example: 5
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeTrialReport

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the trial report.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeTrialReport
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
AddMachineCnt	Int64	Number of new machines. Example: 0
AutoBlockBruteCnt	Int64	Number of automatic blocks (successful). Example: 0

Parameter name	Type	Description
AutoDefenceCnt	Int64	Number of automatic defense vulnerabilities (successful). Example: 0
AutoIsolateMalwareCnt	Int64	Number of automatically isolated Trojans (successful). Example: 0
BaselineRiskCnt	Int64	Number of baseline risks (detection items). Example: 0
BruteAlarmCnt	Int64	Number of successful brute force cracking alarms. Example: 0
IsShow	Bool	Indicates whether to display Example: true
MalwareAlarmCnt	Int64	Number of successful Trojan alarms. Example: 0
VulCnt	Int64	Number of Vulnerabilities Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeUsersConfig

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the user's configuration.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeUsersConfig
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ConfigName	Yes	No	String	Configuration name. • license_monitor: license monitoring configuration. 0: disabled, 1: enabled. Example: license_mon

3. Output Parameters

Parameter name	Type	Description
Value	String	Configuration value Example: 35768
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeVersionStatistics

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the numbers of servers with CWP Basic, servers with CWP Pro, and servers with CWP Ultimate.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-01-09 11:35:47.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVersionStatistics
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
BasicVersionNum	Uint64	Number of basic versions. Example: 1
GeneralVersionNum	Uint64	Number of General Discount Editions Example: 1

Parameter name	Type	Description
ProVersionNum	Uint64	Number of professional versions. Example: 1
UltimateVersionNum	Uint64	Number of servers with CWP Ultimate. Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InternalError.MainDBFail	Failed to operate data.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeVulTrend

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain information of the vulnerability situation.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVulTrend
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
HotVulCount	Uint64	Notable vulnerabilities attacked in the past six months Example: 134
IncreaseHotVulCount	Uint64	New notable vulnerabilities attacked in the past six months Example: 13
IncreaseVulEventCount	Uint64	Number of new vulnerability exploitation attacks in the past six months Example: 0
VulEventCount	Uint64	Number of vulnerability exploitation attacks in the past six months Example: 0

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ExportScanTaskDetails

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export the details of a specified scan task based on a task ID.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportScanTaskDetails
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter conditions. • MachineName - String - Required: No - Host alias. • Ip - String - Required: No - Host IP address. • InstanceID - String - Required: No - Host instance ID. Example:View
ModuleType	Yes	No	String	Model type. Valid values: Malware (trojan), Vul (vulnerability), and Baseline. Example: Malware
TaskId	Yes	No	Uint64	ID of the current check task, which is different from the ID of the task that exports the Excel file of the current check in the output parameters. Example: 1596595610

3. Output Parameters

Parameter name	Type	Description
TaskId	String	Task ID, which can be used to obtain the download URL (DownloadUrl) by calling the ExportTasks API. (This ID differs from the detection task ID in the input parameters.) Example: 1615549629
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ExportSecurityTrends

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting the risk trend

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportSecurityTrends
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
BeginDate	Yes	No	Date	The start time. Example: 2020-06-01
EndDate	Yes	No	Date	The end time. Example: 2020-06-02

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
DownloadUrl	String	Download URL of the exported file. Example: http://www.ay.com/ay
TaskId	String	Task ID. Example: 56
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

ExportTasks

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

It is used to asynchronously export log files with a large amount of data.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportTasks
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
TaskId	Yes	No	String	The task ID. Example: 24563

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	The download URL. Example: http://domain.com/anypath/x
FileName	String	Saved filename. Example: login-6450ca41-35da-4bee-ade8-c842781ea6dd.csv
Status	String	PENDING: the download link is being generated. FINISHED: the download link has been generated. ERROR: abnormal conditions such as network exceptions. Example: FINISHED
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
ResourceNotFound	The resource does not exist.

ModifyEventAttackStatus

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Yunapi Response

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyEventAttackStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
All	No	No	Bool	Whether to update all, that is, whether to operate on all events. When ids is not empty, this parameter is invalid. Example: false
ExcludeId	No	No	Array of Uint64	Excluded IDs Example: [1,2]
Filters	No	No	Array of Filters	Filter criteria. • Type - String Attack Status 0: Attack Attempt 1: Successful Attack - Required or Not: No • Status - String Event Handling Status 0: Pending 1: Handled 2: Allowlisted 3: Ignored 4: Deleted - Required or Not: No • SrcIP - String Source IP - Required or Not: No • DstPort - String Target Attack Port - Required or Not: No • MachineName - String Host Name - Required or Not: No • InstanceID - String Host Instance ID - Required or Not: No • Quuids - String Host CVM UUID - Required or Not: No . Example:View
Ids	No	No	Array of Uint64	Array of event IDs that need to be modified. Batch operation is supported. Example: [1,2]
Status	No	No	Uint64	0: pending processing; 1: processed; 3: ignored; 4: deleted. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyLogClsDeliverInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the CLS log shipping configuration.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyLogClsDeliverInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
LogType	Yes	No	Array of Uint64	Type of logs of the security module Example: [1]
LogsetId	No	No	String	Logset ID Example: 234235
LogsetName	No	No	String	Logset Topic Example: redis_node_log
LogsetRegion	Yes	No	String	Region. Example: ap-region1
SecurityType	Yes	No	Uint64	Log type. 1: intrusion detection; 2: vulnerability management; 3: baseline management; 4: advanced defense; 5: client-related; 6: asset fingerprint; 7: host list; 8: client log. Example: 1
TopicId	No	No	String	Topic ID Example: topic_redis_node_log
TopicName	No	No	String	Topic Name Example: topic_redis_node_log

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.

Error Code	Description
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyLogClsDeliverSwitch

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the CLS shipping switch.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyLogClsDeliverSwitch
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
SecurityType	Yes	No	Uint64	Security module type. 1: intrusion detection; 2: vulnerability management; 3: baseline management; 4: advanced defense; 5: client security; 6: asset fingerprint; 7: host list; 8: client reporting. Example: 1
Switch	Yes	No	Uint64	Log shipping status. 0: disabled. 1: enabled. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyLogStorageConfig

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the log storage configuration.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyLogStorageConfig
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
IsModifyPeriod	Yes	No	Bool	Whether to modify the validity period (deprecated). Example: true
Period	Yes	No	Int64	Log retention time. The value 3640 indicates that the time is unlimited. Example: 3640
Type	No	No	Array of String	Storage type: string array Example: ["malware","risk_process"]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyMachineLoginType

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the host login method.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyMachineLoginType
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
InstanceId	No	No	String	Instance ID (fill in at least one of the instance ID and QUuid). Example: inst-anyinst
LoginType	Yes	No	Uint64	Login method. 0: original method, 1: Scan code for password-free login. Example: 1
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
Quuid	No	No	String	Host QUuid list (fill in at least one of the instance ID and QUuid). Example: 5a540076-d38a-4078-aa98-qwert371d322

3. Output Parameters

Parameter name	Type	Description
ResultCode	Uint64	Modification result. 0: Successful. 1: Agent not installed. 2: Agent offline. 3: Agent version not supported. 4: Unknown error. Example: 0
ResultMessage	String	Modified result description Example: Agent Offline
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyOrder

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Edit Order

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyOrder
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Data	No	No	Array of OrderData	Order configuration array, with a maximum length of 10. New purchase and configuration adjustment are not allowed to occur at the same time. Example:View

3. Output Parameters

Parameter name	Type	Description
BigDealId	String	Main order number, which is not returned for pay-as-you-go orders. Example: any data
DealNames	Array of String	Sub-order number Example: ["32454"]
ResourceIds	Array of String	Resource ID. For postpaid orders, it will be returned. For prepaid (monthly subscription) orders, payment needs to be made first by calling the fee payment API via the large order number or sub-order number. Example: ["32454"]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyUsersConfig

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Modify user configuration

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyUsersConfig
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ConfigName	Yes	No	String	Configuration name. • license_monitor: new license monitoring configuration. 0: disabled, 1: enabled. Example: license_monitor_100
ConfigValue	Yes	No	String	Configuration value Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyVulDefenceSwitch

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the Security Center vulnerability defense and network attack switches.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyVulDefenceSwitch
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
DefenceType	Yes	No	Uint64	Settings type. 0: vulnerability defense. 1: network attack. Example: 1
Enable	Yes	No	Uint64	Whether the switch is on. 1: on, 0: off. Example: 1
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

Security Operations APIs CreateSearchLog

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for creating a historical search record

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateSearchLog
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
SearchContent	Yes	No	String	Content search. Example: success

3. Output Parameters

Parameter name	Type	Description
Status	Uint64	A value of 0 indicates that the request is successful. A non-

Parameter name	Type	Description
		zero value indicates that the request has failed. Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

CreateSearchTemplate

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for creating a search template

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-09 16:57:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateSearchTemplate
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
SearchTemplate	Yes	No	SearchTemplate	Search template. Example:View

3. Output Parameters

Parameter name	Type	Description
Message	String	Failure reason Example: A record with the same name already exists

Parameter name	Type	Description
Status	Uint64	A value of 0 indicates that the request is successful. A non-zero value indicates that the request has failed. Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
InvalidParameter.NameHasRepetition	The name already exists.

DeleteSearchTemplate

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for deleting a search template

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-09 16:57:46.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteSearchTemplate
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Id	Yes	No	Uint64	Template ID Example: 1

3. Output Parameters

Parameter name	Type	Description
Status	Uint64	A value of 0 indicates that the request is successful. A non-zero value indicates that the request has failed. Example: 0

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeESAggregations

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the aggregation result of ES fields

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeESAggregations
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Query	Yes	No	String	ES aggregate condition in the JSON format. Example: {"cwp":"dev"}

3. Output Parameters

Parameter name	Type	Description
Data	String	ES aggregation result in the JSON format. Example: {"took":12,"total":3,"aggs":{"dst_port":{},"src_port":{}},"code":0,"message":"success"}

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
FailedOperation.APIServerFail	Failed to call the API service.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeHistoryService

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying log search service information

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-09 16:53:15.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeHistoryService
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
BuyStatus	Uint64	1: purchase is allowed. 2: only configuration upgrade and downgrade is supported. 3: only redirection to the renewal management page is allowed. Example: 1
EndTime	String	The point in time when it expires. Example: 2020-10-29 00:00:00
InquireNum	Uint64	Purchased capacity. Unit: GB. Example: 1
IsAutoOpenRenew	Uint64	Indicates whether auto-renewal is enabled. 0: initial value. 1: enabled. 2: not enabled. Example: 1
ResourceId	String	Resource ID. Example: 1
StartTime	String	Start time. Example: 2020-09-29 00:00:00
Status	Uint64	0: not enabled. 1: normal. 2: isolated. 3: terminated. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DescribeIndexList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the index list.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeIndexList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
Data	String	ES index information. Example: {"indexSort":{"i1":["userlog-asset_component"]}
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
FailedOperation.APIServerFail	Failed to call the API service.

DescribeLogStorageStatistic

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the usage statistics of the log search capacity

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-09 16:52:41.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLogStorageStatistic
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
TotalSize	Uint64	Total capacity. Unit: GB. Example: 1
UsedSize	Uint64	Used capacity. Unit: GB. Example: 1

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DescribeSearchExportList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting ES query documents

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSearchExportList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Query	Yes	No	String	ES query condition in the JSON format. Example: {"event_type":"vul"}

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	This parameter has been deprecated. Example: http://domain.com/anypath/x
TaskId	Uint64	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeSearchLogs

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying historical search records

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-09 16:57:07.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSearchLogs
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
Data	Array of String	Search records. Only the most recent 10 records are retained. Example: ["yunjing","106.55.40.250","106.55.35.160"]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DescribeSearchTemplates

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying a list of quick searches

Default interface request rate limit: 20 times per second.

Interface update time: 2023-02-09 16:57:20.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSearchTemplates
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Limit	No	No	Uint64	Number of items returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0

3. Output Parameters

Parameter name	Type	Description
List	Array of SearchTemplate	Template list Example:View
TotalCount	Uint64	Total number. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

Settings Center APIs
CreateAgentInstallTask

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to create a CWPP agent installation task.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateAgentInstallTask
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
AssetInfos	No	No	Array of AssetInfo	Host list, which is not required when all are installed. Example:View
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
OpenAll	Yes	No	Bool	Whether to install all agents. Example: true
OpenProtection	Yes	No	Bool	Whether to enable protection after the installation is complete. Example: true

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

CreateLicenseOrder

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

The CreateLicenseOrder API can create Professional/Premium Edition orders.
Supports prepaid and postpaid creation.
Postpaid orders are created directly.
Prepaid orders are placed without payment, requiring calling the billing payment API to pay.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-12-12 15:20:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateLicenseOrder
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
AutoProtectOpenConfig	No	No	String	This field is deprecated. Example: "no config"
AutoRenewFlag	No	No	Bool	Specifies whether to enable auto-renewal. By default, auto-renewal is not enabled. This parameter takes effect only when the billing method is monthly subscription. Example: false
BillingDefineParams	No	No	BillingDefineParams	Business Custom Parameters Example:View
LicenseNum	No	No	Uint64	Number of licenses that you want to purchase. Default value: 1. Example: 1
LicenseType	No	No	Uint64	License type. 0: Pro Edition license; 5: Ultimate Edition license. Example: 0
ModifyConfig	No	No	OrderModifyObject	Configuration Parameters Example:View
ProjectId	No	No	Uint64	Project ID. Default value: 0. Example: 0
RegionId	No	No	Uint64	Code of the region that applies the billing price. Example: 1
Tags	No	No	Array of Tags	Tags. If this parameter is left empty, no tags need to be attached. Example:View
TimeSpan	No	No	Uint64	Unused field. Example: 1

3. Output Parameters

Parameter name	Type	Description
BigDealId	String	Parent order ID. The value of this parameter is an empty string for postpaid orders. Example: order-vmqkfmayay
DealNames	Array of String	Order list. Example: ["cwp-313dfay*", "cwp-vi4d8ay*"]
ResourceIds	Array of String	Resource IDs. The value of this parameter is an empty string for prepaid orders. Example: ["cwp-313dfay*", "cwp-vi4d8ay*"]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

DeleteLicenseRecord

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to delete expired orders in the license management module. Deleted orders will be no longer counted.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-06-09 10:49:46.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DeleteLicenseRecord
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
LicenseId	Yes	No	Uint64	License ID, which can be obtained by querying the license order list. Example: 1
LicenseType	Yes	No	Uint64	License type. 0: Pro Edition license; 5: Ultimate Edition license. Example: 0
ResourceId	Yes	No	String	Resource ID. Example: cwplic-9090ayay

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeAgentInstallResult

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the installation results of a machine.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAgentInstallResult
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
AssetInfos	No	No	Array of AssetInfo	Host list Example:View
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
AgentInstallResults	Array of AgentInstallResult	Installation result list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeAgentInstallTaskResult

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the completion status of an agent installation task.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeAgentInstallTaskResult
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
TaskIds	Yes	No	Array of Uint64	Agent installation task ID. Example: [1]

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
Assets	Array of AgentInstallTaskResult	Agent installation task details. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeChangingAssetInfo

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the list of hosts being modified.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeChangingAssetInfo
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]

3. Output Parameters

Parameter name	Type	Description
AssetInfos	Array of AssetChangeInfo	Asset list Example:View

Parameter name	Type	Description
TaskIds	Array of Uint64	List of agent installation task IDs. Example: [1]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeLicenseBindList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the servers that are bound to a license in the Settings Center > License Management module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-06-09 10:50:08.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLicenseBindList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter conditions. Valid values: • InstanceID, IP, MachineName (fuzzy match), • Keywords (host name or IP address for fuzzy match • AgentStatus: ONLINE: online; OFFLINE: offline; UNINSTALLED: not protected; SHUTDOWN: shut down; TERMINATED_PRO_VERSION: Pro Edition activated and server terminated. Example:View
LicenseId	Yes	No	Uint64	License ID. Example: 1
LicenseType	Yes	No	Uint64	License type. 0: Pro Edition license; 5: Ultimate Edition license. Example: 0
Limit	No	No	Uint64	Maximum number of entries to return. Default value: 10. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
ResourceId	Yes	No	String	Resource ID. Example: any data

3. Output Parameters

Parameter name	Type	Description
List	Array of LicenseBindDetail	Information about bound servers. Example:View
TotalCount	Uint64	Total number. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameterValue	The parameter value is invalid.

DescribeLicenseBindSchedule

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the progress of a license binding task.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:09:36.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLicenseBindSchedule
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Parameter for filtering. Status: binding progress. 0: in progress. 1: completed. 2: failed. Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Default value: 10. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
TaskId	Yes	No	Uint64	The task ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
List	Array of LicenseBindTaskDetail	Details of a binding task. Example:View
Schedule	Uint64	Progress. Example: 20
TotalCount	Uint64	Total number. Example: 12
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.

DescribeLicenseGeneral

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the license overview information in the license management module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-12-12 15:17:14.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLicenseGeneral
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
AutoOpenStatus	Bool	Indicates whether automatic upgrade is enabled. true: enabled. false: disabled. Default value: false. Example: false
AutoRepurchaseRenewSwitch	Bool	Is auto-renewal required for auto-purchase orders, true for ON, false for OFF Example: false
AutoRepurchaseSwitch	Bool	Auto-purchase switch, true for ON, false for OFF Example: false
AvailableFlagshipVersionLicenseCnt	Uint64	Number of available CWP Ultimate licenses. Example: 1
AvailableLHLicenseCnt	Uint64	Number available CWP General licenses. Example: 0
AvailableLicenseCnt	Uint64	Number of available licenses. Example: 3
AvailableProVersionLicenseCnt	Uint64	Number of available CWP Pro licenses, including those billed based on a pay-as-you-go basis. Example: 2
CwpVersionLicenseCnt	Uint64	Total number of CWP General licenses purchased through valid orders. Example: 0
DestroyOrderNum	Uint64	Number of terminated orders Example: 0
ExpireLicenseCnt	Uint64	Number of expired licenses, excluding deleted licenses. Example: 0
FlagshipVersionLicenseCnt	Uint64	Total number of CWP Ultimate licenses purchased through valid orders. Example: 1
IsOpenStatusHistory	Bool	Indicates whether automatic upgrade has been enabled. Example: false
LicenseCnt	Uint64	Total number of licenses, including isolated licenses, expired licenses, and licenses in other unavailable states. Example: 3
NearExpiryLicenseCnt	Uint64	Number of licenses that will expire within 15 days. Example: 0

Parameter name	Type	Description
NotExpiredLicenseCnt	Uint64	Number of licenses that have not expired. Example: 3
ProVersionLicenseCnt	Uint64	Total number of CWP Pro licenses purchased through valid orders. Example: 2
ProtectType	String	PROVERSION_POSTPAY: CWP Pro (pay-as-you-go). PROVERSION_PREPAY: CWP Pro (monthly subscription). FLAGSHIP_PREPAY: CWP Ultimate (monthly subscription). Example: PROVERSION_POSTPAY
RepurchaseRenewSwitch	Bool	Whether automatic renewal is enabled for additional purchase. true: enabled; false: disabled. Example: false
UsedLicenseCnt	Uint64	Number of used licenses. Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DescribeLicenseList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the information about all license orders.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-12-12 15:20:20.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeLicenseList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter conditions. • LicenseStatus: License status. 0: unused; 1: partially used; 2: used up; 3: unavailable; 4: available. • BuyTime: Purchase time. • LicenseType: License type. 0: Pro Edition license; 5: Ultimate Edition license. • DeadlineStatus: Expiration status. NotExpired: not expired; Expire: expired (including terminated); NearExpiry: about to expire. • ResourceId: Resource ID. • Keywords: IP address for filtering. • PayMode: Payment mode. 0: pay-as-you-go; 1: monthly subscription. • OrderStatus: Order status. 1: normal; 2: isolated; 3: terminated. • DealNames: Sub-order numbers. The maximum number of sub-order numbers cannot exceed 10. Otherwise, a failure will occur. Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Default value: 10. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
ResourceIds	No	No	Array of String	Resource IDs, which are used as a filter condition. The ResourceIds parameter and the Filters.ResourceId parameter cannot be specified together. If you specify them together, the ResourceIds parameter takes precedence. Example: ["cwp-1sd324s"]
Tags	No	No	Array of Tags	Tags, which are used as a filter condition. A tag is a key-value pair. Example:View

3. Output Parameters

Parameter name	Type	Description
List	Array of LicenseDetail	Information about license quantities. Example:View
TotalCount	Uint64	Total number. Example: 12
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeSaveOrUpdateWarnings

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to save or update custom alarm settings. This API has been deprecated. You can call the ModifyWarningSetting API to modify the alarm settings.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeSaveOrUpdateWarnings
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
WarningObjects	No	No	Array of WarningObject	Updated alarm settings. Example:View

3. Output Parameters

Parameter name	Type	Description

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

DescribeWarningList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the alarms for the current user

Default interface request rate limit: 20 times per second.

Interface update time: 2022-12-23 11:47:34.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeWarningList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
WarningInfoList	Array of WarningInfoObj	List of alarms. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DescribeWarningServiceIPList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain the IP address list of the alarm service.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeWarningServiceIPList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
List	Array of String	List Example: ["192.168.0.204"]
UpdateTime	String	Latest Update Time Example: 2024-08-01

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DestroyOrder

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to terminate resources.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-27 11:44:19.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DestroyOrder
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
LicenseType	Yes	No	Uint64	License type. 0: Pro Edition license; 5: Ultimate Edition license. Example: 0
ResourceId	Yes	No	String	Resource ID. Example: resource_id

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameterValue	The parameter value is invalid.
InternalError	Internal error.
ResourceNotFound	The resource does not exist.
OperationDenied	Operation denied.

ExportLicenseDetail

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export the license binding information.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-06-01 11:06:27.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportLicenseDetail
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
ExportMonth	No	No	String	Month of data to export. This parameter is available only when the IsHistory parameter is set to False. Example: 2022-03
Filters	No	No	Array of Filters	Conditions. • LicenseType: license type. 0: Pro Edition; 5: Ultimate Edition. • ResourceId: resource ID. Example:View
IsHistory	No	No	Bool	Specifies whether to export the details of all licenses. Example: false
Tags	No	No	Array of Tags	Tags, which are used as a filter condition. A tag is a key-value pair. Example:View

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	Download URL. This parameter has been deprecated. Example: url
TaskId	Uint64	Task ID, required for obtaining the DownloadURL at API Asynchronous Export Task ExportTasks Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
ResourceNotFound	The resource does not exist.

ModifyAssetsProtectionStatus

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the host protection status.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyAssetsProtectionStatus
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
AssetInfos	No	No	Array of AssetInfo	Host list, which is not required when OpenAll is set to True. Example:View
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
OpenAll	Yes	No	Bool	Whether to enable protection for all hosts. Example: true
Status	Yes	No	Uint64	Status. 0: disabled, 1: enabled. Example: 1

3. Output Parameters

Parameter	Type	Description

name		
Assets	Array of AgentInstallResult	Operation result list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyAutoOpenProVersionConfig

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to set whether to automatically activate CWP Pro for newly added servers.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-12-12 15:15:05.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyAutoOpenProVersionConfig
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
AutoRepurchaseRenewSwitch	No	No	Uint64	Auto-renewal or not for auto-purchased orders, 0 by default, 0 for OFF, 1 for ON Example: 1
AutoRepurchaseSwitch	No	No	Uint64	Automatic purchase/ expansion authorization switch, 1 by default, 0 for OFF, 1 for ON. Example: 1
ProtectType	No	No	String	Enhanced protection mode. PROVERSION_POSTPAY: Pro Edition (pay-as-you-go) PROVERSION_PREPAY: Pro Edition (monthly subscription) FLAGSHIP_PREPAY: Ultimate Edition (monthly subscription) Example: PROVERSION_POSTPAY
RepurchaseRenewSwitch	No	No	Uint64	Whether the manually purchased order is automatically renewed (defaults to 0): 0 - off; 1 - on Example: 0
Status	Yes	No	String	Status of the automatic activation feature. • CLOSE: public network-based access to ES is disabled. • OPEN: enabled Example: OPEN

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ModifyLicenseBinds

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to bind a license to one or more servers in the Settings Center > License Management module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-27 11:43:44.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyLicenseBinds
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
IsAll	No	No	Bool	Specifies whether to specify all servers. If the total number of servers exceeds the number of licenses available for the current order, the excess servers will be skipped. Example: true
LicenseType	Yes	No	Uint64	License type. 0: Pro Edition license; 5: Ultimate Edition license. Example: 0
QuuidList	No	No	Array of String	QUUIDs of the servers to which you want to bind licenses. This parameter is required when the IsAll parameter is set to false. If the IsAll parameter is not set to false, ignore this parameter. The maximum length of this parameter is 2,000 bytes. Example: ["4c4c4544-004c-5410-805a-cac04f46ayay"]
ResourceId	Yes	No	String	Resource ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
TaskId	Uint64	The task ID. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyLicenseOrder

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to edit authorization orders.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyLicenseOrder
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Alias	No	No	String	Resource alias. Fill in the original value for no change. Example: use_for_redis
InquireNum	No	No	Uint64	Expected value. If the current value is 10, fill in a larger value for scale-out, a smaller value for scale- down (the expected value must be no less than the usage value during scale-down), or the same value for no change. Example: 1
ProjectId	No	No	Uint64	Project ID. Fill in the original value for no change. Example: 1
ResourceId	Yes	No	String	Resource ID. Example: cwplic-dwsds

3. Output Parameters

Parameter name	Type	Description
DealNames	Array of String	Order number Example: ["6723561253"]

Parameter name	Type	Description
ResourceIds	Array of String	Resource ID. Example: ["cwplic-dwsds"]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ModifyLicenseUnBinds

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to unbind a license from one or more servers in the Settings Center > License Management module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-27 11:43:31.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyLicenseUnBinds
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
IsAll	No	No	Bool	Specifies whether to specify all servers. If the total number of servers exceeds the number of licenses available for the current order, the excess servers will be skipped. Example: true
IsShrink	No	No	Bool	Specifies whether to enable automatic scale-in. If the remaining number of licenses is 1, this API terminates the order. Example: false
LicenseType	Yes	No	Uint64	License type. 0: Pro Edition license; 5: Ultimate Edition license. Example: 0
QuuidList	No	No	Array of String	QUUIDs of the servers to which you want to unbind licenses. This parameter is required when the IsAll parameter is set to false. If the IsAll parameter is not set to false, ignore this parameter. The maximum length of this parameter is 100 bytes. Example: ["4c4c4544-0053-4d10-8052-c4c04f53ayay"]
ResourceId	Yes	No	String	Resource ID. Example: cwplic-92c9ayay

3. Output Parameters

Parameter name	Type	Description
ErrMsg	Array of LicenseUnBindRsp	This value is returned only for unbinding failures. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

ModifyOrderAttribute

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the attribute of an order.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-27 11:37:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyOrderAttribute
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
AttrName	Yes	No	String	Editable attribute name, which currently supports: alias: resource alias. projectId: project ID. Example: alias
AttrValue	Yes	No	String	Attribute value. When AttrName is alias, it allows any string up to 15 characters in length. When AttrName is projectId, it requires the project ID to be real and existing. Example: Resource Name
LicenseType	Yes	No	Uint64	License type. 0: Pro Edition license; 5: Ultimate Edition license. Example: 1
ResourceId	Yes	No	String	Resource ID. Example: resource_id

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

ModifyWarningSetting

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for modifying alarm settings

Default interface request rate limit: 20 times per second.

Interface update time: 2022-12-23 11:48:21.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyWarningSetting
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
WarningObjects	Yes	No	Array of WarningObject	Modify alarm settings. Example:View

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.
FailedOperation	Operation failed.

Vulnerability Management APIs CancelIgnoreVul

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for stopping ignoring vulnerabilities

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-06 14:58:05.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CancelIgnoreVul
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
EventIds	Yes	No	String	ID of one or more vulnerability events. Separate multiple IDs with commas (,). Example: 101,102

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

Error Code	Description
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

CreateEmergencyVulScan

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to create an emergency vulnerability scan task.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: CreateEmergencyVulScan
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
TimeoutPeriod	No	No	Uint64	Scan timeout duration, in seconds. Example: 3600
Uuids	No	No	Array of String	UUIDs of servers. This parameter takes effect for selected servers. Example: ["4aae2527-3030-41a5-a9f1-a2a002e848b6"]
VulId	Yes	No	Uint64	Vulnerability ID. Example: 105006

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeEmergencyVulList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the emergency vulnerability list.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-06 15:57:44.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeEmergencyVulList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: PublishDate, LastScanTime, and HostCount. Example: PublishDate
Filters	No	No	Array of Filters	Filter condition. • Status - String - Required: Yes - Vulnerability status. 0: not checked. 1: at risk. 2: no risk. 3: checking (progress displayed). • Level - String - Required: No - Vulnerability severity. 1: low. 2: moderate. 3: high. 4: informational. • VulName - String - Required: No - Name of the vulnerability. • Uuids - String - Required: No - UUID of the server. • IsSupportDefense - int- Required: No - Whether defense is supported. 0: not supported. 1: supported. Example:View
HotspotAttack	No	No	Bool	Whether hot spot vulnerabilities Example: true
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. asc: ascending order. desc: descending order. Example: desc

3. Output Parameters

Parameter	Type	Description

name		
ExistsRisk	Bool	Indicates whether a risk exists. Example: true
List	Array of EmergencyVul	Vulnerability list. Example:View
TotalCount	Uint64	Total number of vulnerabilities. Example: 0
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeInjectRiskyServiceSwitch

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query whether a Java Webshell and RASP have been injected into risk service.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeInjectRiskyServiceSwitch
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
JavaShellInjectRiskyServiceStatus	Uint64	Whether to inject a Java Webshell into risk service. 0: If a user has not set it, it is not injected by default. 1: Inject. 2: A user specifies not to inject. Example: 1
List	Array of RiskMainClass	Risk Service List Example:View
RaspInjectRiskyServiceStatus	Uint64	Whether to inject the host RASP into risk service. 0: If a user has not set it, it is not injected by default. 1: Inject. 2: A user specifies not to inject. Example: 1
TotalCount	Uint64	Total number of risk services. Example: 10
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeScanSchedule

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the check progress of a task based on a task ID.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:13:13.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeScanSchedule
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
TaskId	Yes	No	Uint64	Task ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
Schedule	Uint64	Check progress. Example: 1

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeScanVulSetting

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the regular check settings.

Default interface request rate limit: 20 times per second.

Interface update time: 2023-03-06 19:25:22.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeScanVulSetting
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
ClickTimeout	Uint64	Timeout period for the quick scan, such as 1800 seconds. Example: 600
EnableScan	Uint64	Indicates whether self-healing notifications are enabled. Example: 1
EndTime	String	End time. Example: 05:00
ScanMethod	Uint64	0: version comparison, 2: version comparison + POC. Example: 0
StartTime	String	Start time. Example: 00:00
TimerInterval	Uint64	Interval for regular scans. Unit: days. Example: 1
TimerTime	String	Regular check time, such as 00:00. Example: 00:00
Uuids	Array of String	If empty, scan hosts with all Professional, Premium, and General Discount editions by default; if not empty, only scan the selected hosts. Example: ["d99a1b46-cc2d-4633-a11f-4a7663d25ay*"]
VulCategories	String	Vulnerability category. 1: Web- CMS vulnerability. 2: application vulnerability. 4: Linux software vulnerability. 5: Windows system vulnerability. Example: 1
VulEmergency	Uint64	Indicates whether it is an emergency vulnerability. 0: no. 1: yes. Example: 1
VulLevels	String	Risk severity. 1: low. 2: medium. 3: high. 4: critical. Multiple risk severity levels are separated with commas (,). Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InternalError.MainDBFail	Failed to operate data.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeUndoVulCounts

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the number of pending vulnerabilities of a specified type, the number of servers of a specified type, and the number of servers of CWP Basic in the vulnerability management module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeUndoVulCounts
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
IfEmergency	No	No	String	Whether the vulnerabilities are emergency vulnerabilities. yes: yes; other values: no. Example: yes
VulCategory	No	No	Uint64	Vulnerability category. 1: Web- CMS vulnerability. 2: application vulnerability. 4: Linux software vulnerability. 5: Windows system vulnerability. Example: 1

3. Output Parameters

Parameter name	Type	Description
NotProfessionCount	Uint64	Number of servers with CWP Basic. Example: 1
UndoHostCount	Int64	Number of pending servers. Example: 1
UndoVulCount	Uint64	Number of pending vulnerabilities. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeVulCountByDates

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the number of vulnerabilities and number of servers of the specified type within the most recent days in the vulnerability management module.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVulCountByDates
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
IfEmergency	No	No	String	Specifies whether it is an emergency vulnerability. To filter the query results based on this condition, set this parameter to yes Example: 0
LastDays	No	No	Array of Uint64	Number of past days for data query. Subtract 1 from the actual number of days and fill in the value. Example: [1]
VulCategory	No	No	Uint64	Vulnerability type. 1: Web- CMS vulnerability. 2: application vulnerability. 4: Linux software vulnerability. 5: Windows system vulnerability. Example: 1

3. Output Parameters

Parameter name	Type	Description
HostCount	Array of Uint64	Number of servers by days. Example: [39]
VulCount	Array of Uint64	Number of vulnerabilities by days. Example: [167]
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeVulDefenceOverviewCount

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to obtain vulnerability defense policies and event statistics.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVulDefenceOverviewCount
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]

3. Output Parameters

Parameter name	Type	Description
StrategyCount	Uint64	Number of policies Example: 1

Parameter name	Type	Description
StrategyOpenCount	Uint64	Number of enabled policies. Example: 1
SupportDefenceVulCount	Uint64	Number of supported defense vulnerabilities. Example: 2
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeVulDefenceSettingList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the list of vulnerability defense settings.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVulDefenceSettingList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter condition: Switch, Keywords. Example:View
Limit	No	No	Uint64	Limit on data. Example: 20
MemberId	No	No	Array of String	Group Account Member ID Example: [{"mem-6wfo0fzks3","mem-85fo0fzks4"}]
Offset	No	No	Uint64	Data offset. Example: 12

3. Output Parameters

Parameter name	Type	Description
List	Array of VulDefenceSetting	Vulnerability defense settings list. Example:View
TotalCount	Uint64	Total number of records. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

DescribeVulEffectHostList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying servers affected by vulnerabilities

Default interface request rate limit: 20 times per second.

Interface update time: 2022-07-25 15:56:07.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVulEffectHostList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter conditions. • AliasName - String - Host name for filtering. • IP - String - Host IP address for filtering. • InstanceID - String - Host instance ID for filtering. • TagIds - String - Array of host tag IDs separated by commas. • Status - String - Status. 0: to be handled; 1: ignored; 3: fixed; 5: detecting; 6: fixing; 8: fixing failed. • Uuid - String array - UUID string array. • Version - String array - Paid edition array. "Flagship": Ultimate Edition; "PRO_Version": Pro Edition; "BASIC_Version": Basic Edition. • InstanceState - String array - Instance Status array. "PENDING": creating; "LAUNCH_FAILED": creation failed; "RUNNING": running; "STOPPED": shut down; "STARTING": starting; "STOPPING": shutting down; "REBOOTING": restarting; "SHUTDOWN": to be terminated; "TERMINATING": terminating; "UNKNOWN": unknown (for scenarios with non-cloud servers and offline client). Example:View
Limit	Yes	No	Uint64	Maximum number of entries to return on each page. Maximum value: 100. Example: 10
Offset	Yes	No	Uint64	The offset for paging. Example: 0
VulId	Yes	No	Uint64	Vulnerability ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
TotalCount	Uint64	Total number of servers in the list. Example: 1
VulEffectHostList	Array of VulEffectHostList	List of affected servers. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeVulHostCountScanTime

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying the number of vulnerabilities to be handled and the number of affected servers

Default interface request rate limit: 20 times per second.

Interface update time: 2022-06-27 19:13:29.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVulHostCountScanTime
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.

3. Output Parameters

Parameter name	Type	Description
IfFirstScan	Bool	Indicates whether it is the first scan. Example: true
LastFixTime	String	Time when the vulnerability was last fixed. Example: 2021-07-09 15:04:01

Parameter name	Type	Description
ScanTime	String	Scan time. Example: 2021-02-01 12:00:00
TaskId	Uint64	ID of the running task. If no task is running, a value of 0 is returned. Example: 1
TotalVulCount	Uint64	Total number of vulnerabilities. Example: 1
VulHostCount	Uint64	Number of servers affected by the vulnerability. Example: 1
hadAutoFixVul	Bool	Indicates whether vulnerability events that support automatic fixing exist. Example: true
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DescribeVulHostTop

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for querying top server risks

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-06 14:58:32.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVulHostTop
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
IsFollowVul	No	No	Uint64	Specifies whether to count only critical vulnerabilities. 1: only counts critical vulnerabilities. 0: counts all types of vulnerabilities Example: 1
Top	Yes	No	Uint64	Top N value, in the range of 1 to 100. Example: 1
VulCategory	No	No	Uint64	1: Web- CMS vulnerability. 2: application vulnerability. 4: Linux software vulnerability. 5: Windows system vulnerability. 6: emergency vulnerability. If this parameter is left empty or set to 0, the supported types of vulnerabilities specified by 1, 2, 4, and 5 will be queried. Example: 2

3. Output Parameters

Parameter name	Type	Description
VulHostTopList	Array of VulHostTopInfo	Top server risks. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeVulInfoCvss

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Vulnerability details, including the CVSS version.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-08-18 10:31:53.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVulInfoCvss
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
VulId	Yes	No	Uint64	Vulnerability ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
CVSS	String	CVSS information. Example: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CveId	String	CVE ID of the vulnerability. Example: CVE-2023-44487
CveInfo	String	CVSS details. Example: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CvssScore	Uint64	CVSS score. Example: 7.5
CvssScoreFloat	Float	CVSS score, which is a floating-point number. Example: 1
DefenseAttackCount	Uint64	Number of prevented attack attempts. Example: 12
Description	String	Description of the vulnerability. Example: Apache OFBiz is an Enterprise Resource Planning (ERP) system of the Apache Software Foundation. The system provides a whole set of Java- based web application components and tools. Versions of Apache OFBiz before 18.12.16 have a vulnerability stemming from coding issues, which is vulnerable to Server- Side Request Forgery and code injection attacks. Apache OFBiz is an Enterprise Resource Planning (ERP) system developed by the Apache Software Foundation, a U.S.-based organization. The system provides a suite of Java- based web application components and tools. Versions of Apache OFBiz before 18.12.16 have a vulnerability that makes it susceptible to server-side request forgery and code injection attacks due to flawed code implementation.
FixSwitch	Int64	Indicates whether fixing is supported. 0: not supported for either Windows or Linux system vulnerabilities. 1: supported for both Windows and Linux system vulnerabilities. 2: supported only for Linux system vulnerabilities. 3: supported only for Windows system vulnerabilities. Example: 1
Labels	String	Tags of the vulnerability, which are separated with commas (,). Example: Tag 1; tag 2
PublicDate	String	Release time. Example: 2024-09-04
Reference	String	Reference link. Example: https://ofbiz.apache.org/download.html https://ofbiz.apache.org/security.html https://issues.apache.org/jira/browse/OFBIZ-13132
RepairPlan	String	Fix solution. Example: The official patch and fixed version have been released. Please assess whether your business is affected and consider upgrading to a secure version accordingly.\n[Note]: It is recommended that you back up your data before upgrading to avoid any accidents.\n https://ofbiz.apache.org/download.html
SuccessFixCount	Uint64	Number of successful fixes in the entire network. If the vulnerability does not support automatic fixing, a value of 0 is returned by default. Example: 1
VulId	Uint64	Vulnerability ID. Example: 1
VulLevel	Uint64	Risk severity. 1: low. 1: medium. 3: high. 4: critical. Example: 1
VulName	String	Vulnerability name. Example: Apache OFBiz SSRF remote code execution vulnerability (CVE-2024-45507)
VulType	Uint64	Vulnerability category. 1: Web-CMS vulnerability. 2: application vulnerability. 4: Linux software vulnerability. 5: Windows system vulnerability. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeVulLevelCount

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the vulnerability count distribution by severity.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-06 14:59:07.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVulLevelCount
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
IsFollowVul	No	No	Uint64	Specifies whether to count only critical vulnerabilities. 1: only counts critical vulnerabilities. 0: counts all types of vulnerabilities Example: 1
VulCategory	No	No	Uint64	1: Web- CMS vulnerability. 2: application vulnerability. 4: Linux software vulnerability. 5: Windows system vulnerability. 6: emergency vulnerability. If this parameter is left empty or set to 0, the supported types of vulnerabilities specified by 1, 2, 4, and 5 will be queried. Example: 1

3. Output Parameters

Parameter name	Type	Description
VulLevelList	Array of VulLevelInfo	Statistical results, Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.

DescribeVulList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query the vulnerability list.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-06-14 18:26:56.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVulList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
By	No	No	String	Field for sorting. Valid values: Level, LastTime, and HostCount. Example: Level
Filters	No	No	Array of Filters	Filtering conditions. • Status - String - required: no - processing status. 0 - pending processing; 1 - allowlisted; 2 - deleted; 3 - fixed; 5 - detecting; 6 - fixing; 8 - fixing failed. • ModifyTime - String - required: no - last occurrence time. • Uuid- String - required: no - Query by host UUID. • VulName- String - • VulCategory- String - required: no - vulnerability category. 1: Web-CMS vulnerability; 2: application vulnerability; 4: Linux software vulnerability; 5: Windows system vulnerability. • IsSupportDefense - int- required: no - whether defense is supported. 0: not supported; 1: supported. • Labels- string- required: no - search by tag. • IsSupportAutoFix- string- required: no - whether automatic fixing is supported. 0: not supported; 1: supported. • CvssScore- string- required: no - lower limit of CVSS score. • AttackLevel- string- required: no - lower limit of attack level. Example:View
Limit	No	No	Uint64	Maximum number of entries to return. Maximum value: 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
Order	No	No	String	Sorting order. Valid values: asc and desc. Default value: asc. Example: desc

3. Output Parameters

Parameter name	Type	Description
FollowVulCount	Uint64	Number of critical vulnerabilities. Example: 23

Parameter name	Type	Description
TotalCount	Uint64	Total number of vulnerabilities. Example: 1
VulInfoList	Array of VulInfoList	Vulnerability list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

DescribeVulTop

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to query statistics about top vulnerabilities.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-06 14:58:45.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: DescribeVulTop
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
IsFollowVul	No	No	Uint64	Specifies whether to count only critical vulnerabilities. 1: only counts critical vulnerabilities. 0: counts all types of vulnerabilities Example: 1
Top	Yes	No	Uint64	Top N value, in the range of 1 to 100. Example: 1
VulCategory	No	No	Uint64	1: Web- CMS vulnerability. 2: application vulnerability. 4: Linux software vulnerability. 5: Windows system vulnerability. 6: emergency vulnerability. If this parameter is left empty or set to 0, the supported types of vulnerabilities specified by 1, 2, 4, and 5 will be queried. Example: 2

3. Output Parameters

Parameter name	Type	Description
VulTopList	Array of VulTopInfo	Top vulnerability list. Example:View
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ExportVulDetectionExcel

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting the Excel file of the current vulnerability scan

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-06 14:55:06.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportVulDetectionExcel
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
TaskId	Yes	No	Uint64	ID of the current vulnerability scan task, which is different from the ID of the task that exports the Excel file of the current vulnerability scan in the output parameters. Example: 1596595610

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	This parameter has been deprecated. Example: http://1.2.3.4/result.zip
TaskId	String	Task ID, which can be used to obtain the download URL (DownloadUrl) by calling the ExportTasks API. (This ID differs from the vulnerability detection task ID in the input parameters.) Example: 1615549629
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ExportVulDetectionReport

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to export a vulnerability check report.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:12:33.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportVulDetectionReport
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filters	Filter parameters. • MachineName - String - Required: No - Host alias. \n • Ip - String - Required: No - Host IP address. \n • InstanceID - String - Required: No - Host instance ID. • Status - String - Required: No - Event Status. 0: to be fixed; 1: ignored; 3: fixed; 5: detecting. Example:View
Limit	No	No	Uint64	Number of items to be returned. The default value is 10, and the maximum value is 100. Example: 10
Offset	No	No	Uint64	Offset. Default value: 0. Example: 0
TaskId	Yes	No	Uint64	ID of the vulnerability scan task, which is different from the ID of the task that exports the scan report in the output parameters. Example: 1596595610

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	Download URL of the exported file. Example: http://1.2.3.4/result.zip
TaskId	String	ID of the task that exports the check report. This ID is different from the ID of the vulnerability scan task specified in the input parameters. Example: 1615549629
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ExportVulEffectHostList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting servers affected by vulnerabilities

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-06 14:54:52.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportVulEffectHostList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filter conditions. • AliasName - String - Host name for filtering. • IP - String - Host IP address for filtering. • InstanceID - String - Host instance ID for filtering. • TagIds - String - Array of host tag IDs separated by commas. • Status - String - Status. 0: to be handled; 1: ignored; 3: fixed; 5: detecting; 6: fixing; 8: fixing failed. • Uuid - String array - UUID string array. • Version - String array - Paid edition array. "Flagship": Ultimate Edition; "PRO_Version": Pro Edition; "BASIC_Version": Basic Edition. • InstanceState - String array - Instance Status array. "PENDING": creating; "LAUNCH_FAILED": creation failed; "RUNNING": running; "STOPPED": shut down; "STARTING": starting; "STOPPING": shutting down; "REBOOTING": restarting; "SHUTDOWN": to be terminated; "TERMINATING": terminating; "UNKNOWN": unknown (for scenarios with non-cloud servers and offline client). Example:View
VulId	Yes	No	Uint64	Vulnerability ID. Example: 1

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	Deprecated parameter. Example: url
TaskId	String	ID of the file export task. You can call the ExportTasks API to download the exported file based on this ID. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
InvalidParameter.IllegalRequest	Invalid request.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ExportVulList

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for exporting vulnerabilities in the vulnerability management module

Default interface request rate limit: 20 times per second.

Interface update time: 2023-03-21 10:26:24.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ExportVulList
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Filters	No	No	Array of Filter	Filtering conditions. • Status - String - required: no - processing status: 0 - pending processing; 1 - allowlisted; 2 - deleted; 3 - ignored. • ModifyTime - String - required: no - last occurrence time. • Uuid- String - required: no - Query by host UUID. • VulName- String - • VulCategory- String - required: no - vulnerability category: 1: Web-CMS vulnerability; 2: application vulnerability; 4: Linux software vulnerability; 5: Windows system vulnerability. • IsSupportDefense - int- required: no - whether defense is supported: 0: not supported; 1: supported. • Labels- string- required: no - search by tag. • IsSupportAutoFix- string- required: no - whether automatic fixing is supported: 0: not supported; 1: supported. • CvssScore- string- required: no - lower limit of CVSS score. • AttackLevel- string- required: no - lower limit of attack level. Example:View
IfDetail	No	No	Uint64	Specifies whether to export details. 1: yes. 0: no. Example: 1

3. Output Parameters

Parameter name	Type	Description
DownloadUrl	String	Download URL of the exported file. This parameter has been deprecated. Example: http://www.ay.com/ay
TaskId	String	ID of the file export task. You can call the ExportTasks API to download the exported file based on this ID. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.MissingParameter	Missing parameter.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

IgnoreImpactedHosts

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to ignore one or more vulnerabilities.

Default interface request rate limit: 20 times per second.

Interface update time: 2022-09-06 14:57:53.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: IgnoreImpactedHosts
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
Ids	Yes	No	Array of Uint64	Vulnerability IDs. Example: [545521374]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

ModifyInjectRiskyServiceSwitch

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

This API is used to modify the switch for injecting a Java Webshell and RASP into risk service.

Default interface request rate limit: 20 times per second.

Interface update time: 0001-01-01 00:00:00.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ModifyInjectRiskyServiceSwitch
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
JavaShellInjectRiskyServiceStatus	No	No	Uint64	Whether to inject a Java Webshell into risk service. 0: If a user has not set it, it is not injected by default. 1: Inject. 2: A user specifies not to inject. Example: 1
RaspInjectRiskyServiceStatus	No	No	Uint64	Whether to inject the host RASP into risk service. 0: If a user has not set it, it is not injected by default. 1: Inject. 2: A user specifies not to inject. Example: 1

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
MissingParameter	Missing parameter.
ResourceNotFound	The resource does not exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ScanVul

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Quick scan API

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ScanVul
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
HostType	Yes	No	Uint64	Server type. 1: server with CWP Pro. 2: selected server. Example: 1
QuuidList	No	No	Array of String	QUUIDs of servers. This parameter takes effect if the HostType parameter is set to 2 (selected server). Example: ["69796250-2a3a-40ef-b418-676e677019a4"]
ScanMethod	No	No	Uint64	0: version comparison, 2: version comparison + POC. Example: 0
TimeoutPeriod	No	No	Uint64	Timeout period. Unit: seconds. Default value: 3600. Example: 180
VulCategories	No	No	String	Vulnerability category. 1: Web- CMS vulnerability. 2: application vulnerability. 4: Linux software vulnerability. 5: Windows system vulnerability. (Separate multiple values with semicolons (;).) Example: 1
VulEmergency	No	No	Uint64	Whether it is an emergency vulnerability. 0: no. 1: yes. Example: 1
VulIds	No	No	Array of Uint64	ID of the vulnerability that you want to scan. Example: [1]
VulLevels	Yes	No	String	Risk severity. 1: low. 2: medium. 3: high. 4: critical. (Separate multiple values with semicolons (;).) Example: 1

3. Output Parameters

Parameter name	Type	Description
TaskId	Uint64	Task ID. Example: 1
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
ResourceNotFound	The resource does not exist.
InvalidParameter.IllegalRequest	Invalid request.
FailedOperation.APIServerFail	Failed to call the API service.
FailedOperation.NoProfessionHost	No servers with CWP Pro exist.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

Error Code	Description
FailedOperation	Operation failed.

ScanVulAgain

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

Vulnerability rescan API

Default interface request rate limit: 20 times per second.

Interface update time: 2022-05-20 15:11:35.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ScanVulAgain
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
EventIds	Yes	No	String	ID of one or more vulnerability events. Separate multiple IDs with commas (,). Example: 1
Uuids	No	No	String	UUIDs of servers that you want to check again. Separate multiple UUIDs with commas (,). Example: 05f0bcab-726c-4ea4-8109-bcd03d5598f7

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.

Error Code	Description
InvalidParameter.InvalidFormat	Incorrect parameter format.
ResourceNotFound	The resource does not exist.
FailedOperation.RescanVul	Failed to scan for vulnerabilities again.
InvalidParameter.IllegalRequest	Invalid request.
FailedOperation.APIServerFail	Failed to call the API service.
InvalidParameter	Invalid parameter.
OperationDenied	Operation denied.
InvalidParameterValue	The parameter value is invalid.

ScanVulSetting

1. Interface Description

Interface request domain name: cwp.api3.convergecloud.com.

API for setting regular vulnerability scanning

Default interface request rate limit: 20 times per second.

Interface update time: 2023-03-06 19:25:31.

The interface is both signature verification and authentication.

2. Input Parameters

The following list of request parameters only lists interface request parameters and some public parameters, For a complete list of public parameters see public request parameters.

Parameter name	Required	Allow NULL	Type	Description
Action	Yes	No	String	Public parameter, The value of this interface: ScanVulSetting
Version	Yes	No	String	Public parameter, The value of this interface: 2018-02-28
Region	No	No	String	Public parameter,Regional information This interface does not need to pass this parameter.
EnableScan	No	No	Uint64	Specifies whether to enable scanning. 1: yes. 0: no. Example: 1
EndTime	No	No	String	Time to stop scanning, such as 08:00. Example: 01:59
ScanMethod	No	No	Uint64	0: version comparison, 2: version comparison + POC. Example: 0
StartTime	No	No	String	Time to start scanning, such as 00:00. Example: 00:00
TimerInterval	Yes	No	Uint64	Interval for regular scans. Unit: days. Example: 1
TimerTime	No	No	String	Regular scan time, such as 02:10:50. Example: 02:10:50
Uuids	No	No	Array of String	If empty, scan hosts with all Professional, Premium, and General Discount editions by default; if not empty, only scan the selected hosts. Example: ["5a540076-d38a-4078-aa98-q45rt371d322"]
VulCategories	No	No	Array of Uint64	Vulnerability category. 1: Web- CMS vulnerability. 2: application vulnerability. 4: Linux software vulnerability. 5: Windows system vulnerability. Pass in the parameter value in the format of an array, such as [1,2]. Example: [1]
VulEmergency	No	No	Uint64	Whether it is an emergency vulnerability. 0: no. 1: yes. Example: 1
VulLevels	No	No	Array of Uint64	Risk severity. 1: low. 2: medium. 3: high. 4: critical. Pass in the parameter value in the format of an array, such as [1,2,3]. Example: [1]

3. Output Parameters

Parameter name	Type	Description
RequestId	String	Unique request id, Each request will return. The RequestId of the request needs to be provided when locating the problem.

4. Error Code

The following lists only the error codes related to the interface business logic, For other error codes, see public ErrorCode.

Error Code	Description
InternalError	Internal error.
InvalidParameter.ParsingError	Parameter parsing error.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
MissingParameter	Missing parameter.
InvalidParameter	Invalid parameter.
InvalidParameterValue	The parameter value is invalid.

Data structure

BaselineItem

Baseline item information.

Referenced by the following interfaces: DescribeBaselineItemList

name	required	NULL allowed	type	description
CanBeFixed	no	yes	Int64	Whether it can be fixed. Example: 1
CategoryId	no	no	Int64	Category of the check item. Example: 50
DetectResultDesc	no	yes	String	Description of the check result. Example: If Redis is started with the root permission and access is not authorized, the arbitrary file write issue occurs, resulting in a command execution vulnerability.
DetectStatus	no	yes	Int64	Check status. 0: not passed. 1: ignored. 3: passed. 5: checking. Example: 1
FirstTime	no	yes	String	First occurrence time. Example: 1
FixMethod	no	no	String	Fix solution. Example: 1. Start Redis with low user permission.
HostId	no	yes	String	Server ID. Example: 1
HostIp	no	yes	String	IP address of the server. Example: 192.168.0.1
HostName	no	yes	String	Server name. Example: redis_node_cvm
ItemDesc	no	no	String	Description of the check item. Example: If Redis is started with the root permission and access is not authorized, the arbitrary file write issue occurs, resulting in a command execution vulnerability.
ItemId	no	no	Int64	Item ID. Example: 1100
ItemName	no	no	String	Item name. Example: Redis baseline compliance check
LastTime	no	yes	String	Last occurrence time. Example: 2021-01-01 12:00:00
Level	no	yes	Int64	Baseline risk level. 0: low; 1: medium; 2: high; 3: critical. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information Example:View
RuleName	no	no	String	Rule name. Example: Weak password check for Linux system
Uuid	no	yes	String	UUID of the CWP agent. Example: 5a540076-d38a-4078-aa98-q45rt371d322
WanIp	no	yes	String	Public IP address. Example: 15.236.25.11

BanWhiteListDetail

Blocklist details, including server information.

Referenced by the following interfaces: DescribeBanWhiteList

name	required	NULL allowed	type	description
CreateTime	yes	no	Datetime	Time when the blocklist was created. Example: 2021-03-03 16:05:00
Id	yes	no	String	Allowlist ID. Example: 1
IsGlobal	yes	no	Bool	Whether the blocklist is global. Example: false
MachineIp	yes	no	String	Server IP address. Example: 10.0.0.2
MachineName	yes	no	String	The instance name Example: machineName
ModifyTime	yes	no	Datetime	Time when the blocklist was modified. Example: 2021-03-03 16:05:00
Quuid	yes	no	String	QUUID of the server. Example: 059cb8b1-98c7-4e44-8345-ba9d87d722e2
Remark	yes	no	String	Alias of the blocklist. Example: remarkName
SrcIp	yes	no	String	Source IP address in the blocklist. Example: 10.0.0.1
Uuid	yes	no	String	UUID of the CWP agent. Example: 059cb8b1-98c7-4e44-8345-ba9d87d722e2

BaselineItemDetect

Baseline check item.

Referenced by the following interfaces: DescribeBaselineItemDetectList

name	required	NULL allowed	type	description
DetectResult	yes	yes	String	Check result, in JSON string format. (This field is deprecated.) Example: Obsolete
DetectStatus	yes	yes	Int64	0: checked not passed. 1: ignored. 3: check passed. 5: checking. Example: 1
FirstTime	yes	yes	String	First scan time. Example: 2021-02-01 12:00:00
FixMethod	yes	yes	String	Fix solution. Example: Create a dedicated user (generally named mongodb) for performing MongoDB database activities, and use this dedicated user to run MongoD...
HostCount	yes	yes	Int64	Number of affected servers. Example: 1
ItemDesc	yes	yes	String	Description of the check item. Example: If Redis is started with the root permission and access is not authorized, the arbitrary file write issue occurs, resulting in a command execution vulnerability.
ItemId	yes	yes	Int64	Item ID. Example: 1401
ItemName	yes	yes	String	Item name. Example: Redis baseline compliance check
LastTime	yes	yes	String	Last detection time. Example: 2021-02-01 12:00:00
Level	yes	yes	Int64	Risk level. Example: 2
NotPassedHostCount	yes	yes	Int64	Number of servers that failed the check. Example: 1
PassedHostCount	yes	yes	Int64	Number of servers that passed the check. Example: 1
RuleId	yes	yes	Int64	Rule ID. Example: 120
RuleName	yes	yes	String	Rule name. Example: Weak password

MachineLoginType

Host login

Referenced by the following interfaces: DescribeMachineLoginType

name	required	NULL allowed	type	description
InstanceId	no	yes	String	Instance ID. Example: ins-36843684
LoginType	no	yes	Uint64	Login method: 0 - original login method; 1 - password-free QR code login; 2 - enable QR code scanning; 3 - disable QR code scanning. Example: 0
Quuid	no	yes	String	Host QUUID. Example: cf7068b1-ebac-47c4-aa68-171888888888

IgnoreRuleEffectHostInfo

Server information affected by an ignored check item.

Referenced by the following interfaces: DescribeIgnoreRuleEffectHostList

name	required	NULL allowed	type	description
EventId	yes	yes	Uint64	Event ID. Example: 1
HostName	yes	yes	String	Server name. Example: redis_node_cvm
LastScanTime	yes	yes	String	Last detection time. Example: 2021-11-10 00:00:00
Level	yes	yes	Uint64	Risk severity. 1: low. 2: medium. 3: high. 4: critical. Example: 1
Quuid	yes	yes	String	QUUID of the server. Example: 915e27b1-d675-4509-80bf-99bf07f64237
Status	yes	yes	Uint64	Status. 0: not passed. 1: ignored. 3: passed. 5: checking. Example: 0
TagList	yes	yes	Array of String	Server tags. Example: ["tag-01"]

VulEventList

Vulnerability events.

Referenced by the following interfaces: DescribeEventList

name	required	NULL allowed	type	description
AliasName	yes	no	String	Host alias. Example: redis_node_cvm
Descript	yes	no	String	Vulnerability description. Example: If Redis is started with the root permission and access is not authorized, the arbitrary file write issue occurs, resulting in a command execution vulnerability.
HostIp	yes	no	String	HostIp Example: 192.168.0.10
Id	yes	no	Uint64	ID of the vulnerability event. Example: 1
IfProfession	yes	no	Bool	Whether CWP Pro is activated. Example: false
LastTime	yes	no	String	Last detection time. Example: 2020-02-01 12:00:00
Level	yes	no	Uint64	Vulnerability severity. 1: low. 2: medium. 3: high. 4: informational. Example: 1
Name	yes	no	String	Vulnerability name. Example: Apache HTTP/2 DoS vulnerability (CVE-2023-44487)
PublishTime	yes	no	String	Time when the vulnerability was published. Example: 2020-02-01 12:00:00
Quuid	yes	no	String	QUUID of the server. Example: 5a540076-d38a-4078-aa98-qwert371d322
Status	yes	no	Uint64	Event status. 0: to be handled. 1: ignored. 3: fixed. 5: checking. You can only manage vulnerabilities in the preceding valid states in the console. Example: 1
Uuid	yes	no	String	Uuid Example: 5a540076-d38a-4078-aa98-qwert371d322

name	required	NULL allowed	type	description
VulId	yes	no	Uint64	Vulnerability ID. Example: 1

LicenseBindTaskDetail

License binding task details.

Referenced by the following interfaces: DescribeLicenseBindSchedule

name	required	NULL allowed	type	description
ErrMsg	yes	no	String	Error message. Example: No machine was found.
FixMessage	no	yes	String	Fix suggestions. Example: Asset management - host list - click Synchronize Assets.
MachineExtraInfo	no	yes	MachineExtraInfo	Additional Information on Machine ExampleView
Quuid	yes	no	String	UUID of the cloud server. Example: 93b5fa8f-f5bc-4cf9-8253-d2739e5aa484
Status	yes	no	Uint64	0: running. 1: successful. 2: failed. Example: 2

FileTamperRule

Core file monitoring rule.

Referenced by the following interfaces: DescribeFileTamperEventRuleInfo, DescribeFileTamperRuleInfo, DescribeMachineFileTamperRules, ModifyFileTamperRule

name	required	NULL allowed	type	description
Action	yes	no	String	Perform an action: skip (to skip), alert (to send alarms). Example: alert
FileAction	yes	no	String	Monitoring behavior. • read: read file • write: modify file • read;write: read or modify file Example: read
ProcessPath	yes	no	String	Process path. Example: /tmp/*
Target	yes	no	String	Path of the accessed file. Example: /etc/shadow

NetAttackEventInfo

Referenced by the following interfaces: DescribeAttackEventInfo

name	required	NULL allowed	type	description
AbnormalAction	no	yes	String	Unusual behavior Example: dinslog:vSgcrlnyt94ka7tk2qls16y0:sec:dnslog:ayay
AttackLevel	no	yes	Uint64	Attack level. If the value is 3 or higher, the attack is a notable attack. Example: 3
CVEId	no	yes	String	CVE number Example: CVE-2023-44487
Count	no	yes	Uint64	Attacks Example: 1
DstPort	no	yes	Uint64	Target port. Example: 80
HostOpProcessTree	no	yes	String	Process Tree, needs to be decoded with base64. Example: W3siaGlkIjoyODc0MCwiZXhlIjoiL3Vzci9iaW4vY3VybCIsImFjY291bnQiOiIwQiAiLCJjbWRsaW5lIjoiY3VybCAtcyAtTCBodHRwczovL2Rvd25sb2FkLmMxcGlv
HostOpType	no	yes	Uint64	0: No Compromised Behavior 1: RCE (command execution) 2: Dnslog 3: Writefile Example: 1
Id	no	yes	Uint64	Event ID. Example: 49754647
Location	no	yes	String	Attack Source Example: location1-location2
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information ExampleView
MergeTime	no	yes	String	Time of Attack Example: 2021-02-01 12:00:00
NetPayload	no	yes	String	Attack packets Example: POST /wls-wsat/CoordinatorPortType HTTP/1.1 X-Stgw-Time: 1730212752.801 Host: h2.bjhd111.com X-Client-Proto: https X-Forwarded-Proto: https X-Client-Proto-Ver: HTTP/1.1
PayVersion	no	yes	Uint64	Machine payment edition. 0: Basic Edition; 1: Professional Edition; 2: Premium Edition; 3: General Discount Edition Example: 1
Quuid	no	yes	String	CVM UUID Example: 3ddf6cc1-9389-4b9a-a10b-85f30491ayay
SrcIP	no	yes	String	Attack source IP address. Example: 192.168.0.204
Status	no	yes	Uint64	Processing Status: 0 Pending, 1 Processed, 2 Allowlisted, 3 Ignored, 4 Deleted, 5: Defense Enabled. Example: 1
SvcPs	no	yes	String	Service Process Base64 Example: eyJhY2NvdW50IjoiMDoxIiwiYXJnd6l0m5naW54OiBtYXNtZXIgcHJvY2VzcyAxdXNyL3NiaW4vbmdpbngiLCJleGUiOiIvdXNyL2lnaW54L25naW54LS1naW54LWdldGVuIjoiMC4wLjAuMDo4MCIsInBpZCI6MTI0ayay
Type	no	yes	Uint64	0: Attack Attempt 1: Successful Attack Example: 1
Uuid	no	yes	String	Host UUID. Example: 3ddf6cc1-9389-4b9a-a10b-85f30491ayay
VulDefenceStatus	no	yes	Uint64	Vulnerability Defense Status: 0 Disabled, 1 Enabled. Example: 1
VulId	no	yes	Uint64	Vulnerability ID. Example: 100386
VulName	no	yes	String	Vulnerability name. Example: Weblogic deserialization and remote code execution vulnerability (CVE-2019-2725)
VulSupportDefense	no	yes	Uint64	Whether vulnerabilities support defense. 0: No 1: Yes Example: 1

FileTamperRuleCount

Quantity information of the core file monitoring rules associated with servers.

Referenced by the following interfaces: DescribeFileTamperRuleCount

name	required	NULL allowed	type	description
Count	yes	no	Uint64	Number of associated rules. Example: 1
Name	yes	yes	String	Name of the associated rule. This value displays only the name of one rule. Example: redis_node_check
Uuid	yes	no	String	Host UUID. Example: 935e27b1-d675-4509-80bf-96fb9f764237

BaselineEventLevelInfo

Information about top servers at risk.

Referenced by the following interfaces: DescribeBaselineHostTop

name	required	NULL allowed	type	description
EventCount	yes	yes	Uint64	Number of vulnerabilities. Example: 10
EventLevel	yes	yes	Uint64	Risk severity. 1: low. 1: medium. 3: high. 4: critical. Example: 2

VulDefenceRangeDetail

Exploit prevention scope details.

Referenced by the following interfaces: DescribeVulDefenceList

name	required	NULL allowed	type	description
Cveid	yes	no	String	cve id Example: CVE-2020-9496
CvssScore	yes	no	Float	CVSS score. Example: 6.1
Label	yes	no	String	Tag. Example: Remote exploit
Level	yes	no	Uint64	Vulnerability severity. 1: low-risk. 2: medium-risk. 3: high-risk. 4: critical. Example: 2
PublishTime	yes	no	String	Release time. Example: 2020-07-16 00:15:00
VulId	yes	no	Int64	Vulnerability ID. Example: 1210168
VulName	yes	no	String	Vulnerability name. Example: Apache HTTP/2 DoS vulnerability (CVE-2023-44487)

ProtectDirInfo

List of protected directories.

Referenced by the following interfaces: DescribeProtectDirList

name	required	NULL allowed	type	description
AutoRestoreSwitchStatus	yes	no	Uint64	Status of automatic recovery. This value is returned when the query results are filtered by QUUID. Default value: 0. Example: 0
DirName	yes	no	String	Website name. Example: nginx web
DirPath	yes	no	String	URL of the protected directory. Example: /opt/nginx
FirstProtectTime	no	yes	String	First enabled Example: 2021-02-01 12:00:00
Id	yes	no	String	Unique ID. Example: 2
LatestProtectTime	no	yes	String	Last enabled Example: 2021-02-01 12:00:00
NoProtectServerNum	yes	no	Uint64	Number of unprotected servers. Example: 0
ProtectException	yes	no	Uint64	Protection exception. Example: 0
ProtectFileType	no	yes	String	Protected file type. Example: php;js
ProtectFilesCount	no	yes	Int64	Protected files Example: 0
ProtectServerNum	yes	no	Uint64	Number of protected servers. Example: 0
ProtectStatus	yes	no	Uint64	Protection status. Example: 0
RelatedServerNum	yes	no	Uint64	Number of associated servers. Example: 0

AssetPlanTask

List of scheduled tasks in the asset management module.

Referenced by the following interfaces: DescribeAssetPlanTaskList

name	required	NULL allowed	type	description
Command	no	no	String	Command or script to run. Example: /root/xshd
ConfigPath	no	no	String	Path of the configuration file. Example: /etc/xshd
Cycle	no	no	String	Execution cycle. Example: 10 *
FirstTime	no	no	String	First collection time. Example: 2022-07-15 11:27:01
IsNew	no	no	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	no	no	String	Server IP. Example: 10.0.0.11
MachineName	no	no	String	Server name. Example: redis_node_cvm
MachineWanIp	no	no	String	Public IP address of a server. Example: 1.1.1.1
OsInfo	no	no	String	Operating system. Example: centos 64bit
Quuid	no	no	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-841162cb8116
Status	no	no	Uint64	Default enabling status. 1: enabled. 2: not enabled. Example: 1
UpdateTime	no	yes	String	Data update time. Example: 2011-11-11 12:12:12
User	no	no	String	User who triggers initialization. Example: root
Uuid	no	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-841162cb8116

CanFixVulInfo

Server information for a vulnerability included in the messages displayed for batch vulnerability fixing.

Referenced by the following interfaces: DescribeCanFixVulMachine

name	required	NULL allowed	type	description
FixTag	yes	yes	Array of String	Fix tags. Example: ["restart needed"]
HostList	yes	yes	Array of VulInfoHostInfo	Information about servers on which the vulnerability can be fixed. Example:View
VulCategory	no	yes	Uint64	Vulnerability category. 1: web CMS vulnerability. 2: application vulnerability. 4: Linux software vulnerability. 5 Windows system vulnerability. Example: 1
VulId	yes	yes	Uint64	Vulnerability ID. Example: 1373
VulName	yes	yes	String	Vulnerability name. Example: Local permission escalation vulnerability

AssetNetworkCardInfo

Network card information in the asset management module.

Referenced by the following interfaces: DescribeAssetMachineDetail, DescribeAssetMachineInfo

name	required	NULL allowed	type	description
DnsServer	yes	no	String	DNS server. Example: 8.8.8.8
GateWay	yes	no	String	Gateway. Example: 10.0.0.1
Ip	yes	no	String	IPv4 address. Example: 172.17.0.1
Ipv6	yes	no	String	IPv6 address. Example: fe80::42:4dff:fe1b:ed8c
Mac	yes	no	String	MAC address. Example: 16:75:bf:b8:73:9c
Name	yes	no	String	Network card name. Example: eth1

BaselineRule

Baseline rule.

Referenced by the following interfaces: DescribeBaselineRuleIgnoreList, DescribeBaselineRuleList, ModifyBaselineRule

name	required	NULL allowed	type	description
AssetType	no	yes	Int64	0: all servers with CWP Pro and all servers with CWP Ultimate. 1: server ID. 2: IP address. Example: 1
CategoryId	no	no	Int64	Rule category ID. Example: 1
HostCount	no	no	Int64	Number of servers. Example: 0
HostIds	no	yes	Array of String	Server IDs. Example: ["F00A8503-6233-452E-913E-DAFEE9ayayay", "E3CB79D9-8892-408C-AE2D-A90059ayayay"]
HostIps	no	yes	Array of String	IP address of the server. Example: ["10.0.1.11","10.0.0.12"]
Items	no	no	Array of Item	Item IDs. Example:View
RuleDesc	no	no	String	Rule description. Example: International standard—CentOS 6 security baseline check
RuleId	no	no	Int64	Rule ID. Example: 11
RuleName	yes	no	String	Rule name. The maximum length is 128 characters. Example: International standard—CentOS 6 security baseline check
RuleType	no	no	Int64	Rule type. 0: system rule. 1: custom rule. Example: 1

KeyValueArrayInfo

Index key information.

Referenced by the following interfaces: DescribeLogIndex

name	required	NULL allowed	type	description
Key	yes	no	String	Field of the key or metafield index that you want to configure. Example: key1
Value	yes	no	ValueInfo	Index description of the field. Example:View

OrderModifyObject

Order Modification Parameter Object

Referenced by the following interfaces: CreateLicenseOrder

name	required	NULL allowed	type	description
InquireNum	no	no	Int64	Scale-up/Scale-down Count, which is ignored for reconfiguration sub-product Example: 1242
NewSubProductCode	no	no	String	New Product Identification. PRO_VERSION: Professional Edition; FLAGSHIP: Premium Edition Example: PRO_VERSION
ResourceId	no	no	String	Resource ID. Example: 'cakf-4mmsayayay'

UnionProtectDetail

Billable item information for jointly purchased container protection.

Referenced by the following interfaces: DescribeLicenseList

name	required	NULL allowed	type	description
Deadline	no	yes	String	The point in time when it expires. Example: 2024-07-30 15:02:19
InquireKey	no	yes	String	Billing Item Example: sv_yunjing_ue_x
Number	no	yes	Int64	Total number. Example: 10
ResourceId	no	yes	String	Resource ID. Example: resource_gdskh12h

AssetUserDetail

Basic account information in the asset management module.

Referenced by the following interfaces: DescribeAssetUserInfo

name	required	NULL allowed	type	description
DisableTime	yes	no	String	Time when the account expires. Example: 2024-10-22 19:44:42
Gid	yes	no	String	Account GID. Example: 16
GroupName	yes	no	String	User group name. Example: root
HomePath	yes	no	String	Home directory. Example: 1
IsDomain	yes	no	Uint64	Whether a domain account: 0: no; 1: yes; 999: null (Windows only). Example: 1
IsRoot	yes	no	Uint64	Whether it is granted the root permissions. 0: no. 1: yes. 999: empty string. This parameter is applicable only to Linux systems. Example: 1
IsSshLogin	yes	no	Uint64	Whether SSH logins are allowed. 1: allowed. 0: not allowed. 999: empty string. This parameter is applicable only to Linux systems. Example: 1
Keys	yes	yes	Array of AssetUserKeyInfo	List of custom public keys. Example:View
LastLoginIp	yes	no	String	Last login IP address. Example: 1.1.1.1
LastLoginLoc	yes	no	String	Last login location. Example: usa
LastLoginTerminal	yes	no	String	Terminal on which it was last logged in. Example: 1
LastLoginTime	yes	no	String	Last login time. Example: 2024-10-22 19:44:19
MachineIp	yes	no	String	Private IP address of the server. Example: 10.0.0.11

name	required	NULL allowed	type	description
MachineName	yes	no	String	Server name. Example: redis_node_cvm
Name	yes	no	String	The username. Example: root
PasswordChangeTime	yes	no	String	Password reset time. Example: 2024-10-22 19:44:42
PasswordChangeType	yes	no	Uint64	Password reset setting. 0: the password cannot be reset. 1: the password can be reset. Example: 1
PasswordDueTime	yes	no	String	Time when the password expires. This parameter is applicable only to Linux systems. Example: 2024-10-22 19:44:42
PasswordLockDays	yes	no	Int64	Number of days for which the password is locked. -1: never locked. 999: empty string. This parameter is applicable only to Linux systems. Example: 1
PasswordWarnDays	yes	no	Uint64	When to send a notification before the password expires. Unit: days. Example: 10
Quuid	yes	no	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Remark	yes	no	String	Description. Example: no login
Shell	yes	no	String	Path of the shell. This parameter is applicable only to Linux systems. Example: /root
ShellLoginStatus	yes	no	Uint64	Whether it is a shell login. 0: no. 1: yes. This parameter is applicable only to Linux systems. Example: 1
Status	yes	no	Uint64	Account status. 0: disabled. 1: enabled. Example: 1
Uid	yes	no	String	Account UID. Example: 134393481
UpdateTime	yes	yes	String	Data update time. Example: 2011-11-11 12:12:12
UserType	yes	no	Uint64	Account type: 0: guest user; 1: standard user; 2: administrator user; 999: null (Windows only). Example: 1
Uuid	yes	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

LoginWhiteCombinedInfo

Login allowlist after merging.

Referenced by the following interfaces: DescribeLoginWhiteCombinedList

name	required	NULL allowed	type	description
CreateTime	yes	no	String	Creation time. Example: 2024-11-04 09:57:28
Desc	yes	no	String	Allowlist description. If IsLocal is set to 1, the description is fixed as All servers. If the allowlist applies to only a single server, the description is the server's name. If the allowlist applies to multiple servers, the description is the server QUUID. Example: 192.168.0.2
EndTime	yes	no	String	End time. Example: 2024-11-04 09:57:28
Id	yes	no	Uint64	Allowlist ID. Example: 1001
IsGlobal	yes	no	Uint64	Whether it takes effect globally. 1: globally effective. 0: valid only for specified servers. Example: 1
Locale	yes	no	String	Region string. Example: locale1
Locations	yes	no	String	Login Location Example: location1
ModifyTime	yes	no	String	The point in time when the namespace was last modified. Example: 2024-11-04 09:57:28
Name	yes	no	String	Allowlist name. If IsLocal is set to 1, the name is fixed as All servers. If the allowlist applies to only a single server, the name is the server's name. If the allowlist applies to multiple servers, the name is the server QUUID. Example: redis_node_cvm
Places	yes	yes	Array of Place	Region of the allowlist. Example:View
Remark	yes	no	String	Description. Example: add redis cvm ip
SrcIp	yes	no	String	IP addresses in the allowlist. Multiple IP addresses are separated with commas (,). Example: 192.168.0.204
StartTime	yes	no	String	Start time. Example: 2024-11-04 09:57:28
UserName	yes	no	String	Users in the allowlist. Separate multiple usernames with commas (,). Example: uname
Uuid	yes	no	String	Server UUID. Example: df133b24-8528-4809-9d07-a9e4d58ad566

ScreenProtectionCnt

Situation data returned from the CWP dashboard visualization module.

Referenced by the following interfaces: DescribeScreenProtectionCnt

name	required	NULL allowed	type	description
Count	yes	no	Uint64	Total number. Example: 12
Name	yes	no	String	cloud: cloud scanning and cleaning engine. detect: detection engine. defend: attack defense. threat: threat intelligence. analysis: exception analysis. ai: AI engine. Example: Threat intelligence
Type	yes	no	String	cloud: cloud scanning and cleaning engine. detect: detection engine. defend: attack defense. threat: threat intelligence. analysis: exception analysis. ai: AI engine. Example: cloud

HostInfo

Server information used for creating a login audit allowlist.

Referenced by the following interfaces: AddLoginWhiteLists, ModifyLoginWhiteRecord

name	required	NULL allowed	type	description
Quuid	yes	no	String	Host QUUID. Example: df93a1b46-cc2d-4633-a11f-4a7663d2523e
Uuid	yes	no	String	Host UUID. Example: df93a1b46-cc2d-4633-a11f-4a7663d2523e

RansomDefenseStrategyMachineInfo

Anti-Ransomware Machine Hard Disk Configuration

Referenced by the following interfaces: CreateRansomDefenseStrategy

name	required	NULL allowed	type	description
DiskInfo	no	yes	String	Specified Hard Disk List. When it is empty, it means all hard disks: disk_id1
Uuid	yes	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

AssetWebLocationInfo

Website information in the asset management module.

Referenced by the following interfaces: DescribeAssetWebLocationInfo

name	required	NULL allowed	type	description
Command	yes	no	String	Start Command Example: true
Ip	yes	no	String	Binds the IP address. Example: 0.0.0.0
MainPath	yes	no	String	Main directory. Example: /data
Name	yes	no	String	Domain name. Example: domain.com
Port	yes	no	String	Port of the website. Example: 22
Proto	yes	no	String	Protocol of the website. Example: tcp
SafeStatus	yes	no	Uint64	Security module status. 0: not enabled. 1: enabled. 999: empty string. This parameter is applicable only to NGINX websites. Example: 1
ServiceType	yes	no	String	Service Type Example: web
UpdateTime	yes	yes	String	Data update time. Example: 2011-11-11 12:12:12
User	yes	no	String	Run user. Example: root

NetAttackTrend

Referenced by the following interfaces: DescribeAttackTrends

name	required	NULL allowed	type	description
AttackCount	no	yes	Uint64	Attacks Example: 1
DateTime	no	yes	String	Time Point, e.g., 2023-05-06 Example: 2023-05-06
SuccAttackCount	no	yes	Uint64	Attack Success Count Example: 0
TryAttackCount	no	yes	Uint64	Attack Attempts Example: 1

FullTextInfo

Full-text index-related configuration.

Referenced by the following interfaces: DescribeLogIndex

name	required	NULL allowed	type	description
CaseSensitive	yes	no	Bool	Whether it is case-sensitive. Example: false
ContainZH	yes	no	Bool	Whether to contain zh characters Example: false
Tokenizer	yes	no	String	Tokenizer. Example: \n\t,!;

ScreenTrendsChart

Attack defense trend chart in the dashboard.

Referenced by the following interfaces: DescribeScreenDefenseTrends

name	required	NULL allowed	type	description
Type	yes	no	String	Data category for statistics collection. Valid values: number of attack defense times and number of attacks. Example: Defended attacks
X	yes	no	String	Time in the X axis. Example: 2021-03-30 19:17:28
Y	yes	no	Uint64	Value in the Y axis. Example: 12

AssetFilters

Container security
Describes a key-value pair filter for conditional filtering queries. For example, filter the ID, name, and status.
If there are multiple filters, the relationship between filters is logical AND.
If you specify multiple values for 1 filter, the OR relationship is used between the values.

Referenced by the following interfaces: DescribeAssetAppList, DescribeAssetCoreModuleList, DescribeAssetDatabaseList, DescribeAssetEmvList, DescribeAssetInitServiceList, DescribeAssetJarList, DescribeAssetPlanTaskList, DescribeAssetWebServiceInfoList, DescribeLoginWhiteHostList, DescribeMachineList, DescribeProtectDirList, DescribeWebPageEventList, ExportAssetAppList, ExportAssetCoreModuleList, ExportAssetDatabaseList, ExportAssetEmvList, ExportAssetInitServiceList, ExportAssetJarList, ExportAssetPlanTaskList, ExportAssetWebServiceInfoList, ExportProtectDirList, ExportWebPageEventList

name	required	NULL allowed	type	description
ExactMatch	no	no	Bool	Whether to fuzzy query. Example: true
Name	yes	no	String	Name of the filter key. Example: Ip
Values	yes	no	Array of String	One or more filter values. Example: ["192.168.0.1"]

AssetInitServiceBaseInfo

List of initialization services in the asset management module.

Referenced by the following interfaces: DescribeAssetInitServiceList

name	required	NULL allowed	type	description
FirstTime	no	no	String	First collection time. Example: 2022-07-15 11:27:01
IsAutoRun	no	yes	Int64	Start at boot [0: No
IsNew	no	no	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	no	no	String	Server IP. Example: 192.168.0.1
MachineName	no	no	String	Server name. Example: redis_node_cvm
MachineWanIp	no	no	String	Public IP address of a server. Example: 43.156.40.46
Name	no	no	String	Name. Example: bootlocal
OsInfo	no	no	String	Operating system. Example: 1
Path	no	no	String	Path Example: 1
Quuid	no	no	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Status	no	no	Uint64	Default enabling status. 0: not enabled. 1: enabled. Example: 1
Type	no	no	Uint64	The attribute type. Valid values: 1: encoder 2: IE plug-in 3: network provider 4: Image File Execution Options 5: LSA provider 6:KnownDLLs 7: boot execution 8:WMI 9: scheduled task 10: Winsock provider 11: print monitor 12: resource manager 13: drive service 14: logon Example: 1
UpdateTime	no	no	String	Data update time. Example: 2011-11-11 12:12:12
User	no	no	String	User who triggers initialization. Example: root
Uuid	no	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

AssetCoreModuleBaseInfo

List of kernel modules in the asset management module.

Referenced by the following interfaces: DescribeAssetCoreModuleList

name	required	NULL allowed	type	description
Desc	no	no	String	Description. Example: system
FirstTime	no	no	String	First collection time. Example: 2022-07-15 11:27:01
Id	no	no	String	Module ID. Example: 10001
IsNew	no	no	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	no	no	String	Server IP. Example: 1.1.1.1
MachineName	no	no	String	Server name. Example: any-ins
MachineWanIp	no	no	String	Public IP address of a server. Example: 1.1.1.1
ModuleCount	no	no	Uint64	Number of dependent modules. Example: 0
Name	no	no	String	Name. Example: core.package
OsInfo	no	no	String	Operating system. Example: centos-64bit
Path	no	no	String	Path Example: /root
ProcessCount	no	no	Uint64	Number of dependent processes. Example: 0
Quuid	no	no	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Size	no	no	Uint64	Module size. Example: 10001
UpdateTime	no	yes	String	Data update time. Example: 2011-11-11 12:12:12
Uuid	no	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Version	no	no	String	Version. Example: 1.0.0.1

BaselineDetail

Baseline details.

Referenced by the following interfaces: DescribeBaselineDetail

name	required	NULL allowed	type	description
Description	yes	yes	String	Baseline description. Example: Using weak passwords for MySQL can make it easier for hackers to guess and obtain access to data privileges, leading to data theft and deletion. Moreover, hackers may further obtain system permissions based on database access.
Level	yes	yes	Uint64	Risk severity. Example: 3
Name	yes	yes	String	Baseline name. Example: Weak password
PackageName	yes	yes	String	Package name. Example: 21.dat
ParentId	yes	yes	Uint64	Parent ID. Example: 1

FieldValueRatioInfo

Quick analysis statistics.

Referenced by the following interfaces: DescribeFastAnalysis

name	required	NULL allowed	type	description
Count	yes	no	Int64	Count. Example: 0
Ratio	yes	no	Float	Proportion. Example: 0.5
Value	yes	no	String	Value. Example: value

MaConnPodInfo

Referenced by the following interfaces: DescribeMaConnEventList

name	required	NULL allowed	type	description
ClusterId	no	yes	String	Cluster ID of the pod. Example: cls-dl8qwyay
Namespace	no	yes	String	Namespace of the pod. Example: tcss
PodName	no	yes	String	Pod Name Example: redis-job-sdfa-9885-sd23

HostTagInfo

Server information and server tag information.

Referenced by the following interfaces: DescribeHostInfo

name	required	NULL allowed	type	description
AliasName	no	yes	String	Server name. Example: redis_node_cvm
CloudTags	no	yes	Array of Tags	Cloud tag information. Example:View
HostIp	no	yes	String	Private IP address of the server. Example: 1.2.3.4
InstanceID	no	yes	String	Host Instance ID Example: ins-dada
KernelVersion	no	yes	String	Kernel version. Example: 5.1.0
MachineStatus	no	yes	String	Connection status of the server. Valid values: ONLINE and OFFLINE. Example: ONLINE
MachineWanIp	no	yes	String	Public IP address of the server. Example: 10.0.0.1
ProtectType	no	yes	String	Protection edition. BASIC_VERSION: Basic Edition. PRO_VERSION: Professional Edition. Flagship: Ultimate Edition. Example: BASIC_VERSION

name	required	NULL allowed	type	description
Quuid	no	yes	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
TagList	no	yes	Array of String	Keys of the tags attached to the server. Example: ["dev"]
Uuid	no	yes	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
VulNum	no	yes	Int64	Number of vulnerabilities. Example: 32

Tag

Tag information

Referenced by the following interfaces: DescribeRansomDefenseMachineList, DescribeRansomDefenseStrategyMachines, DescribeTags

name	required	NULL allowed	type	description
Count	yes	no	Uint64	Number of servers. Example: 100
Id	yes	no	Uint64	Tag ID. Example: 1
Name	yes	no	String	Tag name. Example: business1

BashEventNew

High-risk command data (new).

Referenced by the following interfaces: DescribeBashEventsNew

name	required	NULL allowed	type	description
BashCmd	no	no	String	Command to run. Example: rm
CreateTime	no	no	String	Event time. Example: 2021-03-30 19:17:28
DetectBy	no	yes	Uint64	0: bash command. 1: real-time monitoring (Thunder Edition) Example: 1
Exe	no	yes	String	Process name. Example: 1.exe
HostIp	no	no	String	Private IP address of the server. Example: 127.0.0.1
Id	no	no	Uint64	Data ID. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Additional Information on Machine Example:View
MachineName	no	no	String	Server name. Example: redis_node_cvm
MachineType	no	yes	Int64	0: Basic Edition. 1: Professional Edition. 2: Ultimate Edition. Example: 1
ModifyTime	no	yes	String	Handling time. Example: 2021-03-30 19:17:28
Pid	no	yes	String	Process ID. Example: 1
Platform	no	no	Uint64	Platform type. Example: 1
Quuid	no	no	String	Server ID. Example: dadasda
RegexBashCmd	no	yes	String	Escaped regular expression. Example: rm -rf /tmp/t*
RuleCategory	no	yes	Uint64	Rule type. 0: system rule. 1: custom rule. Example: 0
RuleId	no	no	Uint64	Rule ID. Example: 1
RuleLevel	no	no	Uint64	Rule severity. 1: high. 2: medium. 3: low. Example: 1
RuleName	no	no	String	Rule Name Example: 1
Status	no	no	Uint64	Handling status. 0: to be handled. 1: handled. 2: added to the allowlist. 3: ignored. Example: 1
User	no	no	String	User who performs execution. Example: root
Uuid	no	no	String	CWP ID. Example: 5a540076-d38a-4078-aa98-q45rt37d322

AssetWebFrameBaseInfo

Web application information in the asset management module.

Referenced by the following interfaces: DescribeAssetWebFrameList

name	required	NULL allowed	type	description
FirstTime	no	no	String	First collection time. Example: 2022-07-15 11:27:01
IsNew	no	no	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
Lang	no	no	String	Language. Example: eng
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	no	no	String	Private IP address of the server. Example: 1.1.1.1.
MachineName	no	no	String	Server name. Example: redis_node_cvm
MachineWanIp	no	no	String	Public IP address of the server. Example: 1.1.1.1
Name	no	no	String	Web application name. Example: Nginx
OsInfo	no	no	String	OS information. Example: Centos 64Bit
Path	no	yes	String	Application Path Example: /root
ProjectId	no	no	Uint64	ID of the project to which the server belongs. Example: 1
Quuid	no	no	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
ServiceType	no	no	String	Service Type Example: tcp
Tag	no	yes	Array of MachineTag	Server tags. Example:View
UpdateTime	no	yes	String	Data update time. Example: 2011-11-11 12:12:12
Uuid	no	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Version	no	no	String	Version. Example: 1.0.1

VulOverview

Vulnerability overview.

Referenced by the following interfaces: DescribeVulOverview

name	required	NULL allowed	type	description
TodayCount	yes	no	Int64	New count on the current day. Example: 0
TotalCount	yes	no	Uint64	Total number. Example: 12

BaselineHostTopList

Information about a server affected by a baseline.

Referenced by the following interfaces: DescribeBaselineHostTop

name	required	NULL allowed	type	description
EventLevelList	yes	yes	Array of BaselineEventLevelInfo	Event severity and quantity. Example:View
HostName	yes	yes	String	Server name. Example: v_xxnxxhayay
Quuid	yes	yes	String	Host QUUID. Example: fcf856c9-f45e-457a-bca4-fcae074eayay
Score	yes	yes	Uint64	Score used to calculate the weight. Example: 20

ScreenInvasion

Intrusion event details in the dashboard.

Referenced by the following interfaces: DescribeScreenHostInvasion

name	required	NULL allowed	type	description
Content	yes	no	String	Event data in the JSON format, which varies based on event types. For file scanning and cleaning, the data includes VirusName, FileName, FilePath, FileSize, MD5, CreateTime, LatestScanTime, HarmDescribe, and SuggestScheme. For logins from unusual locations, the data includes SrcIp, Location, UserName, and LoginTime. For password cracking, the data includes SrcIp, City, Country, Protocol, UserName, Port, Count, CreateTime, and ModifyTime. For malicious requests, the data includes Url, ProcessName, ProcessMd5, Pid, AccessCount, MergeTime, HarmDescribe, and SuggestScheme. For high-risk commands, the data includes RuleName, RuleCategory, BashCmd, DetectBy, User, Pid, CreateTime, HarmDescribe, and SuggestScheme. For local privilege escalation, the data includes UserName, ParentProcName, ParentProcGroup, CreateTime, HarmDescribe, and SuggestScheme. For reverse shells, the data includes ProcessName, CmdLine, ParentProcName, DstIp, DstPort, CreateTime, HarmDescribe, and SuggestScheme. Example: {"Id":"20244402329413 6,"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	yes	no	String	Intrusion time. Example: 2021-03-30 19:17:28
EventType	yes	no	Uint64	Event type. 0: file scanning and cleaning. 1: login from an unusual location. 2: password cracking. 3: malicious request. 4: high-command risk. 5: local privilege escalation. 6: reverse shell. Example: 1
Id	yes	no	Uint64	Event ID. Example: 1
Level	yes	no	Uint64	Uniform event severity. 0: informational. 1: low-risk. 2: medium-risk. 3: high-risk. 4: critical. Example: 1
LevelZh	yes	no	String	Level name Example: High-risk
Uuid	yes	no	String	Host UUID. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0

VulDefencePluginStatus

Information about a server exploit prevention plug-in.

Referenced by the following interfaces: DescribeVulDefencePluginStatus

name	required	NULL allowed	type	description

name	required	NULL allowed	type	description
Alias	yes	no	String	Host alias. Example: redis_node_cvm
CreateTime	yes	no	String	Creation time. Example: 2021-01-20 16:17:11
Exception	yes	no	Int64	Plug-in status. 0: normal. 1: abnormal. Example: 1
ModifyTime	yes	no	String	Last update time. Example: 2021-01-20 16:17:11
PrivateIp	yes	no	String	Private IP address. Example: 10.1.1.2
PublicIp	yes	no	String	Public IP address. Example: 112.2.3.2.1
Quuid	yes	no	String	QUUID of the server. Example: d92d723e-4aac-4f4a-bbf9-e5430e29d289

AssetUserKeyInfo

Account key details in the asset management module.

Referenced by the following interfaces: DescribeAssetUserInfo, DescribeAssetUserKeyList

name	required	NULL allowed	type	description
Comment	yes	no	String	Description of the public key. Example: comment
EncryptType	yes	no	String	Encryption method. Example: aes
Value	yes	no	String	Value of the public key. Example: value1

MaGlobalConf

Referenced by the following interfaces: DescribeMaGlobalConf, ModifyMaGlobalConf

name	required	NULL allowed	type	description
MonitorEnabled	yes	yes	Int64	Monitoring enabling status. 1: enabled; 0: disabled. Example: 1
MonitorIpRanges	no	yes	Array of String	Monitoring IP range. Example: ["192.168.0.1"]
MonitorLabelIds	no	yes	Array of Int64	Monitoring tag. Example: [1]
MonitorScope	yes	yes	Int64	Monitoring scope [0: All; 1: Partial]. Example: 0
MonitorWorkloadIds	no	yes	Array of Int64	Excluded workload ID list. Example: [1]
NewEnabled	no	yes	Int64	Whether the new asset is automatically protected [1: Yes; 0: No]. Example: 1
NewEndTime	no	yes	Datetime_iso	End time of self-learning. Example: 2020-02-01 12:00:00
NewIpRanges	no	yes	Array of String	Added asset protection IP range. Example: ["192.168.0.1"]
NewLabelIds	no	yes	Array of Int64	Added asset protection IP range. Example: [1]
NewLearnCycle	no	yes	Int64	Number of self-learning days for new asset. Example: 3
NewScope	no	yes	Int64	Added protection scope [0: All; 1: Selective]. Example: 1
NewStartTime	no	yes	Datetime_iso	Start time of self-learning. Example: 2020-02-01 12:00:00

VulStoreListInfo

Referenced by the following interfaces: DescribeHotVulTop, DescribeVulStoreList

name	required	NULL allowed	type	description
AttackLevel	no	yes	Uint64	Attack level. If the value is 3 or higher, the attack is a notable attack. Example: 1
CveId	no	yes	String	CVE ID. Example: CVE-2021-44487
FixSwitch	no	yes	Uint64	Whether vulnerabilities can be automatically fixed. 0 - disabled for Windows and Linux; 1 - enabled for Windows and Linux; 2 - for Linux only; 3 - for Windows only. Example: 1
Level	no	yes	Uint64	Vulnerability severity. 1: low. 2: medium. 3: high. 4: critical. Example: 1
Method	no	yes	Uint64	Vulnerability Detection Method: 0 - Version Comparison, 1 - POC Verification Example: 0
Name	no	yes	String	Vulnerability name. Example: Apache HTTP/2 DoS vulnerability (CVE-2023-44487)
PublishDate	no	yes	String	Release time. Example: 2012-10-10 07:55:00
SupportDefense	no	yes	Uint64	Whether vulnerabilities support defense. 0: No 1: Yes Example: 1
VulCategory	no	yes	Uint64	1: Web-CMS vulnerability. 2: application vulnerability. 4: Linux software vulnerability. 5: Windows system vulnerability. 0: emergency vulnerability. Example: 1
VulId	no	yes	Uint64	Vulnerability ID. Example: 1

WarningInfoObj

Alarm settings.

Referenced by the following interfaces: DescribeWarningList

name	required	NULL allowed	type	description
BeginTime	yes	no	String	Start time. Format: HH:mm Example: 00:00
ControlBit	yes	no	Uint64	Control bit of the vulnerability severity, which corresponds to the decimal storage of databases. Example: 0
ControlBits	yes	no	String	Binary control bit of the vulnerability severity. Each bit corresponds to the enabling status of each vulnerability severity: low, medium, and high (0: disabled. 1: enabled); For example, a value of 101 indicates that both the low and high severities are selected. Example: 0
Count	yes	yes	Int64	Configured Number of Hosts in the Range of Alarm, used by the frontend to decide when to display prompt information. Example: 0
DisablePhoneWarning	yes	no	Uint64	1: disables alarming. 0: enables alarming. Example: 1
EndTime	yes	no	String	End time. Format: HH:mm Example: 00:00
HostRange	no	yes	Int64	Alarm host range type: 0: all hosts; 1: by project; 2: by cloud tag; 3: by CWP tag; 4: custom hosts. Example: 0
OfflineInterval	yes	yes	Int64	Time duration used to determine a disconnection event. Unit: seconds. Example: 1412524532
TimeZone	yes	no	String	Timezone information. Example: Europe/London
Type	yes	no	Uint64	Event alarm type. 1: disconnection. 2: trojan. 3: login from an unusual location. 4: brute force attack. 5: vulnerability (further divided into four types: 9 to 12). 6: high-risk command. 7: reverse shell. 8: local privilege escalation. 9: application vulnerability. 10: Web-CMS vulnerability. 11: emergency vulnerability. 12: security baseline vulnerability. 13: tampering attack. 14: malicious request. 15: cyberattack. 16: Windows system vulnerability. 17: Linux software vulnerability. 18: core file monitoring and alarming. 19: agent uninstallation. 20: agent disconnection. Example: 1

LicenseExtraParam

Additional parameters for authorization.

Referenced by the following interfaces: DescribeLicenseList

name	required	NULL allowed	type	description
IsUnBind	no	yes	Bool	Whether unbinding/rebinding is allowed. Example: false
UnionBuyDetail	no	yes	Array of UnionProtectDetail	Joint purchase information of containers and hosts. Example:View

AssetMachineDetail

Basic server information in the asset fingerprint module.

Referenced by the following interfaces: DescribeAssetMachineDetail

name	required	NULL allowed	type	description
AgentVersion	no	no	String	Agent version. Example: 1.2.3.1
BootTime	no	no	String	System boot time. Example: 2021-12-21
BuyTime	no	no	String	Time when CWP Pro was activated. Example: 2021-12-21
CoreVersion	no	no	String	Kernel version. Example: 3.10.0-1160.99.1.el7.x86_64
Cpu	no	no	String	CPU information. Example: Intel(R) Xeon(R) Platinum 8255C CPU @ 192.168.0.204
CpuLoad	no	no	String	CPU load. Example: Medium
CpuLoadVul	no	yes	String	CpuLoadVul Example: 10.1
CpuSize	no	no	Uint64	Number of CPU cores. Example: 2
DeviceVersion	no	no	String	Device model. Example: CVM
DiskLoad	no	no	String	Disk usage in percentage. Example: 11
DiskSize	no	no	Uint64	Disk capacity. Unit: GB. Example: 11
Disks	no	no	Array of AssetDiskPartitionInfo	Partition. Example:View
EndTime	no	no	String	Time when CWP Pro expires. Example: 2021-12-21
FirstTime	no	yes	String	Time. Example: 2021-02-01 12:00:00
InstallTime	no	no	String	Installation time. Example: 2021-12-21
InstanceId	no	yes	String	Server ID. Example: cvm-112234
LastLiveTime	no	no	String	Last connection time. Example: 2021-12-21
MachineExtraInfo	no	yes	MachineExtraInfo	Host information Example:View
MachineIp	no	no	String	Server private IP address. Example: 11.22.33.44
MachineName	no	no	String	Server name. Example: tsbj-k8s-main- 192.168.0.204

name	required	NULL allowed	type	description
MachineWanIp	no	no	String	Public IP address of the server. Example: 1.2.3.4
MemLoad	no	no	String	Memory utilization in percentage. Example: 11
MemSize	no	no	Uint64	Memory capacity. Unit: GB. Example: 11
NetCards	no	no	Array of AssetNetworkCardInfo	ENI. Example:View
OfflineTime	no	yes	String	Disconnection time. Example: 2021-12-21
OsInfo	no	no	String	OS name. Example: centos
OsType	no	no	String	Linux/Windows Example: Linux
PartitionCount	no	no	Uint64	Number of partitions Example: 1
Producer	no	no	String	Vendor name. Example: Cloud Cayay
ProjectId	no	no	Uint64	Project ID. Example: 1241252
ProtectDays	no	no	Uint64	Number of days for which the asset is under protection. Example: 11
ProtectLevel	no	no	Uint64	Protection Level. 0 Basic Edition; 1 Professional Edition; 2 Premium Edition; 3 General Discount Edition Example: 1
Quuid	no	no	String	QUUID of the server. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
RiskStatus	no	no	String	Risk status. UNKNOW: unknown status. RISK: at risk. SAFT: secure. Example: RISK
SerialNumber	no	no	String	The serial number. Example: 641eb296-411e-45b5-8003-903d4f4aayay
Status	no	no	Uint64	0: online. 1: offline. Example: 1
UpdateTime	no	yes	String	Data update time. Example: 2011-11-11 12:12:12
Uuid	no	no	String	UUID of the server. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

VulFixStatusInfo

Vulnerability fixing details.

Referenced by the following interfaces: DescribeVulFixStatus

name	required	NULL allowed	type	description
FailCnt	yes	yes	Uint64	Number of servers on which the vulnerability failed to be fixed. Example: 1
FixMethod	no	yes	Uint64	Repair method. 0: Update components or install patches. 1: Disable service. Example: 0
FixSuccessCnt	yes	yes	Uint64	Number of servers on which the vulnerability is fixed. Example: 0
HostList	yes	yes	Array of VulFixStatusHostInfo	Fixing status of the vulnerability on servers. Example:View
Progress	yes	no	Uint64	Fixing progress of the vulnerability. Valid values: 1 to 100. Example: 80
VulId	yes	yes	Uint64	Vulnerability ID. Example: 12
VulName	yes	yes	String	Vulnerability name. Example: Apache HTTP/2 DoS vulnerability (CVE-2023-44487)

Machine

Server list

Referenced by the following interfaces: DescribeMachineList, DescribeMachines

name	required	NULL allowed	type	description
BaselineNum	no	no	Int64	Number of baseline risks. Example: 2
CloudFrom	no	yes	Int64	Cloud server vendor type. 0: cloud 1: IDC 2: Alibaba Cloud 3: Huawei Cloud 4: Amazon 5: Microsoft 6: Google 7: Oracle 8: DigitalOcean Example: 0
CloudTags	no	yes	Array of Tags	Cloud tag information. Example:View
CyberAttackNum	no	no	Int64	Number of network risks. Example: 2
HasAssetScan	no	no	Uint64	Whether there is an asset scan API. 0: no. 1: yes. Example: 1
InstanceId	no	no	String	Instance ID. Example: ins-sad143
InstanceState	no	no	String	Instance status. PENDING: creating; LAUNCH_FAILED: creation failed; RUNNING: running; STOPPED: shut down; STARTING: starting; STOPPING: shutting down; REBOOTING: restarting; SHUTDOWN: shut down and pending termination; TERMINATING: terminating; TERMINATED: terminated; TERMINATED_PRO_VERSION: terminated but Yunjing Pro Edition not expired. Example: TERMINATED_PRO_VERSION
InvasionNum	no	no	Int64	Number of intrusion events. Example: 1
IpList	no	yes	String	Host IP List Example: 1.1.1.1,2.2.2.2
IsAddedOnTheFifteen	no	yes	Uint64	Whether it is a server that is added within the last 15 days. 0: no. 1: yes. Example: 1
IsProVersion	no	no	Bool	Whether it is a professional version. • true: yes. • false: no. Example: false
KernelVersion	no	no	String	Kernel version. Example: 3.10.0-1127.19.1.el7.x86_64
LicenseStatus	no	no	Uint64	License status of anti-tampering. 1: licensed. 0: not licensed. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	no	no	String	IP address of the server. Example: 10.0.0.2
MachineName	no	no	String	Host name. Example: stone
MachineOs	no	no	String	Operating system of the server. Example: centos
MachineStatus	no	no	String	Host status. • OFFLINE: offline. • ONLINE: online. • SHUTDOWN: shutdown. • UNINSTALLED: not protected. Example: ONLINE
MachineType	no	no	String	Zone type of the server. CVM: CVM zone. BM: BM zone. ECM: ECM zone. LH: Lighthouse zone. Other: hybrid cloud zone. Example: CVM
MachineWanIp	no	no	String	Public IP of the host. Example: 114.11.12.13
MalwareNum	no	no	Int64	Number of trojans. Example: 1
PayMode	no	no	String	Host status. • POSTPAY: postpaid mode, that is, pay-as-you-go. • PREPAY: prepaid mode, that is, monthly subscription. Example: PREPAY
Platform	no	yes	String	Platform Example: platform
ProjectId	no	no	Int64	Project ID. Example: 1
ProtectType	no	no	String	Protection edition. BASIC_VERSION: Basic Edition. PRO_VERSION: Professional Edition. Flagship: Ultimate Edition. GENERAL_DISCOUNT: General Edition. Example: BASIC_VERSION
Quuid	no	no	String	UUID of the CVM or BM instance. Example: 8c09e1b1-5611-45b3-9c02-737996013b81
RegionInfo	no	no	RegionInfo	Region information. Example:View
Remark	yes	yes	String	Remarks. Example: redis cvm
SecurityStatus	no	no	String	Risk status. • SAFE: safe. • RISK: risky. • UNKNOWN: unknown. Example: RISK
Tag	no	no	Array of MachineTag	Tag information Example:View
Uuid	no	no	String	CWP UUID. If the CWP client is offline for a long time, an empty character is returned. Example: 8c09e1b1-5611-45b3-9c02-737996013b81
VpcId	no	yes	String	Network Example: vpc-sda
VulNum	no	no	Int64	Number of vulnerabilities. Example: 2

VulDefenceOverview

Exploit prevention trend information, including the plug-in status and the attack defense trend. The trend is stored as three arrays with the same length and whose elements are in one-to-one correspondence.

Referenced by the following interfaces: DescribeVulDefenceOverview

name	required	NULL allowed	type	description
AttackCounts	yes	yes	Array of Int64	Daily attack trend. Example: [0,0,20,0,0,0,0,17,11,2,33,49,105,80]
Date	yes	yes	Array of String	Date Example: ["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	yes	yes	Array of Int64	Daily defense trend. Example: [0,0,20,0,0,0,0,17,11,2,33,49,105,80]
DefendHostCount	yes	no	Int64	Number of servers on which exploit prevention is enabled. Example: 12
Enable	yes	no	Int64	Status of the exploit prevention feature. 0: disabled. 1: enabled. Example: 1
ExceptionCount	yes	no	Int64	Number of abnormal plug-ins. Example: 2

ScreenMachine

Server list

Referenced by the following interfaces: DescribeScreenMachines

name	required	NULL allowed	type	description
BaselineNum	no	no	Int64	Number of baseline risks. Example: 2
CoreVersion	no	no	String	Kernel version. Example: 3.10.0-1127.19.1.el7.x86_64
CpuLoad	no	no	String	CPU load status. Example: Low
CpuSize	no	no	Float	Number of CPU cores. Example: 1
CyberAttackNum	no	no	Int64	Number of network risks. Example: 2
DiskLoad	no	no	String	Disk utilization in percentage. Example: 10.60
DiskSize	no	no	Float	Disk capacity. Unit: GB. Example: 40
InvasionNum	no	no	Int64	Number of intrusion events. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	no	no	String	IP address of the server. Example: 10.0.0.2
MachineName	no	no	String	Host name. Example: redis_node_cvm
MachineOs	no	no	String	Operating system of the server. Example: centos
MachineStatus	no	no	Uint64	Server status in the dashboard. 0: no agent is installed. 1: the server is offline. 2: the server is offline (at risk). 3: the server is offline (critical). 4: the agent is correctly installed and the server runs normally. 5: the agent is correctly installed, the server runs normally, and CWP Pro or CWP Ultimate is activated. 6: the agent is correctly installed, and risks are detected on the server (number of cyberattack events > 0). 7: the agent is correctly installed, risks are detected on the server (number of cyberattack events > 0), and CWP Pro or CWP Ultimate is activated. 8: the agent is correctly installed, and critical events are detected on the server (number of intrusion detection events > 0). 9: the agent is correctly installed, critical events are detected on the server (number of intrusion detection events > 0), and CWP Pro or CWP Ultimate is activated. Example: 1
MachineType	no	no	String	Zone type of the server. CVM: CVM zone. BM: BM zone. ECM: ECM zone. LH: Lighthouse zone. Other: hybrid cloud zone. Example: CVM
MachineWanIp	no	no	String	Public IP of the host. Example: 114.11.12.13
MemLoad	no	no	String	Memory load rate in percentage. Example: 18.66
MemSize	no	no	Float	Memory capacity. Unit: GB. Example: 2
Quuid	no	no	String	UUID of the CVM or BM instance. Example: df99a1b46-cc2d-4633-a11f-4a7663d2523e
SecurityStatus	no	no	String	Risk status. • SAFE: safe. • RISK: risky. • UNKNOWN: unknown. Example: RISK
Uuid	no	no	String	CWP UUID. If the CWP client is offline for a long time, an empty character is returned. Example: df99a1b46-cc2d-4633-a11f-4a7663d2523e
VulNum	no	no	Int64	Number of vulnerabilities. Example: 2

AssetCoreModuleDetail

Kernel module details in the asset management module.

Referenced by the following interfaces: DescribeAssetCoreModuleInfo

name	required	NULL allowed	type	description
Desc	yes	no	String	Description. Example: module
Modules	yes	no	String	Dependent-on modules. Example: module
Name	yes	no	String	Name. Example: test
Params	yes	yes	Array of AssetCoreModuleParam	Parameter information. Example:View
Path	yes	no	String	Path Example: /root
Processes	yes	no	String	Dependent processes. Example: 10011
Size	yes	no	Uint64	Size. Example: 102
UpdateTime	yes	yes	String	Data update time. Example: 2011-11-11 12:12:12
Version	yes	no	String	Version. Example: 1.0.1

BaselineRuleTopInfo

Top baseline check item information.

Referenced by the following interfaces: DescribeBaselineTop

name	required	NULL allowed	type	description
EventCount	yes	yes	Uint64	Number of events. Example: 0
Level	yes	yes	Uint64	Baseline risk level. 0: low; 1: medium; 2: high; 3: critical. Example: 1
RuleId	yes	yes	Uint64	ID of the check item. Example: 20
RuleName	yes	yes	String	Name of the baseline check item. Example: Weak password

AssetInfo

Instance information

Referenced by the following interfaces: CreateAgentInstallTask, DescribeAgentInstallResult, ModifyAssetsProtectionStatus

name	required	NULL allowed	type	description
AppId	no	yes	Uint64	App ID information Example: 3680000000
AssetId	no	yes	String	Asset ID Example: ins-36843684
AssetType	no	yes	String	Asset type Example: CVM
MemberId	no	yes	String	memberid Example: mem-36843684
Region	no	yes	String	Availability zone. Example: ap-region1

BaselineRiskItem

Top 5 baseline check items.

Referenced by the following interfaces: DescribeBaselineItemRiskTop

name	required	NULL allowed	type	description
HostCount	yes	no	Int64	Number of affected servers. Example: 1
ItemId	yes	yes	Int64	ID of the check item. Example: 1
ItemName	yes	no	String	Name of the check item. Example: Weak password
Level	yes	no	Int64	Baseline risk level. 0: low; 1: medium; 2: high; 3: critical. Example: 1

JavaMemShellPluginInfo

Java memory trojan plug-in information.

Referenced by the following interfaces: DescribeJavaMemShellPluginInfo

name	required	NULL allowed	type	description
ErrorLog	yes	no	String	Error log. Example: 1736132722
MainClass	yes	no	String	Main class of the injection process. Example: main.class
Pid	yes	no	Uint64	ID of the injection process. Example: 12
Status	yes	no	Uint64	Injection status. 0: injecting. 1: injected successfully. 2: plug-in timeout. 3: plug-in exit. 4: injection failed. 5: logically deleted. Example: 1

MaWorkload

Referenced by the following interfaces: DescribeMaWorkloadList

name	required	NULL allowed	type	description
HostIp	no	yes	String	Private network IP of the server/pod. Example: 10.0.0.0.1
Id	no	yes	Int64	ID Example: 1
IsSupportMa	no	yes	Int64	Whether to support micro-alarms (1: Yes; 0: No). Example: 0
Labels	no	yes	Array of MaLabel	Tag. Example:View
Name	no	yes	String	Server/Pod name. Example: redis_node_cvm
NotSupportMaCode	no	yes	Int64	Reason for not supporting micro-alarms (0: Supported; 1: Low client version; 2: Not premium edition; 3: Client not installed). Example: 0
PublicIp	no	yes	String	Public IP of the server. Example: 35.168.0.1
Type	no	yes	Int64	Type (0: Server; 1: Pod). Example: 0

BaselineRuleDetect

Baseline rule-based check.

Referenced by the following interfaces: DescribeBaselineRuleDetectList

name	required	NULL allowed	type	description
DetectStatus	yes	no	Int64	0: checked not passed. 1: ignored. 3: check passed. 5: checking. Example: 0
FirstTime	yes	no	String	First scan time. Example: 2021-02-01 12:00:00
HostCount	yes	no	Int64	Number of associated servers. Example: 9

name	required	NULL allowed	type	description
ItemCount	yes	no	Int64	Number of associated items. Example: 32
ItemIds	yes	yes	Array of Int64	Item IDs. Example: [3855]
LastTime	yes	no	String	string Example: 2021-02-01 12:00:00
RuleDesc	yes	no	String	Rule description. Example: International standard—CentOS 6 security baseline check
RuleId	yes	no	Int64	Rule ID. Example: 30
RuleName	yes	no	String	Rule Name Example: International standard—CentOS 6 security baseline check

MalWareList

List of trojans.

Referenced by the following interfaces: DescribeMalWareList

name	required	NULL allowed	type	description
Alias	no	no	String	Host alias. Example: redis_node_cvm
CheckPlatform	no	no	String	Trojan detection platforms. Multiple platforms are separated with commas (,). 1: cloud scanning and cleaning engine. 2: TAV. 3: binaryAI. 4: suspicious behavior. 5: threat intelligence. Example: 1
CreateTime	no	no	String	Creation time. Example: 2024-10-30 09:12:22
FileCreateTime	no	yes	String	Time when the file was first run. Example: 2024-10-30 09:12:22
FileExists	no	no	Uint64	Whether the trojan file exists. 0: the trojan file does not exist. 1: the trojan file exists. Example: 1
FileModifierTime	no	yes	String	Last execution time. Example: 2024-10-30 09:12:22
FilePath	no	no	String	Path Example: /tmp/any
HostIp	no	no	String	Server IP address. Example: 10.0.0.1
Id	no	yes	Uint64	Unique ID. Example: 1
LatestScanTime	no	no	String	Last scan time. Example: 2024-10-30 09:12:22
Level	no	no	Uint64	Risk severity. 0: informational. 1: low. 2: medium. 3: high. 4: critical. Example: 1
MD5	no	no	String	MD5 value of the sample trojan. Example: 708cae4c1814c3de6e4208da228fad4e
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
ProcessExists	no	no	Uint64	Whether the trojan process exists. 0: the trojan process does not exist. 1: the trojan process exists. Example: 1
Quuid	no	no	String	cvm quuid Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
Status	no	no	Uint64	Status. 4 - pending processing; 5 - trusted; 6 - isolated; 8 - files deleted; 14 - processed; 13 - allowlisted. Example: 4
Tags	no	yes	Array of String	Tags. This parameter has been deprecated, and no tags will be returned. Tag information will be returned only in the details. Example: ["tag1"]
Uuid	no	no	String	Unique UUID. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
VirusName	no	no	String	Virus name. Example: Linux.Trojan.Downloader.Snkd

SecurityDynamic

Security event message data.

Referenced by the following interfaces: DescribeSecurityDynamics

name	required	NULL allowed	type	description
EventTime	yes	no	Datetime	Time when the security event occurred. Example: 2018-01-01 00:00:00
EventType	yes	no	String	Type of the security event. • MALWARE: trojan event • NON_LOCAL_LOGIN: login from an unusual location. • BRUTEATTACK_SUCCESS: successful password cracking event • VUL: vulnerability • BASELINE: security baseline vulnerability Example: BASELINE
Message	yes	no	String	Message sent for the security event. Example: Event message
SecurityLevel	yes	no	String	Security Event Level. • RISK: Critical • HIGH: High Risk • NORMAL: Moderate Risk • LOW: Low Risk • UNKNOWNED: Suspicious. Example: High
Uuid	yes	no	String	CWP client UUID. Example: 5a540076-d38a-4078-aa98-q45rt371d322

UsualPlace

Usual login location

Referenced by the following interfaces: DescribeUsualLoginPlaces

name	required	NULL allowed	type	description
CityId	yes	no	Uint64	City ID. Example: 101
CountryId	yes	no	Uint64	Country ID. Example: 2
Id	yes	no	Uint64	ID. Example: 13267
ProvinceId	yes	no	Uint64	Province ID. Example: 21
Uuid	yes	no	String	CWP client UUID. Example: 69E78F7F-FFC7-47D1-B406-13C9852ayayay

AssetAppProcessInfo

Information about a process associated with a software application.

Referenced by the following interfaces: DescribeAssetAppProcessList, DescribeAssetJarInfo, DescribeAssetWebServiceProcessList

name	required	NULL allowed	type	description
Name	yes	no	String	Name. Example: sshd
Path	yes	no	String	Path. Example: /usr/bin/sshd
StartTime	yes	no	String	Start time. Example: 2024-10-23 14:17:00
Status	yes	no	String	Process status. R: executable; S: interruptible; D: uninterruptible; T: paused or traced; Z: zombie; X: to be terminated. Example: R
User	yes	no	String	User. Example: root
Version	yes	no	String	Process version. Example: 1.1.1

Filter

Key-value pair filters for conditional filtering queries. For example, IDs, names, and states can be filtered.

If multiple filters exist, the AND relationship is used between the filters.
If you specify multiple values for 1 filter, the OR relationship is used between the values.

- You can specify a maximum of 5 filters.
- You can specify a maximum of 5 values for each filter.

Referenced by the following interfaces: 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, DescribeCkLogsets, DescribeComponentStatistics, DescribeComponents, DescribeEventList, DescribeExportMachines, DescribeHistoryAccounts, DescribeHostLoginList, DescribeIgnoreHostAndItemConfig, DescribeLicenseBindSchedule, DescribeLoginWhiteCombineList, DescribeLoginWhiteList, DescribeLoginWhiteListNew, DescribeMalConnEventList, DescribeMalCustomPolicyList, DescribeMalHostList, DescribeMalLabelList, DescribeMalSelfLearnPolicyList, DescribeMalWhitelist, DescribeMalWorkloadList, 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, ExportMalWhitelist, ExportNonlocalLoginPlaces, ExportRiskDnsEventList, ExportRiskDnsPolicyList, ExportRiskProcessEvents, ExportVulDefenceEvent, ExportVulDefenceList, ExportVulDefencePluginEvent, ExportVulEffectHostList, ExportVulList, ModifyBaselinePolicy, ModifyBaselineRule, ModifyBaselineRuleIgnore

name	required	NULL allowed	type	description
ExactMatch	no	no	Bool	Fuzzy search. Example: false
Name	yes	no	String	Name of the filter key. Example: Keywords
Values	yes	no	Array of String	One or more filter values. Example: ["1.1.1.1"]

AssetDatabaseBaseInfo

Database information in the asset management module.

Referenced by the following interfaces: DescribeAssetDatabaseList

name	required	NULL allowed	type	description
BinPath	no	no	String	Binary path. Example: /usr/local/bin
ConfigPath	no	no	String	Path of the configuration file. Example: /etc/sshd
DataPath	no	no	String	The data path. Example: /data
ErrorLogPath	no	no	String	Path of the error log. Example: /var/log
FirstTime	no	no	String	First collection time. Example: 2022-07-15 11:27:01
Id	no	no	String	Database ID. Example: 1
Ip	no	no	String	Binds the IP address. Example: 112.52.67.8
IsNew	no	no	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
LogPath	no	no	String	Path of the log file. Example: /var/log
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	no	no	String	Private IP address of the server. Example: 10.0.0.11

name	required	NULL allowed	type	description
MachineName	no	no	String	Server name. Example: redis_node_cvm
MachineWanIp	no	no	String	Public IP address of the server. Example: 112.45.55.12
Name	no	no	String	Database name. Example: yunding
OsInfo	no	no	String	OS information. Example: Centos 64Bit
Param	no	no	String	Boot parameters. Example: --configsvr --port 27019 --keyFile /etc/mongodb/key --dbpath /data/db --replSet d1j49hlz --wiredTigerCacheSizeGB 0.43 --maxConns 10000 --auth --bind_ip_all
Permission	no	no	String	Running permissions. Example: polkitd
PlugInPath	no	no	String	Path of the plug-in. Example: /data
Port	no	no	String	Listening port. Example: 27019
ProjectId	no	no	Uint64	ID of the project to which the server belongs. Example: 1
Proto	no	no	String	Protocol. Example: tcp
Quuid	no	no	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Tag	no	yes	Array of MachineTag	Server tags. Example:View
UpdateTime	no	yes	String	Data update time. Example: 2011-11-11 12:12:12
User	no	no	String	Run user. Example: root
Uuid	no	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Version	no	no	String	Version. Example: 1.1.1

MachineSimple

Server list

Referenced by the following interfaces: DescribeMachinesSimple

name	required	NULL allowed	type	description
CloudFrom	no	yes	Uint64	Cloud server vendor type. 0: cloud 1: IDC 2: Alibaba Cloud 3: Huawei Cloud 4: Amazon 5: Microsoft 6: Google 7: Oracle 8: DigitalOcean Example: 0
CloudTags	no	yes	Array of Tags	Cloud tag information. Example:View
InstanceId	no	yes	String	Instance ID. Example: ins-ddsdsay
InstanceState	no	no	String	Instance status. PENDING: creating; LAUNCH_FAILED: creation failed; RUNNING: running; STOPPED: shut down; STARTING: starting; STOPPING: shutting down; REBOOTING: restarting; SHUTDOWN: shut down and pending termination; TERMINATING: terminating; TERMINATED: terminated; TERMINATED_PRO_VERSION: terminated but Yunjing Pro Edition not expired. Example: RUNNING
IsProVersion	no	no	Bool	Whether it is a professional version. • true: yes. • false: no. Example: false
KernelVersion	no	no	String	Kernel version. Example: 3.10.0-1127.19.1.el7.x86_64
LicenseOrder	no	yes	LicenseOrder	License order object. Example:View
MachineIp	no	no	String	IP address of the server. Example: 10.0.0.2
MachineName	no	no	String	Host name. Example: redis_node_cvm
MachineOs	no	no	String	Operating system of the server. Example: centos
MachineType	no	no	String	Zone type of the server. CVM: CVM zone. BM: BM zone. ECM: ECM zone. LH: Lighthouse zone. Other: hybrid cloud zone. Example: CVM
MachineWanIp	no	no	String	Public IP of the host. Example: 1.1.1.1
PayMode	no	no	String	Host status. • POSTPAY: postpaid mode, that is, pay-as-you-go. • PREPAY: prepaid mode, that is, monthly subscription. Example: PREPAY
ProjectId	no	no	Int64	Project ID. Example: 1
ProtectType	no	no	String	Protection edition. BASIC_VERSION: Basic Edition. PRO_VERSION: Professional Edition. Flagship: Ultimate Edition. GENERAL_DISCOUNT: General Edition. Example: BASIC_VERSION
Quuid	no	no	String	UUID of the CVM or BM instance. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
RegionInfo	no	no	RegionInfo	Region information. Example:View
Tag	no	no	Array of MachineTag	Tag information Example:View
Uuid	no	no	String	CWP UUID. If the client remains offline for a long time, an empty string will be returned. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

HostRiskLevelCount

Number of risks at different severity levels on a server.

Referenced by the following interfaces: DescribeBaselineHostRiskTop

name	required	NULL allowed	type	description
HighCount	yes	no	Int64	Number of high risks. Example: 1
HostId	yes	no	String	Server ID. Example: 1
HostName	yes	yes	String	Server name. Example: 1
LowCount	yes	no	Int64	Number of low risks. Example: 1
MediumCount	yes	no	Int64	Number of medium risks. Example: 1
SeriousCount	yes	no	Int64	Number of critical risks. Example: 1

OrderRenewConfig

Order renewal parameters.

Referenced by the following interfaces: ModifyOrder

name	required	NULL allowed	type	description
SubProductCode	yes	yes	String	Secondary sub-product, which is the target sub-product for renewal. Example: sp_yunjing_vas
TimeSpan	yes	yes	Uint64	Duration. The minimum value is 1 and the maximum value is 36. Example: 36
TimeUnit	yes	yes	String	Time unit. y: year, m: month. Example: y

VersionWhiteConfig

License version allowlist configuration.

Referenced by the following interfaces: DescribeLicenseWhiteConfig

name	required	NULL allowed	type	description
Deadline	yes	no	Uint64	Number of days before expiration. Example: 7
IsApplyFor	yes	no	Bool	Whether it can be applied for. Example: false
LicenseNum	yes	no	Uint64	Number of licenses. Example: 10
SourceType	yes	no	Uint64	Order type. 0: default billing order; 1: trial order; 2: gift; 3: experience. Example: 0

RuleInfo

Index rule.

Referenced by the following interfaces: DescribeLogIndex

name	required	NULL allowed	type	description
FullText	yes	no	FullTextInfo	Full-text index-related configuration. Example:View
KeyValue	yes	no	KeyValueInfo	Key-value index configuration. Example:View
Tag	yes	no	KeyValueInfo	Metafield index configuration Example:View

ShellPolicyList

Reverse shell list data details.

Referenced by the following interfaces: DescribeShellPolicyList

name	required	NULL allowed	type	description
HostScope	no	yes	Uint64	Host range. [0: a group of QUuids, 1: all Pro edition hosts, 2: Premium edition, 3: all hosts.] Example: 2
IsEnabled	no	yes	Uint64	0: enabled, 1: disabled. Example: 0
PolicyAction	no	yes	Uint64	Action to take. 0: alarm. 1: allow. 2: block and alarm Example: 0
PolicyDesc	no	yes	String	Policy description. Example: any policy desc
PolicyId	no	yes	Uint64	Policy ID. Example: 2001
PolicyName	no	yes	String	Policy name. Example: Automatic blocking policy of the system
PolicyType	no	yes	Uint64	0: system policy, 1: custom policy. Example: 0
UpdateTime	no	yes	String	Update time. Example: 0000-00-00 00:00:00

CKafkaInstanceInfo

CKafka instance information.

Referenced by the following interfaces: DescribeLogDeliveryKafkaOptions

name	required	NULL allowed	type	description
Az	yes	no	String	Region. Example: ap1
Bandwidth	yes	no	Int64	instance bandwidth. Unit: Mbit/s. Example: 0
DiskSize	yes	no	Int64	Disk capacity. Unit: GB. Example: 0
Healthy	yes	no	Int64	Status. 1: healthy. 2: alarming. 3: abnormal. Example: 1
InstanceID	yes	no	String	Instance ID. Example: ins-id
InstanceName	yes	no	String	Instance name. Example: instance_name
KafkaVersion	yes	no	String	Version number. Example: 1.1.0
RouteList	yes	no	Array of CKafkaRouteInfo	List of routes. ExampleView
SubnetId	yes	no	String	Subnet ID. Example: 1.1.1.1
TopicList	yes	yes	Array of CKafkaTopicInfo	List of alarm sources. ExampleView
VpcId	yes	no	String	VPC ID. An empty value indicates that the classic network is used. Example: 1.1.1.1
Zone	yes	no	String	Availability zone. Example: zone1

RecordInfo

Client Exception Information Structure

Referenced by the following interfaces: DescribeClientException

name	required	NULL allowed	type	description
HostIP	yes	no	String	IP address of the server. Example: 10.10.10.10
InstanceID	yes	no	String	Host Instance ID Example: ins-gdsgdsd
OfflineTime	yes	no	String	Client Offline Time Example: 2022-11-14 00:00:00
UninstallCmd	yes	no	String	Client Uninstallation Call Chain Example: sh uninstall.sh
UninstallTime	yes	no	String	Client Uninstallation Time Example: 2022-11-14 00:00:00
Uuid	yes	no	String	Client UUID Example: c0bf7a9e-95cf-4048-a6cc-97e85d02e6ee

TopInfo

Referenced by the following interfaces: DescribeAttackTop

name	required	NULL allowed	type	description
Count	no	yes	Uint64	Top Statistical Count Example: 10
Value	no	yes	String	Top Statistical Data, such as IP, and vulnerability name Example: DstPort

ClsTopicInfo

Log topic information

Referenced by the following interfaces: DescribeClsTopics

name	required	NULL allowed	type	description
AssumerName	no	yes	String	Cloud Product Identifier Example: CWP
CreateTime	no	yes	String	Creation Time Example: 2021-04-01 08:00:00
LogsetId	no	yes	String	Logset ID Example: 14526
TopicId	no	yes	String	Topic ID Example: topic_redis_node
TopicName	no	yes	String	Topic Name Example: topic_redis_node

FullMachine

Server information.

Referenced by the following interfaces: DescribeAllMachines

name	required	NULL allowed	type	description
IsProVersion	yes	no	Bool	Whether CWP Pro is activated. true: yes. false: no. Example: true
MachineIp	yes	no	String	IP address of the server. Example: 192.168.0.1
MachineName	yes	no	String	Host name. Example: redis_node_cvm
MachineWanIp	yes	no	String	Public IP of the host. Example: 35.168.0.1
Quuid	yes	no	String	UUID of the server. Example: 5a540076-d38a-4078-aa98-qwert171d322

MaConnEvent

Referenced by the following interfaces: DescribeMaConnEventList

name	required	NULL allowed	type	description
CreateTime	no	yes	String	First time. Example: 2023-10-10 00:00:00
DestIP	no	yes	String	Target IP address. Example: 1.1.1.1
DestInstanceId	no	yes	String	Target Instance ID Example: ins-tsa23
DestLabels	no	yes	Array of MaLabel	Tag of the target workload. The length may be 0, indicating that no tags are matched. ExampleView
DestPodInfo	no	yes	MaConnPodInfo	Basic information of the pod as the target. ExampleView
DestPort	no	yes	Uint64	Target port. Example: 8080
DestUuid	no	yes	String	UUID of the server as the target. Example: 5a540076-d38a-4078-aa98-q45rt171d322
DestWorkloadDeleted	no	yes	Uint64	Whether the target workload is deleted. • 0: Not deleted • 1: Deleted Example: 1
DestWorkloadId	no	yes	Uint64	ID of the target workload, which may be 0, indicating that no workloads are matched. Example: 1
DestWorkloadName	no	yes	String	Name of the target workload, which may be an empty string, indicating that no workloads are matched. Example: redis_node_cvm
DestWorkloadType	no	yes	Int64	Type of the target workload. • 0: IP • 1: Server • 2: Pod Example: 1
Id	no	yes	Uint64	Event ID. Example: 1
MatchCount	no	yes	Uint64	Number of matches. Example: 100
MatchPolicyId	no	yes	Uint64	ID of the matched policy under custom policies. Example: 1
MatchPolicyName	no	yes	String	Name of the matched policy. Example: policy1
MatchPolicyType	no	yes	Uint64	Type of the matched policy. • 0: Self-learning policy • 1: Custom allowlist policy Example: 1
MatchPolicyUniqueId	no	yes	String	Unique key of the matched policy under self-learning policies. Example: 2514
ModifyTime	no	yes	String	Last occurrence time. Example: 2023-10-10 00:00:00
PolicyDeleted	no	yes	Uint64	Whether the matched policy is deleted. • 0: Not deleted • 1: Deleted Example: 1
Protocol	no	yes	String	Protocol: • TCP • UDP Example: TCP
ServiceName	no	yes	String	Service name, used for extension and not supported currently. Example: sshd
SrcIP	no	yes	String	Source IP Example: 1.1.1.1
SrcInstanceId	no	yes	String	Source instance ID Example: instance1
SrcLabels	no	yes	Array of MaLabel	Tag of the source workload. The length may be 0, indicating that no tags are matched. ExampleView
SrcPodInfo	no	yes	MaConnPodInfo	Basic information of the pod as the source. ExampleView
SrcUuid	no	yes	String	UUID of the server as the source. Example: 5a540076-d38a-4078-aa98-q45rt171d322
SrcWorkloadDeleted	no	yes	Uint64	Whether the source workload is deleted. • 0: Not deleted. • 1: Deleted. Example: 1
SrcWorkloadId	no	yes	Uint64	ID of the source workload, which may be 0, indicating that no workloads are matched. Example: 1
SrcWorkloadName	no	yes	String	Name of the source workload, which may be an empty string, indicating that no workloads are matched. Example: 192.168.0.10

name	required	NULL allowed	type	description
SrcWorkloadType	no	yes	Int64	Type of the source workload. • 0: IP • 1: Server • 2: Pod Example: 0
Type	no	yes	Uint64	Event type. • 0: Normal access • 1: Exception access Example: 0

FileTamperRuleDetail

Details of a core file monitoring rule.

Referenced by the following interfaces: DescribeFileTamperEventRuleInfo, DescribeFileTamperRuleInfo

name	required	NULL allowed	type	description
AddWhiteType	no	yes	String	Allowlisting type. • cur: Add only the current item to an allowlist. • all: Add all items that meet conditions to an allowlist. Example: cur
CreateTime	yes	no	String	Creation time. Example: 2021-10-13T11:15:06+08:00
Id	yes	no	Uint64	Rule ID. Example: 1
IsGlobal	yes	no	Uint64	Whether it is a global rule. 0: no. 1: yes. Default value: 0. Example: 1
Level	yes	no	Uint64	Risk severity. 0: no risk. 1: high. 2: medium. 3: low. Example: 1
ModifyTime	yes	no	String	Update time. Example: 2021-10-13T11:15:06+08:00
Name	yes	yes	String	Rule Name Example: Deny Access
Rule	yes	no	Array of FileTamperRule	Rule. Example:View
Status	yes	no	Uint64	Status. 0: enabled. 1: disabled. Example: 1
UuidTotalCount	yes	no	Uint64	Total number of servers on which the rule takes effect. Example: 17
Uuids	yes	yes	Array of String	UUIDs of the servers on which the rule takes effect. If this parameter is left empty, this rule takes effect on all servers. You can use this parameter to limit the number of entries to return. Example: ["935e27b1-d675-4509-80bf-96fbf0764237"]

MemShellRule

Java Webshell allowlist rule.

Referenced by the following interfaces: DescribeMemShellRules

name	required	NULL allowed	type	description
AnnotationsRegexp	no	yes	String	Annotation regular expression, which is not matched if empty. Example: org.apache.catalina.startup.Bootstrap
CallStackRegexp	no	yes	String	Call stack regular expression, which is not matched if empty. Example: eval
ClassNameRegexp	no	yes	String	Class name regular expression, which is not matched if empty. Example: webshell_filter
CodeSourceRegexp	no	yes	String	Source code regular expression, which is not matched if empty. Example: eval
CreateTime	no	yes	String	Creation time. Example: 2024-09-20 15:32:26
FileExist	no	yes	Uint64	Whether a file exists. 0: Default value when a user does not select a rule. 1: File exists; 2: File does not exist. Example: 0
GroupID	no	yes	String	Batch ID. Example: ece9dcb3-e427-4ded-ac6f-727cce7913bb
GroupName	no	yes	String	Policy name. Example: check_for_redis
HandleHistory	no	yes	Uint64	Whether to process historical events. 0: no, 1: yes. Example: 1
Id	no	yes	Uint64	Rule ID. Example: 12
InterfacesRegexp	no	yes	String	Inherited interface regular expression, which is not matched if empty. Example: org.apache.catalina.startup.Bootstrap
IsGlobal	no	yes	Uint64	Whether it is a global rule. (Whether it is effective for all hosts under appid. 0: single UUID. 1: global. The default value is no.) Example: 0
LoaderClassNameRegexp	no	yes	String	Associated class loader regular expression, which is not matched if empty. Example: org.apache.catalina.startup.Bootstrap
LogicalSymbol	no	yes	Uint64	Logical operator. 0: 5 valid regular expression logical ANDs; 1: logical OR. Example: 0
MachinesNums	no	yes	String	Number of servers covered by a rule. When IsGlobal is set to 1, all servers are displayed. Example: 2
ModifyTime	no	yes	String	Modification time. Example: 2024-11-03 15:09:33
Operator	no	yes	String	Operator. Example: Alice
Status	no	yes	Uint64	Status (0: valid, 1: deleted, 2: invalid (enabling switch off)). Example: 0
SuperClassNameRegexp	no	yes	String	Parent class name regular expression, which is not matched if empty. Example: org.apache.catalina.startup.Bootstrap
UuidHostips	no	yes	Array of UuidHostip	Client ID Example:View

MonthInspectionReport

Monthly inspection report provided by the expert service.

Referenced by the following interfaces: DescribeMonthInspectionReport

name	required	NULL allowed	type	description
ModifyTime	yes	no	String	Time when the inspection report was updated. Example: 2021-03-11 09:50:33
ReportName	yes	no	String	Name of the inspection report. Example: report-2021-03.pdf
ReportPath	yes	no	String	Download URL of the inspection report. Example: https://www.domain.xxm/report-2021-03.pdf

RiskDnsPolicy

Anti-malicious request policy.

Referenced by the following interfaces: DescribeRiskDnsPolicyList, ModifyRiskDnsPolicy

name	required	NULL allowed	type	description
Domains	yes	no	Array of String	Domain name. The value must be Base64 encoded when the parameter is used as an input parameter. Example: [domainName1,domainName2]
EventId	no	no	Int64	Event ID. Example: 1
HostIds	yes	no	Array of String	Server ID. Example: [a7c573cb-c228-4211-85e3-64e000f159a5]
HostScope	yes	no	Int64	Server range. 1: all servers with CWP Pro and all servers with CWP Ultimate. 2: all servers with CWP ultimate. 0: some servers. Example: 1
IsDealOldEvent	no	no	Int64	Whether to handle previous events. 0: previous events will not be handled. 1: previous events will be handled. Example: 1
IsEnabled	yes	no	Int64	Specifies whether to take effect. 0: yes. 1: no. Example: 1
PolicyAction	yes	no	Int64	Action to take. 0: alarm. 1: allow. 2: block and alarm Example: 1
PolicyDesc	no	no	String	Policy description. Example: add for nginx web cvm
PolicyId	no	no	Int64	Policy ID. Example: 1
PolicyName	yes	no	String	Policy name. Example: for_nginx_web
PolicyType	yes	no	Int64	Policy type. 0: system policy. 1: custom policy. Example: 1
UpdateTime	no	no	String	Update time. Example: 2022-07-15 11:27:01

EmergencyVul

Emergency vulnerability information.

Referenced by the following interfaces: DescribeEmergencyVulList

name	required	NULL allowed	type	description
AttackLevel	no	yes	Uint64	Attack level. If the value is 3 or higher, the attack is a notable attack. Example: 3
Category	yes	no	Uint64	Vulnerability category. 1: web CMS vulnerability; 2: application vulnerability; 4: Linux software vulnerability; 5: Windows system vulnerability. Example: 2
CveId	yes	yes	String	CVE ID. Example: CVE-2021-3156
CvssScore	yes	yes	Float	CVSS score. Example: 7.4
DefenseAttackCount	yes	yes	Uint64	Number of prevented attack attempts. Example: 12
DefenseState	no	yes	Bool	Whether vulnerable hosts are enabled with vulnerability defense. Example: true
HostCount	yes	yes	Uint64	Number of affected servers. Example: 2
IsSupportDefense	yes	yes	Uint64	Whether to support attack defense. 0: not supported. 1: supported. Example: 1
Labels	yes	yes	String	Tags of the vulnerability, which are separated with commas (,). Example: tag1,tag2
LastScanTime	yes	no	String	Last scan time. Example: 2024-11-04 09:57:28
Level	yes	no	Uint64	Vulnerability risk level. 0: prompt; 1: low; 2: medium; 3: high; 4: critical. Example: 2
Method	no	yes	Uint64	Detection rule. 0: version comparison, 1: POC verification. Example: 0
Progress	yes	no	Uint64	Scan progress. Example: 100
PublishDate	yes	no	String	Publishing date. Example: 2024-09-04
Status	yes	no	Uint64	Vulnerability status. 0: not detected; 1: risk detected; 2: no risk; 3: detecting (Progress field displayed). Example: 1
VulId	yes	no	Uint64	Vulnerability ID. Example: 1001

name	required	NULL allowed	type	description
VulName	yes	no	String	Vulnerability name. Example: Apache HTTP/2 DoS vulnerability (CVE-2023-44487)

BaselineEffectHost

Information about a server affected by a baseline.

Referenced by the following interfaces: DescribeBaselineEffectHostList

name	required	NULL allowed	type	description
AliasName	yes	yes	String	Host alias. Example: redis_node_cvm
FailCount	yes	yes	Uint64	Risk items. Example: 1
FirstScanTime	yes	yes	String	First scan time. Example: 2021-10-27 00:09:38
HostIp	yes	yes	String	IP address of the server. Example: 10.0.0.1
LastScanTime	yes	yes	String	Last detection time. Example: 2021-10-27 00:09:38
MaxStatus	yes	yes	Uint64	Status during scanning. Example: 0
PassCount	yes	yes	Uint64	Check items that the server passed. Example: 1
Quuid	yes	yes	String	Host QUUID. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
Status	yes	yes	Uint64	Handling status of the risk item. 0: not passed. 1: passed. Example: 0
Uuid	yes	yes	String	Host UUID. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0

HistoryAccount

Account change history data.

Referenced by the following interfaces: DescribeHistoryAccounts

name	required	NULL allowed	type	description
Id	yes	no	Uint64	Unique ID. Example: 1
MachineIp	yes	no	String	Private IP address of the server. Example: 1.2.3.4
MachineName	yes	no	String	Server name. Example: stone
ModifyTime	yes	no	Datetime	Point in time when the change took place. Example: 2020-01-01 01:01:01
ModifyType	yes	no	String	Account change type. • CREATE: create an account. • MODIFY: modify an account. • DELETE: delete an account. Example: CREATE
Username	yes	no	String	Account name. Example: user1
Uuid	yes	no	String	CWP client UUID. Example: 8c89e1b1-5611-45b3-9c02-737996011b81

IgnoreBaselineRule

Information about an ignored baseline check item.

Referenced by the following interfaces: DescribeIgnoreBaselineRule

name	required	NULL allowed	type	description
EffectHostCount	yes	yes	Uint64	Number of affected servers. Example: 10
Fix	yes	yes	String	Fix suggestions. Example: 1. Use a more complex password. A strong password should be a combination of letters, numbers, and special characters and should be at least 10 characters long;\n2. Use the CDB.\n3. To delete an account directly, execute the OPTIMIZE TABLE mysql.user; command.
ModifyTime	yes	yes	String	Update time. Example: 2021-02-01 12:00:00
RuleId	yes	yes	Uint64	ID of the baseline check item. Example: 1103
RuleName	yes	yes	String	Name of the baseline check item. Example: Redis baseline compliance check

BaselineCategory

Baseline rule category or baseline check item category.

Referenced by the following interfaces: DescribeBaselineItemInfo, DescribeBaselineRuleCategoryList

name	required	NULL allowed	type	description
CategoryId	yes	no	Int64	Category ID. Example: 1
CategoryName	yes	no	String	Category name. Example: Weak password
ItemCount	no	yes	Uint64	Total number of detection items under a subcategory. Example: 100
ParentCategoryId	yes	no	Int64	ID of the parent category. A value of 0 indicates that no parent category exists. Example: 1

ValueInfo

Description of an index value.

Referenced by the following interfaces: DescribeLogIndex

name	required	NULL allowed	type	description
ContainZH	yes	no	Bool	Whether to contain zh characters Example: false
SqlFlag	yes	no	Bool	Whether the analysis feature is enabled for the field. Example: false
Tokenizer	yes	no	String	Field tokenizer. Example: \n\t\r
Type	yes	no	String	Supported types: long, text, and double. Example: text

Item

Item details.

Referenced by the following interfaces: DescribeBaselineRuleIgnoreList, DescribeBaselineRuleList, ModifyBaselineRule

name	required	NULL allowed	type	description
CategoryId	no	yes	Int64	Category of a detection item. Example: 50
CustomItemValues	no	yes	Array of Uint64	Custom threshold. Example: [1000]
ItemId	yes	no	Int64	Id Example: 100
ItemName	no	no	String	Name. Example: itemname

BruteAttackInfo

Brute force attack information.

Referenced by the following interfaces: DescribeBruteAttackList

name	required	NULL allowed	type	description
AttackStatusDesc	no	yes	String	Cracking status description. Example: fail
BanExpiredTime	no	yes	String	Block expiration time (only valid for blocked events). Example: 2024-10-30 15:58:43
BanStatus	no	yes	Uint64	0 - no blocking (blocking is not supported in the client version). 1 - blocked. 2 - blocking failed (abnormal program). 3 - no blocking (for the private network). 4 - blocking not allowed in availability zones. 10 - blocking in progress. 81 - no blocking (blocking not enabled). 82 - no blocking (non-Pro). 83 - no blocking (added to allowlist). 86 - no blocking (system allowlist). 87 - no blocking (the client is offline). 88 - no blocking (source IP addresses belong to the same customer). 89 - no blocking (IPv6 addresses do not support blocking). Example: 0
City	no	yes	Uint64	City ID. Example: 1
Count	no	yes	Uint64	Number of occurrences. Example: 2
Country	no	yes	Uint64	Country ID. Example: 1
CreateTime	no	yes	String	Creation time. Example: 2021-05-25 12:01:50
DataFrom	no	yes	Int64	Event source. 0: blocking rule, 1: threat intelligence. Example: 0
DataStatus	no	yes	Uint64	0: to be handled. 1: ignored. 5: handled. 6: added to the allowlist. Example: 1
EventType	no	yes	Uint64	Event type: 200 - brute force cracking event; 300 - successful brute force cracking event (the status is displayed on the page); 400 - brute force cracking event for non-existent accounts. Example: 1
Id	no	no	Uint64	Unique ID. Example: 1001
InstanceId	no	yes	String	Instance ID. Example: ins-fs9aw
IsProVersion	no	yes	Bool	Whether Professional Edition is activated. Valid values: true and false. Example: false
Location	no	yes	String	Geographical location name. Example: location1,location2,location3
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	no	yes	String	IP address of the server. Example: 127.0.0.1
MachineName	no	yes	String	Server name. Example: redis_node_cvm
ModifyTime	no	yes	String	Last attack time. Example: 2021-05-25 12:01:50
Port	no	yes	Uint64	Port. Example: 22

name	required	NULL allowed	type	description
Protocol	no	yes	String	Username of the attacked service. Example: ssh/rdp
Province	no	yes	Uint64	Province ID. Example: 1
Quuid	no	yes	String	Server UUID address. Example: 380add75-bb06-4cc4-84c5-cf806d102fba
RiskLevel	no	yes	Uint64	Threat level. 0: low risk, 1: medium risk, 2: high risk. Example: 1
Srcip	no	yes	String	Source IP. Example: 66.12.2.14
Status	no	yes	String	SUCCESS: cracking succeeded. FAILED: cracking failed. Example: FAILED
UserName	no	yes	String	User name. Example: root
Uuid	no	yes	String	CWP client UUID. Example: 380add75-bb06-4cc4-84c5-cf806d102fba

Component

Component list data.

Referenced by the following interfaces: DescribeComponents

name	required	NULL allowed	type	description
ComponentName	no	yes	String	Component name. Example: redis
ComponentType	no	yes	String	Component type. • SYSTEM: system component • WEB: web component. Example: SYSTEM
ComponentVersion	no	yes	String	Version number of the component. Example: 1.0.0.1
Id	no	yes	Uint64	Unique ID. Example: 1
MachineIp	no	yes	String	Private IP address of the server. Example: 192.168.0.1
MachineName	no	yes	String	Server name. Example: redis_cvm
ModifyTime	no	yes	Datetime	Time when the component was modified. Example: 2020-02-01 12:00:00
Uuid	no	yes	String	Unique UUID of the CWP client. Example: 5a540076-d38a-4078-aa98-qwert371d322

ReverseShellRule

Anti-reverse shell rule.

Referenced by the following interfaces: DescribeReverseShellRules

name	required	NULL allowed	type	description
CreateTime	yes	no	String	Creation time. Example: 2024-11-04 09:57:28
DestIp	yes	no	String	Target IP address. Example: 127.0.0.1
DestPort	yes	no	String	Target port. Example: 80
Hostip	yes	no	String	IP address of the server. Example: 192.168.0.204
Id	yes	no	Uint64	Rule ID. Example: 1001
IsGlobal	yes	no	Uint64	Indicates whether it is a global rule. Example: 1
ModifyTime	yes	no	String	Modification time. Example: 2024-11-04 09:57:28
Operator	yes	no	String	Operator. Example: root
ProcessName	yes	no	String	Process name. Example: nginx
Status	yes	no	Uint64	Status. 0: valid. 1: invalid. Example: 0
Uuid	yes	no	String	Client ID. Example: df131b24-8528-4809-9d07-a9e4d58ad566

RiskDnsList

Malicious request list API

Referenced by the following interfaces: DescribeRiskDnsInfo, DescribeRiskDnsList

name	required	NULL allowed	type	description
AccessCount	yes	no	Uint64	Number of access requests. Example: 22
Alias	yes	no	String	Alias. Example: by_nginx
CmdLine	yes	no	String	Command line. Example: cmd
CreateTime	yes	no	String	First access time. Example: 2021-04-26 15:19:04
Description	yes	no	String	Description. Example: desc of this risk
GlobalRuleId	yes	no	Uint64	Whether it is a global rule. 0: no. 1: yes. Example: 22
HostIp	yes	no	String	IP address of the server. Example: 13.22.3.1
Id	yes	no	Uint64	Unique ID. Example: 153
MachineStatus	yes	yes	String	Connection status of the server. Valid values: OFFLINE, ONLINE, and UNKNOWN. Example: OFFLINE
MachineWanIp	yes	yes	String	Public IP. Example: 13.22.3.1
MergeTime	yes	no	String	Last access time. Example: 2021-04-26 15:19:04
Pid	yes	no	Uint64	Process ID. Example: 33
ProcessMd5	yes	no	String	MD5 value of the process. Example: e3bab3f49bbf36bbbe56e057f20f883e
ProcessName	yes	no	String	Process name. Example: nginx
Quuid	yes	no	String	QUUID. Example: 5a540076-d38a-4078-aa98-q45rt371d322
Reference	yes	no	String	Reference. Example: http://www.vxjump.net/files/virus_analysis/virut%20botnet%20anal
Status	yes	no	Uint64	Status. 0: to be handled. 2: added to the allowlist. 3: untrusted. 4: handled. 5: ignored. Example: 0
SuggestScheme	yes	no	String	Suggestion scheme. Example: 1. Check for malicious processes and invalid ports, and delete suspicious startup items and scheduled tasks. 2. Isolate or delete relevant Trojan files.
Tags	yes	no	Array of String	Tags. Example: ["vuair","mle"]
Url	yes	no	String	Domain name for external access. Example: re.r3r.1.org
UserRuleId	yes	no	Uint64	ID of the custom rule. Example: 12
Uuid	yes	no	String	Unique UUID. Example: 5a540076-d38a-4078-aa98-q45rt371d322

ScreenEmergentMsg

API for querying emergency notifications in the dashboard visualization module

Referenced by the following interfaces: DescribeScreenEmergentMsg

name	required	NULL allowed	type	description
Text	yes	no	String	Content of notification. Example: Detected vulnerabilities
Title	yes	no	String	Title of the notification. Example: Notification
Type	yes	no	Uint64	Redirection type. 0: vulnerability management. Example: 0

LicenseDetail

List of license orders.

Referenced by the following interfaces: DescribeLicenseList

name	required	NULL allowed	type	description
Alias	yes	no	String	Alias of the resource. Example: redis_node_cvm
AutoRenewFlag	yes	no	Uint64	0: initialization. 1: auto-renewal is enabled. 2: auto-renewal is not enabled. Example: 0
BuyTime	yes	no	String	Purchase time. Example: 2018-02-28 00:00:00
Deadline	yes	no	String	End date. Example: 2018-02-28 00:00:00
ExtraParam	no	yes	LicenseExtraParam	Additional Parameters Example:View
FreezeNum	no	yes	Int64	Number of frozen licenses. 0: unfrozen, values other than 0: number of frozen licenses. Example: 0
LicenseCnt	yes	no	Uint64	Total number of licenses. Example: 0
LicenseId	yes	no	Uint64	License ID. Example: 1
LicenseStatus	yes	yes	Uint64	License status. 0: not used. 1: partially used. 2: used up. 3: unavailable. Example: 0
LicenseType	yes	no	Uint64	License type. 0: Pro Edition license; 5: Ultimate Edition license. Example: 0
OrderStatus	yes	no	Uint64	Order status. 1: normal. 2: isolated. 3: terminated. Example: 1
ProjectId	yes	no	Uint64	Project ID. Example: 1
ResourceId	yes	no	String	Resource ID of the order. Example: 1c007adc2f0bbf9f7c052860e2d37034a
SourceType	yes	no	Uint64	Order type. 0: default billing order; 1: trial order; 2: gift; 3: experience. Example: 0

name	required	NULL allowed	type	description
Tags	yes	yes	Array of Tags	Platform tags. Example:View
TaskId	yes	no	Uint64	Task ID, which is used to query the binding progress. Default value: 0. Example: 1
UsedLicenseCnt	yes	no	Uint64	Number of used licenses. Example: 0

ProtectMachine

License expiration information of a server.

Referenced by the following interfaces: DescribeWebPageServiceInfo

name	required	NULL allowed	type	description
HostIp	yes	no	String	Server IP address. Example: 10.0.1.92
HostName	yes	no	String	The instance name Example: host1
SafeguardDirNum	yes	no	Uint64	Number of protected directories. Example: 0

AssetChangeInfo

Instance modification information.

Referenced by the following interfaces: DescribeChangingAssetInfo

name	required	NULL allowed	type	description
AppId	no	yes	Uint64	App ID information Example: 1255080011
AssetId	no	yes	String	Asset ID Example: ins-36843684
Status	no	yes	Int64	Modification status. 0: installing, 1: uninstalling, 2: enabling protection. Example: 0

VulEffectModuleInfo

Details of a component affected by vulnerabilities.

Referenced by the following interfaces: DescribeVulEffectModules

name	required	NULL allowed	type	description
FixCmd	yes	no	String	Fixing command. Example: sudo yum update openssl
Name	yes	no	String	Component Name Example: net-wsion
Path	yes	no	String	Component path. Example: /root/
Quuids	yes	no	Array of String	QUUID of the affected server. Example: ["e5b4724c-49af-46ab-bd84-cdbae897e7e0"]
Rule	yes	no	String	Version of the affected component. Example: npt version less than 2.0.0
Uuids	yes	no	Array of String	UUID of the affected server. Example: ["e5b4724c-49af-46ab-bd84-cdbae897e7e0"]
Version	yes	no	String	Component version. Example: 1.1.1

BaselineInfo

Baseline information.

Referenced by the following interfaces: DescribeBaselineList

name	required	NULL allowed	type	description
BaselineFailCount	yes	yes	Uint64	Number of baseline risk items. Example: 0
CategoryId	yes	yes	Uint64	Baseline ID. Example: 1
HostCount	yes	yes	Uint64	Number of affected servers. Example: 0
LastScanTime	yes	yes	String	Last detection time. Example: 2020-11-21 15:16:00
Level	yes	yes	Uint64	Risk severity. 1: low. 1: medium. 3: high. 4: critical. Example: 1
MaxStatus	yes	yes	Uint64	Status during scanning: 5 Example: 5
Name	yes	yes	String	Baseline name. Example: Redis baseline compliance check
RuleCount	yes	yes	Uint64	Number of check items. Example: 0
Status	yes	yes	Uint64	Whether the check is passed. 0: not passed. 1: passed. Example: 1

VulDefenceSetting

Vulnerability defense settings

Referenced by the following interfaces: DescribeVulDefenceSettingList

name	required	NULL allowed	type	description
AppId	no	yes	Uint64	User's App ID Example: 1255080011
DefenceType	no	yes	Uint64	Protection type. 0: vulnerability defense. 1: attack detection. Example: 0
Enable	no	yes	Uint64	0: disabled, 1: enabled. Example: 0
InstanceNum	no	yes	Uint64	Number of custom hosts. Example: 10
MemberId	no	yes	String	User's member ID. Example: qq
Nickname	no	yes	String	User's Nickname Example: Alice
Scope	no	yes	Uint64	1: all Premium edition hosts. 0: custom hosts. Example: 1
StrategyAction	no	yes	Uint64	Policy action. 0: alarm. 1: defense. Example: 0
StrategyId	no	yes	String	Policy ID. Example: any data
StrategyName	no	yes	String	Policy name. Example: defence_redis_cvm
StrategyType	no	yes	Uint64	0: system policy. 1: custom policy. Example: 0
SupportVulNum	no	yes	Uint64	Number of supported vulnerabilities. Example: 180
ThreatLevel	no	yes	Uint64	Threat level. Example: 1
Uin	no	yes	String	User UIN Example: 101223435

RiskProcessEvent

Abnormal Process Event

Referenced by the following interfaces: DescribeRiskProcessEvents

name	required	NULL allowed	type	description
CheckPlatform	no	no	Array of String	Trojan detection platform [1: Cloud search engine
CmdLine	no	no	String	Command to run. Example: /usr/sbin/sshd
DetectTime	no	no	String	Last detection time. Example: 2022-09-23 15:11:46
EventId	no	no	Int64	Event ID. Example: 1
FilePath	no	no	String	File path. Example: /var/www/fscan
HandleStatus	no	no	Int64	Processing Status [0 Pending; 1 Processed; 2 Scanning; 3 Scanned; 4 Exited; 5 Ignore] Example: 1
HostIp	no	no	String	IP address of the server. Example: 10.0.0.1
HostName	no	no	String	Server name. Example: redis_node_cvm
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
OnlineStatus	no	no	Int64	Host Online Status Example: 1
ProcessId	no	no	Int64	Process ID. Example: 1
ReferenceLink	no	no	String	Reference link. Example: https://cloud.domain.com/document/product/296/9604
StartTime	no	no	String	Process start time Example: 2022-09-23 15:11:46
SuggestSolution	no	no	String	Suggestion scheme. Example: 1. Check for malicious processes and invalid ports, and delete suspicious startup items and scheduled tasks. 2. Isolate or delete relevant Trojan files.
ThreatDesc	no	no	String	Threat description. Example: It is detected that a proxy tool process exists on your host. If it is not started by you, your host may have been compromised.
Uuid	no	no	String	Host UUID. Example: e05a66ec-8d54-4041-80a8-07e9ab79ayay
VirusName	no	no	String	Virus name. Example: Linux.Risk.Miner
VirusTags	no	no	Array of String	Tag Example: ["Miner","HackTool"]
WanIp	no	no	String	Public IP address. Example: 10.0.0.1

MachineSnapshotInfo

Snapshot information of a server.

Referenced by the following interfaces: DescribeMachineSnapshot

name	required	NULL allowed	type	description

name	required	NULL allowed	type	description
CreateTime	yes	no	String	Time when the snapshot was created. Example: 2021-03-11 18:15:17
DiskId	yes	no	String	Disk ID. Example: adhakdh
HostIp	yes	no	String	IP address of the server. Example: 145.12.3.12
HostName	yes	no	String	Server name. Example: redis_node_cvm
InstanceId	yes	no	String	Instance ID. Example: ins-xjd734
QuuId	yes	no	String	cvm id Example: 5a540076-d38a-4078-aa98-q45rt371d322
RegionId	yes	no	Uint64	Region ID. Example: 1
SnapshotId	yes	no	String	Snapshot ID. Example: ajdajd
SnapshotName	yes	no	String	Name of the snapshot. Example: backup-2021-03-01

BillingDefineParams

Custom Parameters of Billing and Ordering

Referenced by the following interfaces: CreateLicenseOrder

name	required	NULL allowed	type	description
AutoBindSwitch	no	no	Bool	Auto-Binding Switch Example: false
AutoRepurchaseRenewSwitch	no	no	Bool	Is auto-renewal required for auto-purchase orders? Example: false
AutoRepurchaseSwitch	no	no	Bool	Auto-purchase Switch Example: false
ProtectType	no	no	String	CWPP edition Example: "PRO_VERSION"

ScreenBaselineInfo

Baseline information in the dashboard.

Referenced by the following interfaces: DescribeScreenHostInvasion

name	required	NULL allowed	type	description
BaselineFailCount	yes	yes	Uint64	Number of baseline risk items. Example: 23
CategoryId	yes	yes	Uint64	Baseline ID. Example: 12
LastScanTime	yes	yes	String	Last detection time. Example: 2021-03-30 19:17:28
Level	yes	yes	Uint64	Risk severity. 1: low. 1: medium. 3: high. 4: critical. Example: 1
Name	yes	yes	String	Baseline name. Example: International
Uuid	yes	yes	String	Host UUID. Example: 1c26308c-5403-4eaf-a817-112ec25f4f9e

MalwareRiskOverview

File Scan Overview Information

Referenced by the following interfaces: DescribeMalwareRiskOverview

name	required	NULL allowed	type	description
FileCount	yes	no	Int64	Number of Malicious Files Example: 1
HostCount	yes	no	Int64	Number of affected servers. Example: 1
IsFirstScan	yes	no	Bool	Is it the first Scan.False: No
ProcessCount	yes	no	Int64	Exceptional Process Count Example: 1
ScanTime	yes	no	String	Last scan time. Example: 2022-09-23 15:11:46

ProcessStatistics

Process statistics.

Referenced by the following interfaces: DescribeProcessStatistics

name	required	NULL allowed	type	description
MachineNum	yes	no	Uint64	Number of servers. Example: 0
ProcessName	yes	no	String	Process name. Example: nginx

BaselineWeakPassword

Baseline weak password.

Referenced by the following interfaces: DescribeBaselineWeakPasswordList, ModifyBaselineWeakPassword

name	required	NULL allowed	type	description
CreateTime	no	no	String	Creation time. Example: 2006-01-02 15:04:05
ModifyTime	no	no	String	Modification time. Example: 2006-01-02 15:04:05
PasswordId	yes	no	Int64	Password ID. Example: 1002
WeakPassword	yes	no	String	Password. Example: passwd-01

EmergencyResponseInfo

Emergency response information in the expert service module.

Referenced by the following interfaces: DescribeEmergencyResponseList

name	required	NULL allowed	type	description
EndTime	yes	no	String	Time when the service ends. Example: 2021-02-01 17:12:28
HostNum	yes	no	Uint64	Number of hosts. Example: 12
ReportPath	yes	no	String	Download URL of the report. Example: http://anydomainc.com/anypath/1.pdf
StartTime	yes	no	String	Time when the service starts. Example: 2021-02-01 17:12:28
Status	yes	no	Uint64	Service status. 0: not started. 1: responding. 2: response completed. Example: 0
TaskId	yes	no	String	Task ID. Example: cve2021-4451451

AccountStatistics

Account statistics.

Referenced by the following interfaces: DescribeAccountStatistics

name	required	NULL allowed	type	description
MachineNum	yes	no	Uint64	Number of servers. Example: 100
Username	yes	no	String	Username. Example: root

PrivilegeEscalationProcess

Local privilege escalation data.

Referenced by the following interfaces: DescribePrivilegeEvents

name	required	NULL allowed	type	description
CmdLine	no	no	String	Command to run. Example: /a
CreateTime	no	no	String	Event time. Example: 2024-10-30 02:19:08
FullPath	no	no	String	Process path. Example: /tmp/any
Hostip	no	no	String	Private IP address of the server. Example: 10.0.0.1
Id	no	no	Uint64	Data ID. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineName	no	no	String	The host name. Example: 2024-10-30 02:19:08
ParentProcGroup	no	no	String	User group of the parent process. Example: root
ParentProcName	no	no	String	Parent process name. Example: bash
ParentProcPath	no	no	String	Path of the parent process. Example: /bin/bash
ParentProcUser	no	no	String	Username of the parent process. Example: root
Pid	no	yes	Int64	Process ID. Example: 1
ProcFilePrivilege	no	no	String	Permissions on the process file. Example: rws
ProcTree	no	no	String	Process tree. Example: a(root),bash(ubuntu),sshd(ubuntu),sshd(root),sshd(root),init(root)
ProcessName	no	no	String	Process name. Example: /etc/sshd
Quuid	no	no	String	Server ID. Example: e5b4724c-49af-46ab-bd84-cdbee897e7e0
Status	no	no	Uint64	Handling status. 0: to be handled. 2: added to the allowlist. 3: handled. 4: ignored. Example: 0
UserGroup	no	no	String	User Group Example: root
UserName	no	no	String	User name. Example: root

name	required	NULL allowed	type	description
Uuid	no	no	String	CWP ID. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0

BaselineBasicInfo

Basic baseline information.

Referenced by the following interfaces: DescribeBaselineBasicInfo

name	required	NULL allowed	type	description
BaselineId	yes	yes	Uint64	Baseline ID. Example: 1
Name	yes	yes	String	Baseline name. Example: Weak password
ParentId	yes	yes	Uint64	Parent ID. Example: 0

HostDesc

Server information returned for displaying a login audit allowlist.

Referenced by the following interfaces: DescribeLoginWhiteHostList

name	required	NULL allowed	type	description
MachineIp	yes	no	String	IP address of the server. An empty string is returned for a terminated server. Example: 1.1.1.1
MachineName	yes	no	String	The host name. Example: redis_node_cvm
MachineWanIp	yes	no	String	Public IP address of the server. An empty string is returned for a terminated server. Example: 1.1.1.1
QuuId	yes	no	String	Machine UUID Example: 380add75-bb06-4cc4-84c5-c8806d102fba
Tags	yes	no	Array of MachineTag	Tags. Example:View
Uuid	yes	no	String	UUID of the CWP agent. Example: 380add75-bb06-4cc4-84c5-c8806d102fba

TagMachine

Tagged server information

Referenced by the following interfaces: DescribeTagMachines

name	required	NULL allowed	type	description
Id	yes	no	String	ID Example: 100
MachineIp	yes	no	String	Private IP address of the server. Example: 192.168.0.204
MachineName	yes	no	String	Server name. Example: tcs-dev1
MachineRegion	yes	no	String	Server region. Example: None
MachineType	yes	no	String	Server type. Example: CVM
MachineWanIp	yes	no	String	Public IP address of the server. Example: 192.168.0.204
QuuId	yes	no	String	Server ID. Example: 0096440e-9a9f-4e80-a82d-0b018637ayay

BashRule

Anti-high-risk command rule.

Referenced by the following interfaces: DescribeBashRules

name	required	NULL allowed	type	description
CreateTime	yes	no	String	Creation time. Example: 2021-03-30 19:17:28
DealOldEvents	yes	yes	Uint64	Whether to handle previous events. 0: does not handle previous events. 1: handles previous events. Example: 0
Decription	yes	no	String	Rule description. Example: 192.168.0.1
Description	no	yes	String	Rule description. Example: desc of rule
Hostip	yes	no	String	IP address of the server. Example: 172.27.16.14
Id	yes	no	Uint64	Rule ID. Example: 10003
IsGlobal	yes	no	Uint64	Indicates whether it is a global rule. Example: 0
Level	yes	no	Uint64	Risk severity 0: no risk. 1: high. 2: medium. 3: low. Example: 1
ModifyTime	yes	no	String	Modification time. Example: 2021-03-30 19:17:28
Name	yes	no	String	Rule Name Example: redis_node_use
Operator	yes	no	String	Operator. Example: admin
Rule	yes	no	String	Regular expression. Example: vim
Status	yes	no	Uint64	Status. 0: valid. 1: invalid. Example: 0
Uuid	yes	no	String	Client ID Example: 451f36cf-ac23-4635-bb96-23cd721b4b25
Uuids	yes	yes	Array of String	UUIDs of the servers on which the rule takes effect. Example: ["451f36cf-ac23-4635-bb96-23cd721b4b25"]
White	yes	yes	Uint64	0: blocklist. 1: allowlist. Example: 1

AssetKeyVal

General data structure in the key-value format.

Referenced by the following interfaces: DescribeAssetAppCount, DescribeAssetDatabaseCount, DescribeAssetHostTotalCount, DescribeAssetMachineTagTop, DescribeAssetPortCount, DescribeAssetProcessCount, DescribeAssetRecentMachineInfo, DescribeAssetTotalCount, DescribeAssetTypeTop, DescribeAssetUserCount, DescribeAssetWebAppCount, DescribeAssetWebFrameCount, DescribeAssetWebLocationCount, DescribeAssetWebServiceCount

name	required	NULL allowed	type	description
Desc	yes	yes	String	Description. Example: none
Key	yes	no	String	Tag. Example: app
NewCount	yes	yes	Int64	New count on the current day. Example: 10
Value	yes	no	Int64	Total number. Example: 21

AssetProcessBaseInfo

Basic resource information in the asset management module.

Referenced by the following interfaces: DescribeAssetProcessInfoList

name	required	NULL allowed	type	description
Desc	no	no	String	Description of the process. Example: user any
FirstTime	no	no	String	First collection time. Example: 2022-07-15 11:27:01
GroupName	no	no	String	Process user group. Example: root
HasSign	no	no	Uint64	Whether there is a digital signature: 0: no; 1: yes; 999: null (Windows only). Example: 1
InstallByPackage	no	no	Uint64	Whether it is installed by using an installation package. 0: no. 1: yes. 999: empty string. This parameter is applicable only to Linux systems. Example: 1
IsNew	no	no	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Host information Example:View
MachineIp	no	no	String	Private IP address of the server. Example: 10.0.0.11
MachineName	no	no	String	Server name. Example: 1
MachineWanIp	no	no	String	Public IP address of the server. Example: 112.42.66.11
Md5	no	no	String	MD5 value of the process. Example: e10adc3949ba59abbe56e057f20f883e
Name	no	no	String	Process name. Example: rsyslogd
OsInfo	no	no	String	OS information. Example: Centos 64bit
PackageName	no	no	String	Software package name. Example: rsyslog
Param	no	no	String	Boot parameters. Example: /usr/sbin/rsyslogd -n
ParentProcessName	no	no	String	Name of the parent process. Example: systemd
Path	no	no	String	Process path. Example: /usr/sbin/rsyslogd
Pid	no	no	String	Process ID. Example: 10021
Ppid	no	no	String	ID of the parent process. Example: 1
ProjectId	no	no	Uint64	ID of the project to which the server belongs. Example: 1
QuuId	no	no	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
StartTime	no	no	String	Start time. Example: 2024-10-23 14:17:00
Status	no	no	String	Process status. R: executable; S: interruptible; D: uninterruptible; T: paused or traced; Z: zombie; X: to be terminated. Example: R
Tag	no	yes	Array of MachineTag	Server tags. Example:View
Tty	no	no	String	Process TTY. Example: ?
UpdateTime	no	yes	String	Data update time. Example: 2011-11-11 12:12:12
User	no	no	String	Run user. Example: root

name	required	NULL allowed	type	description
Uuid	no	no	String	Host UUID. Example: acdd5474-6360-46d4-bfc7-843162cb8116
Version	no	no	String	Process version. Example: 1

VulEffectHostList

API for querying servers affected by vulnerabilities

Referenced by the following interfaces: DescribeVulEffectHostList

name	required	NULL allowed	type	description
AliasName	no	yes	String	Host alias. Example: redis_node_cvm
CloudTags	no	yes	Array of Tags	Cloud tag information. Example:View
Description	no	yes	String	Help. Example: If Redis is started with the root permission and access is not authorized, the arbitrary file write issue occurs, resulting in a command execution vulnerability.
DescriptionEn	no	yes	String	Help. Example: English description.
EventId	no	yes	Uint64	Event ID. Example: 1
FirstDiscoveryTime	no	yes	String	First time when it was found. Example: 2021-03-24 16:37:57
FixStatusMsg	no	yes	String	Cause of failure. Example: Fixing timeout
HostIp	no	yes	String	IP address of the server. Example: 10.12.78.56
HostVersion	no	yes	Uint64	Edition. 0: Basic Edition. 1: Professional Edition. 2: Ultimate Edition. 3: General Edition. Example: 1
InstanceState	no	yes	String	Instance status. "PENDING": the instance is being created. "LAUNCH_FAILED": the instance has failed to be created. "RUNNING": the instance is running. "STOPPED": the instance has stopped. "STARTING": the instance is being started. "STOPPING": the instance is being stopped. "REBOOTING": the instance is rebooting. "SHUTDOWN": the instance is shut down and waiting to be terminated. "TERMINATING": the instance is being terminated. Example: RUNNING
IsSupportAutoFix	no	yes	Uint64	Whether it can be automatically fixed. 0: the vulnerability cannot be automatically fixed. 1: the vulnerability can be automatically fixed. 2: the agent is offline. 3: the server is not associated with a CWP Ultimate license, and the vulnerability can only be manually fixed. 4: automatic vulnerability fixing is not supported for this device model. 5: the vulnerability is being fixed. 6: the vulnerability has been fixed. 7: the vulnerability is being checked. 10: the vulnerability has failed to be Example: 2
LastTime	no	yes	String	Last detection time. Example: 2021-03-24 16:37:57
Level	no	yes	Uint64	Risk severity. 1: low. 1: medium. 3: high. 4: critical. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information Example:View
PublicIpAddresses	no	yes	String	Public IP. Example: 120.12.78.73
Quuid	no	yes	String	Host QUUID. Example: 5a540076-d38a-4078-aa98-a45e371d322
Status	no	yes	Uint64	Status. 0: to be handled. 1: ignored. 3: fixed. 5: checking. 6: fixing. 7: rolling back. 8: fix failed. Example: 0
Tags	no	yes	Array of String	Server tags. Example: ["tag-01"]
Uuid	no	yes	String	Host UUID. Example: 5a540076-d38a-4078-aa98-a45e371d322

ScreenDefendAttackLog

Cyberattack log information in the dashboard.

Referenced by the following interfaces: DescribeScreenHostInvasion

name	required	NULL allowed	type	description
CreatedTime	yes	no	String	Attack time. Example: 2021-01-30 19:17:28
DstIp	yes	no	String	Target IP address. Example: 120.22.1.22
DstPort	yes	no	Uint64	Target port. Example: 2343
HttpMethod	yes	no	String	Attack method. Example: POST
Id	yes	no	Uint64	Log ID. Example: 1
Quuid	yes	no	String	QUUID of the server. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
SrcIp	yes	no	String	Source IP address. Example: 120.22.1.22
SrcPort	yes	no	Uint64	Source port. Example: 546
Uuid	yes	no	String	Client ID Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
VulType	yes	no	String	Threat type. Example: CMD-EXEC

AssetScanTaskHostDetail

Task status on each server in an asset scan task.

Referenced by the following interfaces: DescribeAssetScanTaskDetail

name	required	NULL allowed	type	description
ErrorMessage	yes	no	String	Exception message. Example: some message
MachineIp	yes	no	String	IP address of the server. Example: 192.168.0.1
MachineName	yes	no	String	Server name. Example: redis_node_cvm
Quuid	yes	no	String	Host QUUID. Example: 5a540076-d38a-4078-aa98-qwert371d322
Status	yes	no	Uint64	Task status. 0: in progress. 1: successful. 2: failed. Example: 1

VulHostTopInfo

Top 5 servers at risk.

Referenced by the following interfaces: DescribeVulHostTop

name	required	NULL allowed	type	description
HostName	yes	yes	String	Server name. Example: redis_node_cvm
Quuid	yes	yes	String	Host QUUID. Example: 8e4a1586-c390-4131-ad90-19c1ff64eyaw
Score	yes	yes	Uint64	Top score. Example: 511
VulLevelList	yes	yes	Array of VulLevelCountInfo	Vulnerability severity and the corresponding quantity statistics. Example:View

ZoneInfo

Information on availability zones.

Referenced by the following interfaces: DescribeBanRegions

name	required	NULL allowed	type	description
ZoneName	yes	no	String	AZ name. Example: zone1

MaLabel

Referenced by the following interfaces: DescribeMaConnEventList, DescribeMaCustomPolicyList, DescribeMaHostList, DescribeMaLabel, DescribeMaLabelList, DescribeMaRcdList, DescribeMaSelfLearnPolicyList, DescribeMaWorkloadLabel, DescribeMaWorkloadList, ModifyMaCustomPolicy, ModifyMaLabel

name	required	NULL allowed	type	description
Id	no	yes	Int64	Tag ID. Example: 1
Key	yes	yes	String	Tag key. Example: evn
Source	no	yes	String	Tag source. • learn: self-learning. • custom: custom. • cwp: CWP. • tcloud: cloud. Example: learn
Value	yes	yes	String	Tag value Example: ma
WorkloadCount	no	yes	Int64	Associated workload count. Example: 10

ProductStatusInfo

Data returned from the product beta status query API.

Referenced by the following interfaces: DescribeProductStatus

name	required	NULL allowed	type	description
CanApplyTrial	yes	no	Bool	Whether beta applications can be submitted. true: yes. Example: true
CanNotApplyReason	yes	no	String	Reason why beta applications cannot be summited. An empty string is returned if beta applications can be submitted. Example: Not an enterprise user and not meeting the trial conditions.
FWUserStatus	yes	no	Uint64	Protection status. 1: unprotected. 2: under protection. 3: in beta. 4: expired. Example: 1
LastTrialTime	yes	no	String	End of the last beta use. Example: 2022-06-23 10:25:45

VulTopInfo

Top vulnerabilities.

Referenced by the following interfaces: DescribeVulTop

name	required	NULL allowed	type	description
VulCategory	no	yes	Uint64	1: Web-CMS vulnerability. 2: application vulnerability. 4: Linux software vulnerability. 5: Windows system vulnerability. 0: emergency vulnerability. Example: 2
VulCount	yes	yes	Uint64	Number of vulnerabilities. Example: 82
VulId	yes	yes	Uint64	Vulnerability ID. Example: 104994
VulLevel	yes	yes	Uint64	Risk severity. 1: low. 1: medium. 3: high. 4: critical. Example: 3
VulName	yes	yes	String	Vulnerability name. Example: Apache HTTP/2 DoS vulnerability (CVE-2023-44487)

PrivilegeRule

Anti-local privilege escalation rule.

Referenced by the following interfaces: DescribePrivilegeRules

name	required	NULL allowed	type	description
CreateTime	yes	no	String	Creation time. Example: 2024-11-04 09:57:28
HostIp	yes	no	String	IP address of the server. Example: 192.168.0.204
Id	yes	no	Uint64	Rule ID. Example: 10001
IsGlobal	yes	no	Uint64	Indicates whether it is a global rule. Example: 1
ModifyTime	yes	no	String	Modification time. Example: 2024-11-04 09:57:28
Operator	yes	no	String	Operator. Example: master
ProcessName	yes	no	String	Process name. Example: nginx
SMode	yes	no	Uint64	Whether the process is an S-privilege process. 1: yes; 0: no. Example: 1
Status	yes	no	Uint64	Status. 0: valid. 1: invalid. Example: 0
Uuid	yes	no	String	Client ID Example: df13.1b24-8528-4809-9d07-a9e4d58ad566

Broadcasts

API for querying security notices

Referenced by the following interfaces: DescribeSecurityBroadcasts

name	required	NULL allowed	type	description
CreateTime	yes	no	String	Release time. Example: 2021-03-30 19:17:28
Id	yes	no	Uint64	Unique ID of the notice. Example: 12
Level	yes	no	Uint64	Risk severity. 0: no risk. 1: critical. 2: high. 3: medium. 4: low. Example: 1
Subtitle	yes	no	String	Subtitle of the notice. Example: The new version supports vulnerability fixing.
Title	yes	yes	String	Title of the notice. Example: Vulnerability outbreak
Type	yes	yes	Uint64	Type. 0: emergent notification. 1: feature update. 2: industrial honor. 3: version release. Example: 1

ReverseShellRuleAggregation

Reverse shell rule for the aggregated version.

Referenced by the following interfaces: DescribeReverseShellRulesAggregation

name	required	NULL allowed	type	description
CreateTime	no	yes	String	Creation time. Example: 2020-10-01 00:00:00
DestIp	no	yes	String	Target IP address. Example: 1.2.1.4
DestPort	no	yes	String	Target port. Example: 80
GroupID	no	yes	String	Batch ID. Example: 1
HandleHistory	no	yes	Uint64	Whether to process historical events. 0: no, 1: yes. Example: 0
Id	no	yes	Uint64	Rule ID. Example: 1
IsGlobal	no	yes	Uint64	Indicates whether it is a global rule. Example: 1
MachinesNums	no	yes	String	Number of servers covered by a rule. When IsGlobal is set to 1, all servers are displayed. Example: 12
ModifyTime	no	yes	String	Modification time. Example: 2020-10-01 00:00:00
Operator	no	yes	String	Operator. Example: opt1
ProcessName	no	yes	String	Process name. Example: /etc/sshd
RuleRegexp	no	yes	String	Base64-encoded rule (regular expression). Example: c2pgcmVkaXMuc2g=
Status	no	yes	Uint64	Status. 0: valid. 1: invalid. Example: 0
UuidHostips	no	yes	Array of UuidHostip	Client ID Example:View
WhiteType	no	yes	Uint64	Allowlisting method. 0: regular allowlisting. 1: regular expression allowlisting. Example: 1

VulDefenceEvent

Vulnerability details.

Referenced by the following interfaces: DescribeVulDefenceEvent

name	required	NULL allowed	type	description
Alias	no	no	String	Server name. Example: redis_node_cvm
City	no	no	String	City where the attack source IP address resides. Example: city1
Count	no	no	Int64	Number of occurrences of the event. Example: 1
CreateTime	no	no	String	Time when the event was created. Example: 2021-01-20 16:17:11
CveId	no	no	String	CVE ID. Example: CVE-2014-8500
EventType	no	no	Uint64	0: attempted attack (available for WeDetect). 1: successful attack attempt (available for WeDetect). 2: RASP defense event. Example: 1
FixType	no	no	Int64	0: fixing is not supported. 1: fixing is supported. Example: 1
Id	no	no	Int64	ID of the vulnerability event. Example: 11844
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information Example:View
MergeTime	no	no	String	Time when the event was updated. Example: 2021-01-20 16:17:11
PrivateIp	no	no	String	Private IP address. Example: 10.2.3.1
PublicIp	no	no	String	Public IP address. Example: 111.2.3.1
Quuid	no	no	String	QUUID of the server. Example: d92d723e-4aac-4f4a-bbf8-e5430e29d289
SourceIp	no	no	String	Attack source IP address. Example: 11.2.3.1
SourcePort	no	no	Array of Uint64	Attack source port. Example: [50001,50002]
Status	no	no	Int64	Status. 0: to be handled. 1: prevented. 2: handled. 3: ignored. 4: deleted. Example: 1
UpgradeType	no	no	Int64	0: Professional Edition. 1: Ultimate Edition. 2: Lighthouse General Edition (available only for Lighthouse instances) 3: CVM General Edition (available only for CVM instances). Example: 1
Uuid	no	no	String	Host UUID. Example: d92d723e-4aac-4f4a-bbf8-e5430e29d289
VulId	no	no	Uint64	Vulnerability ID. Example: 14004
VulName	no	no	String	Vulnerability name. Example: Vulnerability

NetAttackWhiteRule

Referenced by the following interfaces: DescribeNetAttackWhiteList

name	required	NULL allowed	type	description
CreateTime	no	yes	String	Creation time. Example: 2024-10-30 02:18:51
DealChildEvents	no	yes	Uint64	Whether to handle previous events. 0: does not handle previous events. 1: handles previous events. Example: 1
Description	no	yes	String	Rule description. Example: add for redis cvm
Id	no	yes	Uint64	Rule ID. Example: 1
ModifyTime	no	yes	String	Modification time. Example: 2024-10-30 02:18:51
Quuids	no	yes	String	Host QUUIDs, separated by semicolons (;). Example: aa71992a-b484-4d9c-882a-4198b6d0a5b0
Scope	no	yes	Uint64	0: A group of Quuid 1: All hosts Example: 1
SrcIP	no	yes	String	Source IP. Single IP: 1.1.1.1, IP Range: 1.1.1.1-1.1.2.1, IP Range: 1.1.1.0/24, separated by semicolons (;) Example: 127.0.0.1

ScreenEventsCnt

Intrusion detection statistics.

Referenced by the following interfaces: DescribeScreenEventsCnt

name	required	NULL allowed	type	description
Category	yes	no	Array of ScreenNameValue	Name: displays the content type, including the attack event, potential risk, compromised asset, and potential asset at risk. Value: counts the number of events. Example:View
Title	yes	no	String	Content displayed, including the total number of pending risks and the total number of affected assets. Example: Total number of risks pending processing
Total	yes	no	Uint64	Number of events. Example: 12

BaselineHost

Baseline server information.

Referenced by the following interfaces: DescribeBaselineHostIgnoreList, DescribeIgnoreHostAndItemConfig

name	required	NULL allowed	type	description

name	required	NULL allowed	type	description
HostId	no	no	String	Server ID. Example: 11cb73df-ea71-4678-8114-5af94e63ayay
HostIp	no	yes	String	Private IP address. Example: 192.168.0.204
HostName	no	yes	String	Server name. Example: redis_node_cvm
HostTag	no	yes	String	Server tags. Example: ["tag-01"]
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information Example:View
WanIp	no	yes	String	Public IP address. Example: 192.168.0.204

LicenseBindDetail

License binding details.

Referenced by the following interfaces: DescribeLicenseBindList

name	required	NULL allowed	type	description
AgentStatus	no	no	String	CWP client status: OFFLINE, ONLINE, and UNINSTALL. Example: OFFLINE
IsSwitchBind	no	no	Bool	Whether the license can be unbound from a server and bound to another server. false: the bound server cannot be changed. Example: false
IsUnBind	no	no	Bool	Whether the license can be unbound. false: unbinding is not allowed. Example: false
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information Example:View
MachineIp	no	no	String	Private IP address of the server. Example: 1.1.1.1
MachineName	no	no	String	Alias of the server. Example: redis_node_cvm
MachineWanIp	no	no	String	Public IP address of the server. Example: 1.1.1.1
Quuid	no	no	String	UUID of the cloud server. Example: 935e27b1-d675-4509-80bf-99bf0764237
Tags	no	no	Array of String	Tag information. Example: ["redis_cvm_01"]
Uuid	no	no	String	CWP client UUID. Example: 935e27b1-d675-4509-80bf-99bf0764237

MachineClearHistory

Machine Cleanup Record Object

Referenced by the following interfaces: DescribeMachineClearHistory

name	required	NULL allowed	type	description
AgentLastOfflineTime	yes	no	String	Client Last Offline Time Example: 2020-03-28 17:33:04
CreateTime	yes	no	String	Creation time. Example: 2019-03-28 17:33:04
Id	yes	no	Uint64	ID Value Example: 1
InstanceId	yes	no	String	Instance ID. Example: ins-vd9y7dl
InstanceName	yes	no	String	Instance name. Example: redis_node_cvm
PrivateIp	yes	no	String	Private IP. Example: 10.0.0.1
PublicIp	yes	no	String	Public IP Example: 8.8.8.8

ScreenRegionMachines

3D server charts in the dashboard.

Referenced by the following interfaces: DescribeScreenMachines

name	required	NULL allowed	type	description
AttackCnt	yes	no	Uint64	Number of servers with potential risks. Example: 12
IgnoreCnt	yes	no	Uint64	Number of servers that are ignored in the display. A value of 0 indicates that all servers are displayed. Example: 1
Machines	yes	no	Array of ScreenMachine	Server list Example:View
Region	yes	no	String	Region. Example: ap-bangkok
RegionName	yes	no	String	Region description. Example: region1
RiskCnt	yes	no	Uint64	Number of servers at risk. Example: 1
SafetyCnt	yes	no	Uint64	Number of servers with no risks. Example: 12
TotalCount	yes	no	Uint64	Number of servers in the region. Example: 14
UnAgentOfflineCnt	yes	no	Uint64	Number of offline servers or servers with no agent installed. Example: 12

VulInfoList

Vulnerability list in the CWP vulnerability management module.

Referenced by the following interfaces: DescribeVulList

name	required	NULL allowed	type	description
AttackLevel	no	yes	Uint64	Attack level. If the value is 3 or higher, the attack is a notable attack. Example: 1
CveId	yes	yes	String	CVE ID. Example: CVE-2021-3156
CvssScore	yes	yes	Float	CVSS score. Example: 9
DefenseAttackCount	yes	yes	Uint64	Number of prevented attack attempts. Example: 12
Descript	yes	yes	String	Description. Example: Vulnerability description
DescriptWisteria	yes	yes	String	Deprecated parameter. Example: Obsolete
FirstAppearTime	yes	yes	String	First occurrence time. Example: 2021-03-30 19:17:28
FixNotNeedRestart	no	yes	Bool	Whether a restart is required after vulnerability repair. Example: true
FixSwitch	yes	yes	Uint64	Whether automatic fixing is supported and servers that support automatic fixing are included. 0: no. 1: yes. Example: 1
From	yes	yes	Uint64	Deprecated parameter. Example: 0
HostCount	yes	no	Uint64	Number of affected servers. Example: 2
Ids	yes	no	String	One or more event IDs. Multiple event IDs are separated with commas (,). Example: 1
IsSupportDefense	yes	yes	Uint64	Whether to support attack defense. 0: not supported. 1: supported. Example: 1
Labels	yes	yes	String	Vulnerability tags. Multiple tags are separated by a comma. EXP exists: EXP. Zero-day attack: KNOWN_EXPLOITED. Local exploitation: LOCAL. Mandatory vulnerabilities to be fixed: NEED_FIX. Remote exploitation: NETWORK. POC exists: POC. System restart: RESTART. Example: LOCAL,NETWORK
LastTime	yes	no	String	Last detection time. Example: 2021-03-16 16:21:51
Level	yes	no	Uint64	Vulnerability severity. 1: low. 2: medium. 3: high. 4: critical. Example: 1
Method	no	yes	Uint64	Detection method. 0: version comparison, 1: POC verification. Example: 1
Name	yes	no	String	Vulnerability name. Example: Apache HTTP/2 DoS vulnerability (CVE-2023-44487)
NameWisteria	yes	yes	String	Deprecated parameter. Example: Obsolete
PublishTime	yes	no	String	Time when the vulnerability was published. Example: 2021-03-16 16:21:51
PublishTimeWisteria	yes	yes	String	Deprecated parameter. Example: Obsolete
Status	yes	no	Uint64	0: to be handled. 1: ignored. 3: fixed. 5: checking. 6: fixing. 8: fix failed. Example: 1
StatusStr	yes	yes	String	Event status after aggregation. Example: 1,2
TaskId	yes	yes	Uint64	ID of the last scan task. Example: 12
VulCategory	yes	yes	Uint64	Vulnerability category. 1: Web-CMS vulnerability. 2: application vulnerability. 4: Linux software vulnerability. 5: Windows system vulnerability. Example: 1
VulFixSwitch	no	yes	Uint64	Whether vulnerability fixing is supported. 0: not supported; 1: supported. Example: 1
VulId	yes	no	Uint64	Vulnerability ID. Example: 1

ProtectEventLists

List of protection events.

Referenced by the following interfaces: DescribeWebPageEventList

name	required	NULL allowed	type	description
CreateTime	no	no	String	Detection time. Example: 2020-10-01 01:01:10
EventDir	no	no	String	Event directory. Example: event
EventStatus	no	no	Uint64	Event status. 1: recovered. 0: not recovered. Example: 0
EventType	no	no	Uint64	Event type. 0: the content was modified and recovered. 1: the permissions were modified and recovered. 2: the ownership was modified and recovered. 3: deleted and recovered. 4: the newly added content was deleted. Example: 0
FileType	no	no	Uint64	File type. 0: regular file. 1: directory. 2: soft link. Example: 0
HostIp	no	no	String	Server IP address. Example: 172.16.100.1

name	required	NULL allowed	type	description
HostName	no	no	String	Server name. Example: host1
Id	no	no	Uint64	Unique ID. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information Example:View
Quuid	no	yes	String	Machine instance UUID. Example: 8c09e1b1-5611-45b3-9c02-737996011b81
RestoreTime	no	no	String	Time when the alarm was cleared. Example: 2020-10-01 01:01:10

ProtectStat

Protection information.

Referenced by the following interfaces: DescribeWebPageProtectStat

name	required	NULL allowed	type	description
Name	yes	no	String	Name. Example: /tmp
Num	yes	no	Uint64	Total number. Example: 56

LogHistogram

Histogram statistics collected within a period.

Referenced by the following interfaces: DescribeLogHistogram

name	required	NULL allowed	type	description
Count	yes	no	Int64	Number of log entries within a statistical period. Example: 0
TimeStamp	yes	no	Int64	UNIX timestamp rounded by period. Unit: milliseconds. Example: 0

MaliciousRequestWhiteListInfo

Information about the allowlist of the Anti-Malicious Requests feature.

Referenced by the following interfaces: DescribeMaliciousRequestWhiteList

name	required	NULL allowed	type	description
CreateTime	yes	no	String	Creation time. Example: 2021-02-08 14:46:25
Domain	yes	no	String	Domain name. Example: www.domain.com
Id	yes	no	Uint64	Allowlist ID. Example: 1
Mark	yes	no	String	Description. Example: add redis cvm
ModifyTime	yes	no	String	Update time. Example: 2021-02-08 14:46:25

ReverseShellEventInfo

Reverse shell event details.

Referenced by the following interfaces: DescribeReverseShellEventInfo

name	required	NULL allowed	type	description
CmdLine	yes	no	String	Command details. Example: ./reverse_out
CmdLineQuote	no	no	String	Escaped content of command details. It is used when regular expressions match allowlisted full strings. Example: ./reverse_out
CreateTime	yes	no	String	Time when the command was generated. Example: 2021-05-20 17:00:33
DetectBy	yes	no	Uint64	Detection method. Example: 1
DstIp	yes	no	String	Target IP address. Example: 127.0.0.1
DstPort	yes	no	Uint64	Target port. Example: 12
FullPath	yes	no	String	Process path. Example: /home
HarmDescribe	yes	no	String	Description. Example: After hacking a server, hackers may perform operations such as downloading malicious files, connecting to a mining pool, adding public keys, and viewing sensitive files for further malicious actions.
HostIp	yes	no	String	Private IP address of the server. Example: 127.0.0.1
Id	yes	no	Uint64	Primary key ID. Example: 11
MachineName	yes	no	String	Server name. Example: redis_node_cvm
MachineStatus	yes	no	String	Connection status of the server. Valid values: OFFLINE and ONLINE. Example: OFFLINE
MachineWanIp	yes	no	String	Public IP address of the server. Example: 124.2.4.55
ModifyTime	yes	no	String	Handling time. Example: 2021-03-30 19:17:28
ParentProcGroup	yes	no	String	User group of the parent process. Example: root
ParentProcName	yes	no	String	Parent process name. Example: 2.exe
ParentProcPath	yes	no	String	Path of the parent process. Example: /home
ParentProcUser	yes	no	String	User of the parent process. Example: root
ProcessName	yes	no	String	Process name. Example: reverse_out
PsTree	yes	yes	String	Process tree in the JSON format. pid: process ID. exe: file path. account: user group and user to which the process belongs. cmdline: command to be run. ssh_service: SSH service. ssh_source: login source. Example: [{"pid":"1"}]
Quuid	yes	no	String	Host UUID. Example: e8fc6e04-5b1d-405d-ab61-da7cc8be2583
References	yes	no	Array of String	Reference link. Example: ["http://www.domain.com"]
Status	yes	no	Uint64	Handling status. 0: to be handled. 2: added to the allowlist. 3: handled. 4: ignored. Example: 2
SuggestScheme	yes	no	String	Suggestion scheme. Example: 1. Check for malicious processes and invalid ports, and delete suspicious startup items and scheduled tasks. 2. Isolate or delete relevant Trojan files.
Tags	yes	no	Array of String	Tag. Example: ["Tag 1","tag 2"]
UserGroup	yes	no	String	User group that performs execution. Example: root
UserName	yes	no	String	User who performs execution. Example: root
Uuid	yes	no	String	UUID of the CWP agent. Example: e8fc6e04-5b1d-405d-ab61-da7cc8be2583

RiskDnsEvent

Malicious request event.

Referenced by the following interfaces: DescribeRiskDnsEventInfo, DescribeRiskDnsEventList

name	required	NULL allowed	type	description
AccessCount	no	no	Int64	Number of access requests. Example: 10
AgentId	no	no	String	Client ID Example: a1f53e38-3f03-4a72-bf16-afa78dd698f3
CmdLine	no	no	String	Command line. Example: cmd
Domain	no	no	String	Access domain name. Example: nx1lr3.org
FirstTime	no	no	String	First access time. Example: 2021-04-26 15:19:04
HandleStatus	no	no	Int64	Handling status. 0: to be handled. 2: added to the allowlist. 3: untrusted. 4: handled. 5: ignored. Example: 1
HostId	no	no	String	Server ID. Example: d1f53e38-3f03-4a72-bf16-afa78ed698f2
HostIp	no	no	String	IP address of the server. Example: 10.0.0.1
HostName	no	no	String	Server name. Example: security-data-seayay
HostStatus	no	no	String	Connection status of the server. Valid values: OFFLINE, ONLINE, and UNKNOWN. Example: ONLINE
Id	no	no	Int64	Event ID. Example: 153
LastTime	no	no	String	Last access time. Example: 2022-07-15 11:27:01
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
OsType	no	yes	Int64	[1:CentOS
Pid	no	no	Int64	Process ID. Example: 1
PolicyId	no	no	Int64	Policy ID. Example: 10000
PolicyName	no	no	String	Name of the hit policy. Example: System rule (standard)
PolicyType	no	no	Int64	Hit policy type. -1: unknown. 0: system policy. 1: custom policy. Example: 1
ProcessMd5	no	no	String	MD5 value of the process. Example: 3c59dc048e8850243be8079a5c74d079
ProcessName	no	no	String	Process name. Example: bash
ProtectLevel	no	no	Int64	Protection level. 0: Basic Edition. 1: Professional Edition. 2: Ultimate Edition. Example: 1
ReferenceLink	no	no	String	Reference link. Example: http://www.xxjump.net/files/virus_analysis/virut%20botnet%20anal
SuggestSolution	no	no	String	Fix solution. Example: 1. Check for malicious processes and invalid ports, and delete suspicious startup items and scheduled tasks. 2. Isolate or delete relevant Trojan files.
Tags	no	no	Array of String	Tags. Example: ["user","role"]
ThreatDesc	no	no	String	Threat description. Example: It is detected that your host has accessed malicious IP addresses/domain names. Your host may have been compromised.\nMalicious IP addresses/domain names could be remote control servers, malware download sources, or mining pool addresses.

name	required	NULL allowed	type	description
WanIp	no	no	String	Public IP address. Example: 13.22.3.1

NetAttackTopInfo

Referenced by the following interfaces: DescribeAttackTop

name	required	NULL allowed	type	description
Agent	no	yes	Array of TopInfo	Top Statistical Data on Network Attack Host Dimension Example:View
DstPort	no	yes	Array of TopInfo	Top Statistical Data on Network Attack Target Port Dimension Example:View
SrcIp	no	yes	Array of TopInfo	Top Statistical Data on Network Attack IP Source Dimension Example:View
Vul	no	yes	Array of TopInfo	Top Statistical Data on Network Attack Vulnerability Dimension Example:View

RansomDefenseStrategyMachineDetail

Anti-Ransomware Host List

Referenced by the following interfaces: DescribeRansomDefenseStrategyMachines

name	required	NULL allowed	type	description
CloudTags	yes	yes	Array of Tag	Cloud tag Example:View
DiskInfo	yes	yes	String	Hard Disk Information, effective for all disks when empty: diskId1
HostVersion	yes	yes	Uint64	Edition. 0: Basic Edition. 1: Professional Edition. 2: Ultimate Edition. 3: General Edition. Example: 0
InstanceId	yes	no	String	Host Instance ID Example: cvm-asasa
MachineIp	yes	no	String	Private IP address. Example: 10.0.0.22
MachineName	yes	no	String	Server name. Example: redis_node_cvm
MachineWanIp	yes	yes	String	Public IP. Example: 112.11.33.22
Quuid	yes	no	String	Host QUUID. Example: acdd5474-6360-46d4-bfc7-841162cb8116
RegionInfo	yes	yes	RegionInfo	Information on availability zones. Example:View
Status	yes	yes	Uint64	Protection status: 0 Disabled, 1 Enabled. Example: 0
StrategyId	yes	yes	Uint64	Policy ID. 0 indicates no binding to any policy. Example: 0
StrategyName	yes	yes	String	Policy name. Example: tt1
Tag	yes	yes	Array of MachineTag	Host Security Tag Example:View
Uuid	yes	no	String	Host UUID. Example: acdd5474-6360-46d4-bfc7-841162cb8116

OpenPortStatistics

Port statistics list

Referenced by the following interfaces: DescribeOpenPortStatistics

name	required	NULL allowed	type	description
MachineNum	yes	no	Uint64	Number of hosts. Example: 100
Port	yes	no	Uint64	Port number. Example: 8080

BaselineItemInfo

Baseline information.

Referenced by the following interfaces: DescribeBaselineItemIgnoreList, DescribeBaselineItemInfo, DescribeIgnoreHostAndItemConfig

name	required	NULL allowed	type	description
FixMethod	yes	no	String	Fix solution of the check item. Example: Weak password rectification
ItemDesc	yes	no	String	Description of the check item. Example: Weak password
ItemId	yes	no	Int64	ID of the baseline check item. Example: 1
ItemName	yes	no	String	Name of the check item. Example: Set password expiration time.
Level	yes	no	Int64	Baseline risk level. 0: low; 1: medium; 2: high; 3: critical. Example: 1
RelatedCustomRuleInfo	yes	yes	Array of BaselineCustomRuleIdName	Information about the referenced custom rule. Example:View
RuleId	yes	yes	Uint64	ID of the rule to which the check item belongs. Example: 45617
RuleName	yes	no	String	Name of the rule to which the check item belongs. Example: Weak password
SysRuleId	yes	yes	Int64	ID of the system rule. Example: 1

UpdateHostLoginWhiteObj

Object used to modify an allowlist.

Referenced by the following interfaces: ModifyLoginWhiteInfo

name	required	NULL allowed	type	description
EndTime	no	no	String	End time. Example: 2024-01-01 23:59:59
Id	yes	no	Uint64	ID of the data record that you want to update. Example: 128
Places	yes	no	Array of Place	Region information. Example:View
Remark	yes	no	String	Remarks. Example: updateRemark1
SrcIp	yes	no	String	Source IP. Example: 1.2.3.4
StartTime	no	no	String	Start time. Example: 2024-01-01 00:00:00
UserName	yes	no	String	User name. Example: username

VulDetailInfo

Vulnerability details.

Referenced by the following interfaces: DescribeScanTaskDetails

name	required	NULL allowed	type	description
CveId	yes	no	String	CVE ID. Example: cve_ay
Cvss	yes	no	String	CVSS details. Example: dadad
CvssScore	yes	no	Float	CVSS score. Example: 1.1
Descript	yes	no	String	Vulnerability description. Example: desc of this vul
Fix	yes	no	String	Fix suggestions. Example: Repair
Level	yes	no	Uint64	Vulnerability severity. Example: 1
Name	yes	no	String	Vulnerability name. Example: Vulnerability
PublishTime	yes	no	String	Release time. Example: 11
Reference	yes	no	String	Reference link. Example: http://www.domain.com/any/any
VulCategory	yes	no	Uint64	1: Web-CMS vulnerability. 2: application vulnerability. 4: Linux software vulnerability. 5: Windows system vulnerability. 0: emergency vulnerability. Example: 1
VulId	yes	no	Uint64	Vulnerability ID. Example: 1

CloudVendorAccountAK

Cloud vendor account AK information.

Referenced by the following interfaces: DescribeCloudVendorAccountAKList

name	required	NULL allowed	type	description
AccessKey	no	yes	String	AccessKeyId Example: LtDsgdo
CloudType	no	yes	Int64	Cloud vendor type. • 1: Alibaba Cloud. Example: 1
Id	no	yes	Uint64	The record ID. Example: 1
Message	no	yes	String	Prompt Message Example: some message
Reason	no	yes	String	Reason Example: any reason
Status	no	yes	Int64	AK status. • 0: normal. 1: abnormal. Example: 0
Uid	no	yes	String	Root Account ID Example: 15443424353

AttackSourceEvent

Attack backtracking event.

Referenced by the following interfaces: DescribeAttackSourceEvents

name	required	NULL allowed	type	description
Content	yes	no	String	For file scanning and cleaning, the content includes VirusName, FileName, FilePath, FileSize, MD5, CreateTime, LatestScanTime, HarmDescribe, and SuggestScheme.

name	required	NULL allowed	type	description
				For logins from unusual locations, the content includes SrcIp, Location, UserName, and LoginTime. For password cracking, the content includes SrcIp, City, Country, Protocol, UserName, Port, Count, CreateTime, and ModifyTime. For malicious requests, the content includes Url, ProcessName, ProcessMd5, Pid, AccessCount, MergeTime, HarmDescribe, and SuggestScheme. For high-risk commands, the content includes RuleName, RuleCategory, BashCmd, DetectBy, User, Pid, CreateTime, HarmDescribe, and SuggestScheme. Example: VirusName
CreatedTime	yes	no	String	Intrusion time. Example: 2021-03-30 19:17:28
EventType	yes	no	Uint64	Event type. 0: file scanning and cleaning. 1: login from an unusual location. 2: password cracking. 3: malicious request. 4: high-command risk. Example: 1
Id	yes	no	Uint64	Event ID. Example: 12
Level	yes	no	Uint64	Uniform event severity. 0: informational. 1: low-risk. 2: medium-risk. 3: high-risk. 4: critical. Example: 1
LevelZh	yes	no	String	Level name Example: Critical
Uuid	yes	no	String	Host UUID. Example: e5b4724c-4faf-46ab-bd84-cdbae897e7e0

AssetPortBaseInfo

Basic account information in the asset management module.

Referenced by the following interfaces: DescribeAssetPortInfoList

name	required	NULL allowed	type	description
BindIp	no	no	String	Binds the IP address. Example: 192.168.0.1
FirstTime	no	no	String	First collection time. Example: 2022-07-15 11:27:01
GroupName	no	no	String	User group. Example: staffs
IsNew	no	no	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Host information ExampleView
MachineIp	no	no	String	Private IP address of the server. Example: 10.33.0.155
MachineName	no	no	String	Server name. Example: 1
MachineWanIp	no	no	String	Public IP address of the server. Example: 112.44.64.99
Md5	no	no	String	MD5 value of the process. Example: c2caac18e871b6dae87c6167791ff97a8
OsInfo	no	no	String	OS information. Example: Centos 64Bit
Param	no	no	String	Boot parameters. Example: /usr/sbin/crupsd -l
ParentProcessName	no	no	String	Name of the parent process. Example: root
Pid	no	no	String	Process ID. Example: 1024
Port	no	no	String	Port. Example: 22
Ppid	no	no	String	ID of the parent process. Example: 1
ProcessName	no	no	String	Process name. Example: a.out
ProcessPath	no	no	String	Process path. Example: /root
ProcessVersion	no	no	String	Process version. Example: 1.1.1
ProjectId	no	no	Uint64	ID of the project to which the server belongs. Example: 1
Proto	no	no	String	Port protocol, which can be UDP or TCP. Example: tcp
Quuid	no	no	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
StartTime	no	no	String	Start time. Example: 2024-10-23 14:12:54
Tag	no	yes	Array of MachineTag	Server tags. ExampleView
Teletype	no	no	String	Process TTY. Example: ?
UpdateTime	no	yes	String	Data update time. Example: 2011-11-11 12:12:12
User	no	no	String	Run user. Example: root
Uuid	no	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

Vul

Vulnerability list data

Referenced by the following interfaces: DescribeVuls

name	required	NULL allowed	type	description
ImpactedHostNum	yes	no	Uint64	Number of affected servers. Example: 1
LastScanTime	yes	no	Datetime	Last scan time. Example: 2020-02-01 12:00:00
VulId	yes	no	Uint64	Vulnerability category ID. Example: 1
VulLevel	yes	no	String	Risk severity of the vulnerability. HIGH: high MIDDLE: medium LOW: low NOTICE: informational Example: LOW
VulName	yes	no	String	Vulnerability name. Example: Apache
VulStatus	yes	no	String	Vulnerability status. *UN_OPERATED: pending* FIXED: fixed. Example: UN_OPERATED

BaselineHostDetect

Baseline check on a server.

Referenced by the following interfaces: DescribeBaselineHostDetectList

name	required	NULL allowed	type	description
DetectStatus	no	no	Int64	0: checked not passed. 1: ignored. 3: check passed. 5: checking. Example: 0
FirstTime	no	no	String	First scan time. Example: 2021-02-01 12:00:00
HostId	no	no	String	Server ID. Example: 7b2effb9-d1d9-4bb7-9b5d-d80c88ddayay
HostIp	no	no	String	Private IP address. Example: 192.168.0.204
HostName	no	no	String	Server name. Example: redis_node_cvm
ItemCount	no	no	Int64	Number of associated check items. Example: 1
LastTime	no	no	String	Last detection time. Example: 2021-02-01 12:00:00
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information ExampleView
NotPassedItemCount	no	no	Int64	Number of check items that are not passed. Example: 1
PassedItemCount	no	no	Int64	Number of check items that are passed. Example: 0
Uuid	no	yes	String	UUID of the CWP agent. Example: 1bc7422a-2366-11e9-a4c5-525400f7ayay
WanIp	no	no	String	Public IP address. Example: 192.168.0.204

OsName

OS name.

Referenced by the following interfaces: DescribeMachineOsList

name	required	NULL allowed	type	description
MachineOSType	yes	no	Uint64	Operating system type. 1: CentOS; 2: Debian; 3: Gentoo; 4: Red Hat; 5: Ubuntu; 6: Windows Server; 7: TOS; 8: CoreOS; 9: FreeBSD; 10: SUSE; 11: Aliyun Linux; 12: OpenCloud. Example: 1
Name	yes	no	String	OS name. Example: Linux

ReverseShell

Reverse shell data.

Referenced by the following interfaces: DescribeReverseShellEvents

name	required	NULL allowed	type	description
CmdLine	no	no	String	Command details. Example: dadad
CmdLineQuote	no	no	String	Escaped content of command details. It is used when regular expressions match allowlisted full strings. Example: c2pgcmVsaXMuc2g=
CreateTime	no	no	String	Time when the command was generated. Example: 2021-05-20 17:00:33
DetectBy	no	no	Uint64	Detection method. 0: behavior analysis; 1 command feature detection Example: 1
DstIp	no	no	String	Target IP address. Example: 127.0.0.1
DstPort	no	no	Uint64	Target port. Example: 12
FullPath	no	no	String	Process path. Example: /home
HostIp	no	no	String	Private IP address of the server. Example: 127.0.0.1
Id	no	no	Uint64	Primary key ID. Example: 11
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information ExampleView

name	required	NULL allowed	type	description
MachineName	no	no	String	Server name. Example: redis_node_cvm
ParentProcGroup	no	no	String	User group of the parent process. Example: root
ParentProcName	no	no	String	Parent process name. Example: check_reverse
ParentProcPath	no	no	String	Path of the parent process. Example: /home
ParentProcUser	no	no	String	User of the parent process. Example: root
Pid	no	yes	Int64	Process ID. Example: 1
ProcTree	no	no	String	Process tree. Example: bash(25605),python3.7(25604),bash(25603),bash(25579),bash(25578),bash(3477),login(1307)
ProcessName	no	no	String	Process name. Example: 1.exe
Quuid	no	no	String	Server ID. Example: check_reverse
RiskLevel	no	yes	Uint64	Threat level. 0: medium risk, 1: high risk. Example: 1
Status	no	no	Uint64	Processing status. 0 - pending processing; 2 - allowlisted; 3 - processed; 4 - ignored; 6 - blocked. Example: 2
UserGroup	no	no	String	User group that performs execution. Example: root
UserName	no	no	String	User who performs execution. Example: root
Uuid	no	no	String	UUID of the CWP agent. Example: 5a540076-d38a-4078-aa98-c4f5c137d322

AssetWebAppBaseInfo

Web application information in the asset management module.

Referenced by the following interfaces: DescribeAssetWebAppList

name	required	NULL allowed	type	description
Desc	no	no	String	The description of the application. Example: no name
Domain	no	no	String	Domain name of the website. Example: www.ay.com
FirstTime	no	no	String	First collection time. Example: 2022-07-15 11:27:01
Id	no	no	String	Application ID. Example: 10001
IsNew	no	no	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	no	no	String	Private IP address of the server. Example: 10.0.0.11
MachineName	no	no	String	Server name. Example: agent-domain
MachineWanIp	no	no	String	Public IP address of the server. Example: 192.168.0.204
Name	no	no	String	Application name. Example: Nginx
OsInfo	no	no	String	OS information. Example: Centos 64Bit
PluginCount	no	no	Uint64	Number of plug-ins. Example: 10
ProjectId	no	no	Uint64	ID of the project to which the server belongs. Example: 1
Quuid	no	no	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
RootPath	no	no	String	Root path. Example: /root
ServiceType	no	no	String	Service Type Example: Web
Tag	no	yes	Array of MachineTag	Server tags. Example:View
UpdateTime	no	yes	String	Data update time. Example: 2011-11-11 12:12:12
Uuid	no	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Version	no	no	String	Version. Example: 1.0.1
VirtualPath	no	no	String	Virtual path. Example: /data/tmp

ScreenNameValue

Name-value data in the dashboard visualization module for cloud security alarming.

Referenced by the following interfaces: DescribeScreenEventsCnt, DescribeScreenGeneralStat, DescribeScreenRiskAssetsTop

name	required	NULL allowed	type	description
Name	yes	no	String	Data type. The value varies by API. Example: offline/shut down
Value	yes	no	Uint64	Number of data records. Example: 12

LogStorageRecord

Record of stored log size

Referenced by the following interfaces: DescribeLogStorageRecord

name	required	NULL allowed	type	description
InquireSize	no	yes	Uint64	Total volume, in bytes. Example: 0
Month	no	yes	String	Year and month. Example: 202304
UsedSize	no	yes	Uint64	Storage amount, in bytes. Example: 0

AssetCoreModuleParam

Kernel module parameters in the asset management module.

Referenced by the following interfaces: DescribeAssetCoreModuleInfo

name	required	NULL allowed	type	description
Data	yes	no	String	Data. Example: 16384
Name	yes	no	String	Name. Example: hashsize

BaselineDetectParam

Baseline check parameters.

Referenced by the following interfaces: StartBaselineDetect

name	required	NULL allowed	type	description
HostIds	no	no	Array of String	IDs of servers to be checked. Example: ["df00265c-081a-4e47-8b92-3e59d902aaay"]
ItemIds	no	no	Array of Int64	Set of check items. Example: [1001,1002]
PolicyIds	no	no	Array of Int64	Set of check policies. Example: [101,102,103]
RuleIds	no	no	Array of Int64	Set of check rules. Example: [10]

AssetWebLocationBaseInfo

Website information in the asset management module.

Referenced by the following interfaces: DescribeAssetWebLocationList

name	required	NULL allowed	type	description
FirstTime	no	no	String	First collection time. Example: 2022-07-15 11:27:01
Id	no	no	String	ID of the website. Example: 1
IsNew	no	yes	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	no	no	String	Private IP. Example: 10.0.11
MachineName	no	no	String	Server name. Example: any-ins
MachineWanIp	no	no	String	Public IP address. Example: 112.54.121.11
MainPath	no	no	String	Main directory. Example: /root
MainPathOwner	no	no	String	Owner of the main directory. Example: 1
Name	no	no	String	Domain name. Example: any.com
OsInfo	no	no	String	Operating system. Example: centos 64bit
PathCount	no	no	Uint64	Number of website paths. Example: 1
Permission	no	no	String	Owner permissions. Example: 1
Port	no	no	String	Port of the website. Example: 22
ProjectId	no	no	Uint64	ID of the project to which the server belongs. Example: 1
Proto	no	no	String	Protocol of the website. Example: http
Quuid	no	no	String	Host QUUID Example: acdd5474-6360-4fd4-bfc7-843162cb8116
ServiceType	no	no	String	Service type. Valid values: Tomcat, Apache, Nginx, WebLogic, Websphere, JBoss, Jetty, IHS, and Tengine. Example: Tomcat

name	required	NULL allowed	type	description
Tag	no	no	Array of MachineTag	Server tags. Example:View
UpdateTime	no	yes	String	Data update time. Example: 2011-11-11 12:12:12
User	no	no	String	Run user. Example: root
Uuid	no	no	String	Host UUID. Example: acdd5474-6360-4f64-bfc7-843162cb8116

Filters

Key-value pair filters for conditional filtering queries. For example, IDs, names, and states can be filtered.

If multiple filters exist, the AND relationship is used between the filters.
If you specify multiple values for 1 filter, the OR relationship is used between the values.

Referenced by the following interfaces: DescribeBaselineEffectHostList, DescribeBaselineList, DescribeCanNotSeparateMachine, DescribeEmergencyResponseList, DescribeEmergencyVulList, DescribeFileTamperEvents, DescribeFileTamperRules, DescribeGeneralStat, DescribeIgnoreRuleEffectHostList, DescribeImportMachineInfo, DescribeJavaMemShellList, DescribeJavaMemShellPluginInfo, DescribeJavaMemShellPluginList, DescribeLicenseBindList, DescribeLicenseList, DescribeMalPodList, DescribeMachineClearHistory, DescribeMaliciousRequestWhiteList, DescribeOrderList, DescribeRansomDefenseBackupList, DescribeRansomDefenseEventsList, DescribeRansomDefenseMachineList, DescribeRansomDefenseRollBackTasksList, 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

name	required	NULL allowed	type	description
ExactMatch	no	no	Bool	Whether to use fuzzy matching. This parameter will be passed in for frontend frameworks and can be ignored. Example: false
Name	yes	no	String	Name of the filter key. Example: Name
Values	yes	no	Array of String	One or more filter values. Example: ["value"]

MalwareWhiteListAffectEvent

Component list data.

Referenced by the following interfaces: DescribeMalwareWhiteListAffectList

name	required	NULL allowed	type	description
CreateTime	yes	no	String	Time when a policy is added. Example: 2024-10-30 09:12:21
FilePath	yes	no	String	File path. Example: /tmp/any
HostIp	yes	no	String	IP address of the server. Example: 10.0.0.1
Id	yes	no	Uint64	Unique ID. Example: 1
Md5	yes	no	String	MD5 value. Example: 708cae4cf814c3deda4208da228fed4e

OrderList

Order list object members.

Referenced by the following interfaces: DescribeOrderList

name	required	NULL allowed	type	description
Alias	no	yes	String	Alias of the resource. Example: redis_node_cvm
AutoRenewFlag	no	yes	Uint64	Auto-renewal flag. 0: Disabled by default (auto-renewal available for key accounts). 1: Automatically renew. 2: Manually set to not automatically renew (auto-renewal not available for key accounts). Example: 0
BeginTime	no	yes	String	Order start time. Example: 0000-00-00 00:00:00
DealName	no	yes	String	Current sub-order number. Example: name-anyone
EndTime	no	yes	String	Order end time. Example: 0000-00-00 00:00:00
ExtraParam	no	yes	OrderExtraParam	Additional parameters for orders. Example:View
InquireKey	no	yes	String	4-tier billable item name, which starts with sv_. Example: sv_yunjing_se_x
InquireNum	no	yes	Uint64	Resource purchase quantity. Example: 1
PayMode	no	yes	Uint64	Billing mode. 0: pay-as-you-go, 1: prepaid (monthly subscription). Example: 0
ProductCode	no	yes	String	Associated product p_. Example: p_arae
ProjectID	no	yes	Uint64	Project ID. Example: 0
RegionID	no	yes	Uint64	Region ID. Example: 1
ResourceId	no	yes	String	Resource ID. Example: any data
SourceType	no	yes	Uint64	Order type. 0: default billing order; 1: trial order; 2: gift; 3: experience. Example: 0
Status	no	yes	Uint64	Order status. 1: normal; 2: isolated; 3: terminated. Example: 1
SubProductCode	no	yes	String	Subproduct SP_. Example: sp_yunjing_0014
TagList	no	yes	Array of Tags	Cloud tag Example:View
UsedNum	no	yes	Uint64	Resource usage Example: 0
ZoneID	no	yes	Uint64	Zone ID Example: 100001

FileTamperRuleInfo

API for querying core file monitoring rules

Referenced by the following interfaces: DescribeFileTamperRules

name	required	NULL allowed	type	description
AddWhiteType	no	yes	String	Allowlisting type. • cur: Add only the current item to an allowlist. • all: Add all items that meet conditions to an allowlist. Example: cur
CreateTime	yes	no	String	Creation time. Example: 2021-03-30 19:17:28
FileAction	yes	yes	String	Monitoring behavior. • read: read files. • write: modify files. • read-write: read and modify files. Example: read
HostCount	yes	yes	Uint64	Number of affected servers. Example: 12
Id	yes	no	Uint64	Rule ID. The value of this parameter for a system rule is 0. Example: 12
IsGlobal	yes	no	Uint64	Whether it is a global rule. 0: no. 1: yes. Example: 1
Level	yes	no	Uint64	Risk severity. 0: no risk. 1: high. 2: medium. 3: low. Example: 3
ModifyTime	yes	no	String	Update time. Example: 2021-03-30 19:17:28
Name	yes	yes	String	Rule Name Example: Deny Access
ReadRuleCount	yes	no	Uint64	Number of read entries for a subrule. Example: 1
ReadWriteRuleCount	yes	no	Uint64	Number of read and write entries for a subrule. Example: 1
RuleCategory	yes	no	Uint64	Rule type. 0: system rule. 1: custom rule. Example: 1
Status	yes	no	Uint64	Status. 0: enabled. 1: disabled. Example: 1
WriteRuleCount	yes	no	Uint64	Number of write entries for a subrule. Example: 1

VulEmergentMsgInfo

Emergent notification information.

Referenced by the following interfaces: DescribeVulEmergentMsg

name	required	NULL allowed	type	description
Name	yes	no	String	Vulnerability name. Example: Apache HTTP/2 DoS vulnerability (CVE-2023-44487)
NameEn	no	no	String	Vulnerability name in English. Example: Apache HTTP/2 DoS vulnerability (CVE-2023-44487)
PublishTime	yes	no	String	Time when the vulnerability was published. Example: 2021-02-01 12:00:00
VulId	yes	no	Uint64	Vulnerability ID. Example: 105375

OrderExtraParam

Additional parameters for orders.

Referenced by the following interfaces: DescribeOrderList

name	required	NULL allowed	type	description
DisposableStatus	no	yes	Bool	One-time service delivery status, which is only available for one-time resource orders. false: not accepted. true: accepted. Example: true
Mode	no	yes	String	PrePay: monthly subscription. PostPay: pay-as-you-go. Disposable: one-time delivery. Example: PrePay

ScreenVulInfo

Vulnerability list in the dashboard.

Referenced by the following interfaces: DescribeScreenHostInvasion

name	required	NULL allowed	type	description
Category	yes	yes	Uint64	Vulnerability category. 1: Web-CMS vulnerability. 2: application vulnerability. 4: Linux software vulnerability. 5: Windows system vulnerability. Example: 1
Id	yes	no	Uint64	ID of the vulnerability event. Example: 1
LastTime	yes	no	String	Last detection time. Example: 2021-03-16 16:21:51
Level	yes	no	Uint64	Vulnerability severity. 1: low. 2: medium. 3: high. 4: informational. Example: 1

name	required	NULL allowed	type	description
Name	yes	no	String	Vulnerability name. Example: Git injection
Uuid	yes	yes	String	UUID of the server. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
VulId	yes	no	Uint64	Vulnerability ID. Example: 1

MaHost

Referenced by the following interfaces: DescribeMaHostList

name	required	NULL allowed	type	description
AlarmCount	no	yes	Int64	Number of exception accesses. Example: 10
HostIp	no	yes	String	Private IP Example: 10.0.0.1
Id	no	yes	Int64	ID Example: 1
InstanceId	no	yes	String	Instance ID. Example: ins-hmef3y81
IsEnabled	no	yes	Int64	Monitoring switch [1: On
IsNew	no	yes	Int64	Whether it is added in 15 days [1: Yes; 0: No]. Example: 1
IsSupportMa	no	yes	Int64	Whether to support micro-alarms [1: Yes; 0: No]. Example: 0
Labels	no	yes	Array of MaLabel	Associate Tag. Example:View
LearnEndTime	no	yes	String	End time of learning for a single workload. Example: 2024-01-01 00:00:00
LearnStartTime	no	yes	String	Start time of learning for a single workload. Example: 2024-01-01 00:00:00
Name	no	yes	String	Server name. Example: redis_node_cvm
NotSupportMaCode	no	yes	Int64	Reason for not supporting micro-alarms [0: Supported; 1: Low client version; 2: Not premium edition; 3: Client not installed]. Example: 0
OsName	no	yes	String	Operating system. Example: CentOS Linux release 7.8.2003 (Core)
PublicIp	no	yes	String	Public IP Example: 8.8.8.8
Region	no	yes	String	Region. Example: ap-region1
Uuid	no	yes	String	UUID of the server. Example: b5389fcc-e666-408a-aa94-fc5280b5d629
VpcId	no	yes	String	Network Example: vpc-82h54yji

FileTamperEvent

Core file monitoring event.

Referenced by the following interfaces: DescribeFileTamperEvents

name	required	NULL allowed	type	description
CreateTime	no	no	String	Event time. Example: 2024-10-28 20:23:23
Description	no	no	String	Risk description. Example: It is detected that the user configuration file '/opt/redis/redis.cfg' is tampered with.
EventCount	no	no	Uint64	Number of event occurrences. Example: 1
ExeMd5	no	no	String	Process name. Example: 0c0f9309e0bf2912ae5242d144bcayay
ExeName	no	yes	String	Process name. Example: vim
ExePermission	no	no	String	Process permission. Example: rwx
ExePid	no	no	Uint64	Process pid. Example: 1
ExeSize	no	no	Uint64	Size of the process file. Example: 100
ExeTime	no	no	Uint64	Execution duration of the process. Example: 1000
FileAction	no	yes	String	File threat behavior. • read: Read files. • write: Modify files. Example: read
HostIp	no	no	String	Server IP address. Example: 10.0.0.1
HostName	no	no	String	The instance name Example: redis_node_cvm
Id	no	no	Uint64	Event ID. Example: 1
Level	no	no	Uint64	Risk severity. 0: no risk. 1: high. 2: medium. 3: low. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information Example:View
MachineStatus	no	no	String	Connection status of the server. Valid values: ONLINE and OFFLINE. Example: ONLINE
ModifyTime	no	no	String	Last occurrence time. Example: 2024-10-28 20:23:23
PrivateIp	no	no	String	Private IP address. Example: 10.0.0.1
ProcessArgv	no	no	String	Process parameter. Example: vim /home/seadmin/.bashrc
ProcessExe	no	no	String	Process path. Example: /tmp/any
Pstree	no	no	String	Event details in the JSON format. Example: [{"pid":2403140,"exe":"/usr/bin/vim","account":"1000:1000","cmdline":"vim /home/seadmin/.bashrc","ssh_service":"10.31.132.68:22"}]
Quuid	no	no	String	cvm id Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
Reference	no	no	String	Reference link. Example: http://www.ay.com/ay
RuleCategory	no	no	Uint64	Rule type. 0: system rule. 1: custom rule. Example: 0
RuleId	no	no	Uint64	Rule ID. Example: 1
RuleName	no	no	String	Rule Name Example: redis_node_check
Status	no	no	Uint64	Handling status. 0: to be handled. 1: added to the allowlist. 2: deleted. 3: ignored. 4: manually handled. Example: 0
Suggestion	no	no	String	Maintenance suggestions. Example: Check whether the modification is required for normal businesses.
Target	no	no	String	Path of the target file. Example: /home/seadmin/.bashrc
TargetCreatTime	no	yes	String	Time when the target file was created. Example: 2021-01-02 15:04:05
TargetModifyTime	no	yes	String	Time when the target file was updated. Example: 2021-01-02 15:04:05
TargetName	no	no	String	The file name. Example: .bashrc
TargetPermission	no	no	String	Permissions on the target file. Example: rwx
TargetSize	no	no	Uint64	Size of the target file. Example: 1000
Type	no	no	Uint64	Event type or action. 0: alarming. Example: 0
UserGroup	no	no	String	User Group Example: root
UserName	no	no	String	User name. Example: root
Uuid	no	no	String	Host UUID. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0

BashEvent

High-risk command data.

Referenced by the following interfaces: DescribeBashEvents

name	required	NULL allowed	type	description
BashCmd	yes	no	String	Command to run. Example: rm
CreateTime	yes	no	String	Event time. Example: 2021-03-30 19:17:28
DetectBy	yes	yes	Uint64	0: bash command. 1: real-time monitoring (Thunder Edition) Example: 1
Exe	yes	yes	String	Process name. Example: 1.exe
HostName	no	yes	String	Host name. Example: redis_node_cvm
Hostip	yes	no	String	Private IP address of the server. Example: 127.0.0.1
Id	yes	no	Uint64	Data ID. Example: 1
MachineName	yes	no	String	Server name. Example: redis_node_cvm
ModifyTime	yes	yes	String	Handling time. Example: 2021-03-30 19:17:28
Pid	yes	yes	String	Process ID. Example: 1
Platform	yes	no	Uint64	System type. 2: Windows; 4: Linux. Example: 4
Quuid	yes	no	String	Server ID. Example: 380add75-bb06-4cc4-84c5-c1806d102fba
RegexBashCmd	yes	yes	String	Auto-generated regular expression. Example: rm -rf /tmp/t*
RuleCategory	yes	yes	Uint64	Rule type. 0: system rule. 1: custom rule. Example: 0
RuleId	yes	no	Uint64	Rule ID. Example: 1
RuleLevel	yes	no	Uint64	Rule severity. 1: high. 2: medium. 3: low. Example: 1

name	required	NULL allowed	type	description
RuleName	yes	no	String	Rule Name Example: redis_node_use
Status	yes	no	Uint64	Handling status. 0: to be handled. 1: handled. 2: added to the allowlist. 3: ignored. Example: 1
User	yes	no	String	User who performs execution. Example: root
Uuid	yes	no	String	CWP ID. Example: 380add75-bb06-4cc4-84c5-cf806d102fba

Tags

Platform tags.

Referenced by the following interfaces: CreateLicenseOrder, DescribeHostInfo, DescribeImportMachineInfo, DescribeLicenseList, DescribeMachineList, DescribeMachines, DescribeMachinesSimple, DescribeOrderList, DescribeVulEffectHostList, ExportLicenseDetail, ModifyOrder

name	required	NULL allowed	type	description
TagKey	yes	no	String	Tag key. Example: business1
TagValue	yes	no	String	Tag value. Example: businessValue

VulInfoByCveId

Vulnerability details queried based on CVE IDs.

Referenced by the following interfaces: DescribeVulCveIdInfo

name	required	NULL allowed	type	description
FixSwitch	yes	no	Uint64	Fixing support status: 0 - not support fixing for Windows and Linux; 1 - support fixing for both Windows and Linux; 2 - support fixing for Linux only; 3 - support fixing for Windows only. Example: 1
VulId	yes	no	Uint64	Vulnerability ID. Example: 12

LoginWhiteListsNew

Login allowlist

Referenced by the following interfaces: DescribeLoginWhiteListNew

name	required	NULL allowed	type	description
CreateTime	yes	no	String	Time when the blocklist was created. Example: 2020-02-01 12:00:00
EndTime	yes	yes	String	End time. Example: 2020-02-01 12:00:00
HostIp	yes	no	String	Server IP address. Example: 192.168.0.10
Id	yes	no	Uint64	The record ID. Example: 1
IsGlobal	yes	no	Uint64	Whether the rule is valid globally. 1: valid globally. 0: valid only for a single server. Example: 1
Locale	yes	no	String	Region string. Example: locale1
MachineName	yes	no	String	The host name. Example: redis_node_cvm
ModifyTime	yes	no	String	Time when the blocklist was modified. Example: 2020-02-01 12:00:00
Places	yes	yes	Array of Place	Region of the allowlist. Example:View
Quuid	yes	no	String	Host QUUID. Example: 5a540076-d38a-4078-aa98-qwert371d322
Remark	yes	yes	String	Description. Example: add redis cvm ip
SrcIp	yes	no	String	IP addresses in the allowlist. Multiple IP addresses are separated with commas (,). Example: 192.168.0.1
StartTime	yes	yes	String	Start time. Example: 2020-02-01 12:00:00
UserName	yes	no	String	Users in the allowlist. Separate multiple usernames with commas (,). Example: Alice
Uuid	yes	no	String	ID of the CWP agent. Example: 5a540076-d38a-4078-aa98-qwert371d322

PolicyRules

Policy rule expression.

Referenced by the following interfaces: CheckBashPolicyParams, DescribeBashPolicies, ModifyBashPolicy

name	required	NULL allowed	type	description
AProcess	no	yes	CommandLine	Ancestral Process Example:View
PProcess	no	yes	CommandLine	Parent Process Example:View
Process	no	yes	CommandLine	Processes Example:View

UuidHostip

Machine that passed the check and the corresponding host IP address.

Referenced by the following interfaces: DescribeMemShellRules, DescribeReverseShellRulesAggregation

name	required	NULL allowed	type	description
Hostip	no	yes	String	Server IP address. Example: 172.16.0.9
Uuid	no	yes	String	Server ID Example: 82727b6e-3676-4660-ac4e-c281dba1b21f

AssetLoadDetail

Load information in the asset management module.

Referenced by the following interfaces: DescribeAssetLoadInfo

name	required	NULL allowed	type	description
Desc	yes	no	String	Description. Example: 4G
MachineName	yes	no	String	Server name. Example: redis_node_cvm
Quuid	yes	no	String	Host QUUID. Example: d99a1b46-cc2d-4633-a11f-4a7663d2523e
Uuid	yes	no	String	Host UUID. Example: d99a1b46-cc2d-4633-a11f-4a7663d2523e
Value	yes	no	Float	Load. Example: 0.4

MachineTag

Server tag information

Referenced by the following interfaces: DescribeAssetAppList, DescribeAssetDatabaseList, DescribeAssetMachineList, DescribeAssetPortInfoList, DescribeAssetProcessInfoList, DescribeAssetWebAppList, DescribeAssetWebFrameList, DescribeAssetWebLocationList, DescribeAssetWebServiceInfoList, DescribeImportMachineInfo, DescribeLoginWhiteHostList, DescribeMachineList, DescribeMachines, DescribeMachinesSimple, DescribeRansomDefenseMachineList, DescribeRansomDefenseStrategyMachines

name	required	NULL allowed	type	description
Name	yes	no	String	Tag name. Example: redis_node
Rid	yes	no	Int64	Associated tag ID. Example: 10
TagId	yes	no	Uint64	Tag ID. Example: 1010

RansomDefenseStrategy

Tag information of a server returned from the server list query API.

Referenced by the following interfaces: DescribeRansomDefenseStrategyList

name	required	NULL allowed	type	description
BackupType	yes	yes	Uint64	Backup pattern: 0 weekly, 1 daily Example: 0
CreateTime	yes	yes	String	Creation time. Example: 2022-12-12 12:12:12
Description	yes	yes	String	Policy Remarks Example: subtitle
ExcludeDir	yes	yes	String	Includes directories, separated by semicolons (;). Example: /usr
Hour	yes	no	String	Backup Execution Time Point (0-23): 11:00; 12:00 Example: 11:00
Id	yes	no	Int64	Policy ID. Example: 1
IncludeDir	yes	yes	String	Includes directories, separated by semicolons (;). Example: /root
IsAll	yes	no	Uint64	Whether it takes effect for all hosts. Example: 1
MachineCount	yes	yes	Uint64	Number of Bound Machines Example: 12
ModifyTime	yes	yes	String	The point in time when the namespace was last modified. Example: 2022-12-12 12:12:12
Name	yes	no	String	Policy name. Example: strategyName
SaveDay	yes	no	Uint64	Storage Days, 0 for Permanent Example: 5
Status	yes	no	Uint64	Enabling Status: 0 Disabled, 1 Enabled. Example: 1
Uin	yes	yes	String	Operating UIN Example: 1
Weekday	yes	yes	String	Backup days in a week (1-7): 1; 2; 3; 4. Example: 1;2;3

LicenseUnBindRsp

License unbinding information.

Referenced by the following interfaces: ModifyLicenseUnBinds

name	required	NULL allowed	type	description
ErrMsg	yes	no	String	Cause of failure. Example: Insufficient unbinding attempts
Quuid	yes	no	String	UUID of the server. Example: 91bb5a8f-f5bc-4cf9-8253-d273fe5aa484

BashPolicy

Anti-high-risk command policy.

Referenced by the following interfaces: DescribeBashPolicies, ModifyBashPolicy

name	required	NULL allowed	type	description
BashAction	yes	no	Int64	0: alarming. 1: allowlisting. 2: blocking. Example: 1
Category	no	no	Int64	Policy type. 0: system policy. 1: custom policy. Example: 1
CreateTime	no	no	String	Creation time. Example: 2020-12-12 00:00:00
DealChildEvents	no	yes	Int64	Whether to add previous events to the allowlist. 0: no. 1: yes. Example: 1
Descript	no	yes	String	Policy description. Example: System rule (standard)
Enable	yes	no	Int64	1: valid. 0: invalid. Example: 0
EventId	no	yes	Int64	ID of the event, which must be passed in when you add the event to the allowlist. Example: 1
Id	no	no	Int64	Policy ID. Example: 1
Level	yes	no	Int64	Risk severity. 0: no risk. 1: high. 2: medium. 3: low. Example: 1
ModifyTime	no	no	String	Modification time. Example: 2020-12-12 00:00:00
Name	yes	no	String	Policy name. Example: policy
Quuids	no	yes	Array of String	QUUIDs of the servers on which the policy becomes invalid. Example: ["d99a1b46-cc2d-4633-a11f-4a7663d25ay"]
Rule	yes	no	String	Regular expression, encrypted with Base64. This field is deprecated. If you enter this parameter, it will be automatically replaced with Rules.Process.CmdLine. Example: L2RhdGEvZGlyZmFtZS8=
Rules	no	yes	PolicyRules	Rule expression Example:View
Scope	yes	no	Int64	Effective scope. 0: a set of QUUIDs. 1: all servers with CWP Pro, including servers with CWP Ultimate. 1: all servers with CWP Ultimate. 3: all servers. Example: 1
Uuids	no	no	Array of String	This is parameter is used for compatibility with the previous version. Example: ["d99a1b46-cc2d-4633-a11f-4a7663d25ay"]
White	yes	no	Int64	0: blocklist. 1: allowlist. Example: 1

LogInfo

Log details

Referenced by the following interfaces: SearchLog

name	required	NULL allowed	type	description
Content	yes	no	String	Serialized string of the log data in the JSON format. Example: {"quuid":"fb934eba-1f06-491a-a9c6-ca679d733dd","recv_time":"1730423894","hostip":"192.168.11.19","count":"1","pid":"5820","appid":"1258352045","cls_event_type":"dns_log"}
FileName	yes	no	String	Name of the log file. Example: fileNameTest.txt
Source	yes	no	String	Source IP address of the log. Example: 1.1.1.1
TimeStamp	yes	no	Int64	Log timestamp. Unit: ms. Example: 0

ProtectDirRelatedServer

Information about server associations with protected directories.

Referenced by the following interfaces: DescribeProtectDirRelatedServer

name	required	NULL allowed	type	description
Authorization	no	no	Bool	Whether the server is associated with a license. Example: true
AutoRestoreSwitchStatus	no	no	Uint64	Automatic recovery switch. Example: 0
Exception	no	no	Uint64	Exception status. Example: 0
ExceptionMessage	no	no	String	Exception message. Example: Starting
HostIp	no	no	String	Server IP. Example: 192.168.0.204
HostName	no	no	String	Server name. Example: redis_node_cvm
Id	no	no	String	Unique ID. Example: 6961
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information Example:View
MachineOs	no	no	String	Operating system of the server. Example: CentOS 192.168.0.204
Progress	no	no	Uint64	Progress. Example: 0
ProtectStatus	no	no	Uint64	Protection status. Example: 6
ProtectSwitch	no	no	Uint64	Protection status. Example: 0
Quuid	no	no	String	Unique ID of the server. Example: 8ce366dc-624e-429c-a8da-5ab870ecayay
RelateDirNum	no	no	Uint64	Number of associated directories. Example: 0

LicenseOrder

License order information.

Referenced by the following interfaces: DescribeImportMachineInfo, DescribeMachinesSimple

name	required	NULL allowed	type	description
LicenseId	yes	no	Uint64	License ID. Example: 667445
LicenseType	yes	no	Uint64	License type. 0: Pro Edition license; 5: Ultimate Edition license. Example: 1
ResourceId	yes	no	String	Resource ID. Example: resource_id
SourceType	yes	no	Uint64	Order type. 0: default billing order; 1: trial order; 2: gift; 3: experience. Example: 0
Status	yes	no	Uint64	Status of the resource in the license order. 1: normal; 2: isolated; 3: terminated. Example: 1

AgentInstallTaskResult

Agent installation task details in the Security Center.

Referenced by the following interfaces: DescribeAgentInstallTaskResult

name	required	NULL allowed	type	description
Assets	no	yes	Array of AgentInstallResult	All Instances Example:View
CreateTime	no	yes	String	Task Start Time Example: 2020-02-01 12:00:00
Id	no	yes	Int64	Task ID Example: 1

AssetSystemPackageInfo

System installation package information in the asset management module.

Referenced by the following interfaces: DescribeAssetSystemPackageList

name	required	NULL allowed	type	description
Desc	yes	no	String	Description. Example: utils
FirstTime	yes	no	String	First collection time. Example: 2022-07-15 11:27:01
InstallTime	yes	no	String	Installation time. Example: 2024-10-23 14:17:00
IsNew	yes	no	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	yes	no	String	IP address of the server. Example: 1.1.1.1
MachineName	yes	no	String	Server name. Example: redis_node_cvm
Name	yes	no	String	Package name. Example: libxrdev
OsInfo	yes	no	String	Operating system. Example: Centos
Quuid	no	yes	String	Server ID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Type	yes	no	String	package type (rpm dpkg java system) Example: rpm
UpdateTime	yes	yes	String	Data update time. Example: 2011-11-11 12:12:12
Uuid	no	yes	String	Agent Id Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Version	yes	no	String	Version. Example: 1.0.1

AssetDatabaseDetail

Database information in the asset management module.

Referenced by the following interfaces: DescribeAssetDatabaseInfo

name	required	NULL allowed	type	description
BinPath	yes	no	String	Binary path. Example: /usr/local/bin
ConfigPath	yes	no	String	Path of the configuration file. Example: /etc/mysqld
DataPath	yes	no	String	The data path. Example: /data/mysql
ErrorLogPath	yes	no	String	Path of the error log. Example: /var/log
Ip	yes	no	String	Binds the IP address. Example: 0.0.0.0

name	required	NULL allowed	type	description
LogPath	yes	no	String	Path of the log file. Example: /data/log
MachineIp	yes	no	String	Private IP address of the server. Example: 10.0.0.11
MachineWanIp	yes	no	String	Public IP address of the server. Example: 1.1.1.1
Name	yes	no	String	Database name. Example: MySQL
OsInfo	yes	no	String	OS information. Example: Centos 64Bit
Param	yes	no	String	Boot parameters. Example: --configsvr --port 27019 --keyFile /etc/mongodb/key --dbpath /data/db --replSet d1j49fdz --wiredTigerCacheSizeGB 0.43 --maxConns 10000 --auth --bind_ip_all
Permission	yes	no	String	Running permissions. Example: polkitd
PluginPath	yes	no	String	Path of the plug-in. Example: /etc/mysql
Port	yes	no	String	Listening port. Example: 3306
Proto	yes	no	String	Protocol. Example: tcp
Quuid	yes	no	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
UpdateTime	yes	yes	String	Data update time. Example: 2011-11-11 12:12:12
User	yes	no	String	Run user. Example: nginx
Uuid	yes	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Version	yes	no	String	Version. Example: 5.6.7

BaselineItemsCategory

Baseline detection item category tree structure.

Referenced by the following interfaces: DescribeBaselineItemInfo

name	required	NULL allowed	type	description
CategoryCount	no	yes	Int64	Number of baseline detection item subcategories. Example: 53
CategoryLists	no	yes	Array of BaselineCategory	Baseline detection item subcategory list. ExampleView
ParentCategoryId	no	yes	Int64	Parent category ID of a baseline detection item. Example: 1
ParentCategoryName	no	yes	String	Parent category name of a baseline detection item. Example: Weak password

RansomDefenseEvent

Prevention of Ransomware, Bait and Tamper Events

Referenced by the following interfaces: DescribeRansomDefenseEventsList

name	required	NULL allowed	type	description
BaitFilePath	yes	no	String	Tampered File Path Example: /var/www/index.html
CreateTime	yes	no	String	Event Sending Time Example: 2024-10-30 09:12:21
FileMd5	yes	no	String	Malicious File MD5 Example: 708cae4c8154c3ded4208da2289ad4e
FilePath	yes	no	String	Malicious File Path Example: /tmp/any
FileSize	yes	no	Uint64	Malicious File Size Example: 1
HostIp	yes	no	String	Public IP address of the server. Example: 10.0.0.1
HostName	yes	no	String	Server name. Example: redis_node_cvm
Id	yes	no	Uint64	Event ID. Example: 1
InstanceId	yes	no	String	CVM Instance ID Example: ins-eubsdt5
ModifyTime	yes	no	String	Event Modification Event Example: 2024-10-30 09:12:21
Pid	yes	no	Uint64	Malicious Process ID Example: 1
PidParam	yes	no	String	Malicious Process Parameters Example: bash -c echo "C:\zip data any" > > /home/yjfile/121hc3h.doc ayay
ProcessStartTime	yes	no	String	Process start time Example: 2024-10-30 09:12:21
PsTree	yes	no	String	Process Tree Base64 Json Example: W3sicGlkIjoxMjI3NCwiZXhlIjoiL3Vzci9kaW4i*
Quuid	yes	no	String	CVM UUID Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
SnapshotNum	yes	no	Uint64	Number of Snapshot Backups Owned by the Host Example: 1
Status	yes	no	Uint64	Event Status: 0-Pending, 1-Processed, 2-Trusted, 3-In Process, 4-Backup Resumed Example: 1
StrategyId	yes	no	Uint64	Policy ID. Example: 1
StrategyName	yes	no	String	Policy name. Example: anyname
Type	yes	no	Uint64	Event Type: 0 Encrypted Ransom, 1 File Tampering Example: 0
Uuid	yes	no	String	Host UUID. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
WanIp	yes	no	String	Host Intranet IP Example: 10.0.0.1

RansomDefenseRollbackTask

Anti-Ransomware Rollback Task

Referenced by the following interfaces: DescribeRansomDefenseRollBackTaskList

name	required	NULL allowed	type	description
BackupTime	yes	no	String	Snapshot Time Example: 2022-11-11 11:00:00
CreateTime	yes	no	String	Operation Time Example: 2022-11-11 11:00:00
Disks	yes	no	String	Hard drive ID list, separated by semicolons (;) Example: disk-dsdsdsdsdisk-dsads
Id	yes	no	Uint64	Task ID Example: 1
MachineName	yes	no	String	Server name. Example: redis_node_cvm
ModifyTime	yes	no	String	Status!=0 indicates the completion time. Example: 2022-11-11 11:00:00
Quuid	yes	no	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
RegionInfo	yes	no	RegionInfo	Information on availability zones. ExampleView
Status	yes	no	Uint64	Rollback Task Status: 0 - In Progress, 1 - Succeeded, 2 - Failed Example: 1
Uuid	yes	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

AssetWebServiceBaseInfo

Web service information in the asset management module.

Referenced by the following interfaces: DescribeAssetWebServiceInfoList

name	required	NULL allowed	type	description
BinPath	no	no	String	Binary path. Example: /usr/bin
ConfigPath	no	no	String	The configuration file path. Example: /root
Desc	no	no	String	Description. Example: 1
FirstTime	no	no	String	First collection time. Example: 2022-07-15 11:27:01
Id	no	no	String	ID of the web service. Example: 1001
InstallPath	no	no	String	Installation path. Example: /root
IsNew	no	no	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information ExampleView
MachineIp	no	no	String	Private IP address of the server. Example: 10.0.0.11
MachineName	no	no	String	Server name. Example: agentinstance
MachineWanIp	no	no	String	Public IP address of the server. Example: 1.1.1.1
Name	no	no	String	Service Name Example: Nginx
OsInfo	no	no	String	OS information. Example: Centos 64Bit
ProcessCount	no	no	Uint64	Number of associated processes. Example: 1
ProjectId	no	no	Uint64	ID of the project to which the server belongs. Example: 1
Quuid	no	no	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Tag	no	yes	Array of MachineTag	Server tags. ExampleView
UpdateTime	no	yes	String	Data update time. Example: 2011-11-11 12:12:12
User	no	no	String	User who triggers initialization. Example: root
Uuid	no	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

name	required	NULL allowed	type	description
Version	no	no	String	Version. Example: 1.0.1

ProtectHostConfig

Protected server information.

Referenced by the following interfaces: CreateProtectServer, ModifyWebPageProtectDir

name	required	NULL allowed	type	description
AutoRecovery	yes	no	Uint64	Status of automatic recovery. 0: disabled. 1: enabled. Example: 0
ProtectSwitch	yes	no	Uint64	Protection status. 0: disabled. 1: enabled. Example: 0
Quuid	yes	no	String	Unique ID of the server. Example: 15c76928-e4e1-4f6d-8a2a-46c7de78asay

MachineFileTamperRule

Details of the core file monitoring rule associated with specified servers.

Referenced by the following interfaces: DescribeMachineFileTamperRules

name	required	NULL allowed	type	description
Id	yes	no	Uint64	The unique ID of the user. Example: 11
Name	yes	yes	String	Rule Name Example: Deny Access
Rule	yes	no	Array of FileTamperRule	Rule. Example:View
RuleCategory	yes	no	Uint64	Rule type. 0: system rule. 1: custom rule. Example: 1

BanWhiteList

Blocklist rules.

Referenced by the following interfaces: CreateBanWhiteList, ModifyBanWhiteList

name	required	NULL allowed	type	description
CreateTime	no	no	Datetime	Time when the blocklist was created. Example: 2021-01-01 00:00:00
Id	no	no	String	Allowlist ID. Example: id_10001
IsGlobal	no	yes	Bool	Whether the blocklist is global. Example: false
ModifyTime	no	no	Datetime	Time when the blocklist was modified. Example: 2021-01-01 00:00:00
Quuids	no	yes	Array of String	QUUIDs of the servers for which the blocklist is configured. Example: ["1ce68339-8828-4571-b358-d5b1b1b4e4e9"]
Remark	no	no	String	Alias of the blocklist. Example: Alias
Srcip	no	no	String	Source IP address in the blocklist. Example: 1.1.1.1
Uuid	no	yes	String	UUID of the server for which the blocklist is configured. Example: 1ce68339-8828-4571-b358-d5b1b1b4e4e9

Strategy

Information about a custom baseline security policy.

Referenced by the following interfaces: DescribeBaselineStrategyList

name	required	NULL allowed	type	description
CategoryIds	yes	yes	String	Baseline ID. Example: 1
Enabled	yes	yes	Uint64	Whether it is available. Example: 1
HostCount	yes	yes	Uint64	Number of hosts. Example: 42
IsDefault	yes	yes	Uint64	Specifies whether to use a default policy. Example: 0
PassRate	yes	yes	Uint64	Pass rate. Example: 100
RuleCount	yes	yes	Uint64	Total number of baseline check items. Example: 9
ScanAt	yes	yes	String	Scan time. Example: 01:35:30
ScanCycle	yes	yes	Uint64	Scan cycle. Example: 7
StrategyId	yes	yes	Uint64	Policy ID. Example: 1089429
StrategyName	yes	yes	String	Policy name. Example: check_redis_node

OrderData

Order Parameters

Referenced by the following interfaces: ModifyOrder

name	required	NULL allowed	type	description
AutoRenewFlag	no	yes	Uint64	Auto-renewal flag. 0: Disabled by default (auto-renewal available for key accounts). 1: Automatically renew. 2: Manually set to not automatically renew (auto-renewal not available for key accounts). Example: 1
InquireKey	yes	yes	String	Billing item sc_ Example: sv_yunjing_se_x
InquireNum	no	yes	Uint64	Purchase quantity, with a maximum value of 99999. Example: 1
NewConfig	no	yes	OrderModifyConfig	New order configuration, which is required for configuration adjustment. Example:View
OldConfig	no	yes	OrderModifyConfig	Old order configuration, which is required for configuration adjustment. Example:View
PayMode	yes	yes	Uint64	Billing mode. 0: pay-as-you-go, 1: prepaid (monthly subscription). Example: 1
ProjectID	no	yes	Uint64	Project ID. Example: 1
RegionID	yes	yes	Uint64	Region ID. Example: 1
RenewConfig	no	yes	OrderRenewConfig	Renewal configuration parameter. Example:View
ResourceId	no	yes	String	Resource ID. Example: fgtw124qerg1423221dsa231
SubProductCode	yes	yes	String	Subproduct SP_ Example: sp_yunjing_0014
Tags	no	yes	Array of Tags	Cloud tag, which is required when the tag needs to be bound. Example:View
TimeSpan	no	yes	Uint64	Purchase duration. For new purchase and renewal orders, it is an int. It is not required for configuration adjustment. Example: 1
TimeUnit	no	yes	String	Purchase Time Unit. Year-y, Month-m, Day-d, Time-h, Minute-M, Second-s, No Billing Cycle-p. Example: 2020-02-01 12:00:00
ZoneID	yes	yes	Uint64	Zone ID Example: 1

CommandLine

Command line content.

Referenced by the following interfaces: CheckBashPolicyParams, DescribeBashPolicies, ModifyBashPolicy

name	required	NULL allowed	type	description
Cmdline	no	yes	String	Command line, which needs to be encrypted using Base64. Example: c2lgcmVlakMuc2g=
Exe	no	yes	String	Path, which needs to be encrypted using Base64. Example: L2RhdGEvZGlybmFtZS8=

EffectiveMachineInfo

Server information in a batch import operation.

Referenced by the following interfaces: DescribeImportMachineInfo

name	required	NULL allowed	type	description
CloudFrom	no	yes	Int64	CVM source. Example: 0
CloudTags	no	yes	Array of Tags	Cloud tag information. Example:View
InstanceID	no	yes	String	Machine Instance ID Example: ins-sdsds
KernelVersion	no	yes	String	Kernel version. Example: 3.5
LicenseOrder	no	yes	LicenseOrder	License order object. Example:View
MachineName	no	yes	String	The instance name Example: redis_node_cvm
MachinePrivateIp	no	yes	String	Private IP address of the server. Example: 1.2.3.4
MachinePublicIp	no	yes	String	Public IP address of the server. Example: 1.2.3.4
MachineStatus	no	yes	String	Connection status. Valid values: OFFLINE and ONLINE. Example: OFFLINE
MachineTag	no	yes	Array of MachineTag	Server tag. Example:View
Quuid	no	yes	String	QUUID of the server. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
Uuid	no	yes	String	Host UUID. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
VulNum	no	yes	Uint64	Number of vulnerabilities. Example: 1

VulLevelInfo

Vulnerability count distribution statistics based on severity levels.

Referenced by the following interfaces: DescribeVulLevelCount

name	required	NULL allowed	type	description
Count	yes	no	Uint64	Total number. Example: 100

name	required	NULL allowed	type	description
VulLevel	yes	no	Uint64	Risk severity. 1: low. 2: medium. 3: high. 4: critical. Example: 1

BaselineRuleInfo

Baseline check item information.

Referenced by the following interfaces: DescribeBaselineRule

name	required	NULL allowed	type	description
Description	yes	no	String	Description of the check item. Example: Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.
EventId	yes	no	Uint64	Unique event ID. Example: 3634
FixMessage	yes	no	String	Fix suggestions. Example: Set the /etc/audit/auditd.conf parameter according to the site policy:
LastScanAt	yes	no	String	Last detection time. Example: 2024-11-04 09:57:28
Level	yes	no	Uint64	Baseline risk level. 0: low; 1: medium; 2: high; 3: critical. Example: 3
RuleId	yes	no	Uint64	ID of the check item. Example: 1026
RuleName	yes	no	String	Detection item name. Example: Ensure that the audit log storage size is configured for low risks.
RuleRemark	yes	no	String	Reason description. Example: Log remark
Status	yes	no	Uint64	State. Example: 0
Uuid	yes	no	String	Unique user ID. Example: df131b24-8528-4809-9d07-a9e4d58ad566

CKafkaRouteInfo

CKafka domain name information.

Referenced by the following interfaces: DescribeLogDeliveryKafkaOptions

name	required	NULL allowed	type	description
AccessType	yes	no	Int64	Access type. 0: PLAINTEXT (plaintext, without containing user information, supported by the earlier versions and community edition). 1: SASL_PLAINTEXT (plaintext, with SASL login authentication at the beginning of data transmission, only supported by the community edition). 2: SSL (SSL-based encrypted communication, without containing user information, supported by the earlier versions and community edition). 3: SASL_SSL (SSL-based encrypted communication, with SASL login authentication at the beginning of data transmission, only supported by the community edition). Example: 1
Domain	yes	no	String	Domain name. Example: www.a.com
DomainPort	yes	no	Uint64	Domain name and port. Example: 80
RouteID	yes	no	Int64	Route ID. Example: 1
Vip	yes	no	String	Virtual IP address. Example: 1.1.1.1
VipType	yes	no	Int64	Virtual IP address type. 1: public network TGW; 2: basic network; 3: VPC; 4: supporting network (standard edition); 5: SSL public network access; 6: VPC in the bare metal environment; 7: supporting network (Pro). Example: 1

NetAttackEvent

Referenced by the following interfaces: DescribeAttackEvents

name	required	NULL allowed	type	description
Count	no	yes	Uint64	Attacks Example: 1
DstPort	no	yes	Uint64	Target port. Example: 443
Id	no	yes	Uint64	Log ID. Example: 49992719
Location	no	yes	String	Source location Example: location1-location2
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information ExampleView
MergeTime	no	yes	String	Attack time. Example: 2021-02-01 12:00:00
New	no	yes	Bool	Whether to add new hosts today Example: false
PayVersion	no	yes	Uint64	Machine payment edition. 0: Basic Edition; 1: Professional Edition; 2: Premium Edition; 3: General Discount Edition Example: 1
Quuid	no	yes	String	CVM UUID Example: ebc62d3a-a4de-46ad-a0d5-b94cb8fdaeay
SrcIP	no	yes	String	Source IP address. Example: 192.168.0.204
Status	no	yes	Uint64	Processing Status: 0 Pending, 1 Processed, 2 Allowlisted, 3 Ignored, 4 Deleted, 5: Defense Enabled. Example: 0
Type	no	yes	Uint64	Attack Status: 0: Attack Attempt 1: Confirmed Attack (Successful Attack). Example: 0
Uuid	no	yes	String	Client ID Example: ebc62d3a-a4de-46ad-a0d5-b94cb8fdaeay
VulDefenceStatus	no	yes	Uint64	Whether to enable vulnerability defense: 0 - No, 1 - Yes Example: 0
VulId	no	yes	Uint64	Vulnerability ID. Example: 100377
VulName	no	yes	String	Vulnerability name. Example: Apache HTTP/2 DoS vulnerability (CVE-2023-44487)
VulSupportDefense	no	yes	Uint64	Whether vulnerabilities support defense. 0: No 1: Yes Example: 0

AssetWebAppPluginInfo

Web application plug-in details in the asset management module.

Referenced by the following interfaces: DescribeAssetWebAppPluginList

name	required	NULL allowed	type	description
Desc	yes	no	String	Description. Example: memo
Link	yes	no	String	Upload link. Example: /usr/bin/name
Name	yes	no	String	Name. Example: any-app
Version	yes	no	String	Version. Example: 1.0.0.1

ScreenRegionInfo

Region information.

Referenced by the following interfaces: DescribeScreenMachineRegions

name	required	NULL allowed	type	description
Region	yes	no	String	Region. Example: ap-region1
RegionCode	yes	no	String	Region code, such as gz, sh, bj. Example: gz
RegionId	yes	no	Uint64	Region ID. Example: 1
RegionName	yes	no	String	Region name Example: region1
RegionNameEn	yes	no	String	English name of the region. Example: ap-region1

RansomDefenseBackup

Host Snapshot Backup List

Referenced by the following interfaces: DescribeRansomDefenseBackupList

name	required	NULL allowed	type	description
BackupStatus	yes	no	Uint64	Backup Status: 0 - Backing up, 1 - Normal, 2, 3 - Failed, 4 - Snapshot expired, 9 - Snapshot deleted Example: 1
BackupTime	yes	no	String	Backup time Example: 2022-11-11 11:00:00
DiskCount	yes	no	Uint64	Backup Disk Quantity Example: 1
Disks	yes	no	String	Hard Disk Information, separated by semicolons (;). Example: id1
EventStatus	yes	no	Uint64	Ransom Status: 0 - No Alarm, 1 - Alarm Present Example: 1
SnapshotIds	yes	no	String	Snapshot List, separated by semicolons (;) Example: id1;id2
StrategyId	yes	no	Uint64	Policy ID. Example: 1
StrategyName	yes	no	String	Policy name. Example: tt1
StrategyStatus	yes	no	Uint64	Policy Status: 0 Disabled, 1 Enabled, 9 Deleted Example: 1

RegionInfo

Region information.

Referenced by the following interfaces: DescribeMachineList, DescribeMachineRegionList, DescribeMachineRegions, DescribeMachines, DescribeMachinesSimple, DescribeRansomDefenseMachineList, DescribeRansomDefenseRollBackTaskList, DescribeRansomDefenseStrategyMachines

name	required	NULL allowed	type	description
Region	yes	no	String	Region. Example: region1
RegionCode	yes	no	String	Region code, such as gz, sh, bj. Example: gz
RegionId	yes	no	Uint64	Region ID. Example: 1
RegionName	yes	no	String	Region name Example: region1
RegionNameEn	yes	no	String	English name of the region. Example: ap-region1

VulDefencePluginDetail

Status of the single-process exploit prevention plug-in.

Referenced by the following interfaces: DescribeVulDefencePluginDetail

name	required	NULL allowed	type	description
ErrorLog	yes	no	String	Error log. Example: [Error] Injection failed.
InjectLog	yes	no	String	Injection log. Example: [Info] Injection is successful.
MainClass	yes	no	String	Name of the main class of the injection process. Example: Main.class
Pid	yes	no	Int64	ID of the injection process. Example: 1
Status	yes	no	Int64	Plug-in status. 0: injecting. 1: injected successfully. 2: plug-in timeout. 3: plug-in exit. 4: injection failed. 5: logically deleted. Example: 2

MaCustomPolicyWorkload

Referenced by the following interfaces: DescribeMaCustomPolicyList, ModifyMaCustomPolicy

name	required	NULL allowed	type	description
Id	yes	yes	Uint64	Workload ID. Example: 1
Name	yes	yes	String	Workload name. Example: workload1
Type	yes	yes	Uint64	Workload type. • 0: Server workload • 1: Pod workload Example: 1

ExportInfo

Log download task list.

Referenced by the following interfaces: DescribeLogExports

name	required	NULL allowed	type	description
CosPath	yes	no	String	Log export path. Example: /tmp/data/
Count	yes	no	Int64	Number of log entries to export. Example: 12
CreateTime	yes	no	String	Time when the log export task was created. Example: 2021-02-01 12:00:00
EndTime	yes	no	Int64	End of the time range to export log entries. The value is a UINX timestamp in milliseconds. Example: 0
ExportId	yes	no	String	ID of the log export task. Example: export-d3ef1b2c-64f6-4193-b251-e583a810adeay
FileName	yes	no	String	Name of the exported log file. Example: fieldName.txt
FileSize	yes	no	Int64	Size of the log file. Example: 0
Format	yes	no	String	Format in which to export log entries. Example: json
Order	yes	no	String	Exported log sorting by time. Example: desc
Query	yes	no	String	Query statement for the log export. Example: dev
StartTime	yes	no	Int64	Beginning of the time range to export log entries. The value is a UINX timestamp in milliseconds. Example: 0
Status	yes	no	String	Log download status. Processing: the export task is in progress. Complete: the export task is complete. Failed: the export task has failed. Expired: the exported log file has expired (valid within 3 days). Example: Complete

BruteAttackRuleList

List of rules for determining a brute force attack.

Referenced by the following interfaces: DescribeBruteAttackRules

name	required	NULL allowed	type	description
Enable	yes	no	Bool	Whether the rule is empty. If yes, the default rule is populated. Example: true
LoginFailTimes	yes	no	Uint64	Number of failed brute force attack events. Example: 5
LoginFailTimesDefault	yes	no	Uint64	Number of failed brute force attack events. This parameter applies to the default rule. Example: 10
TimeRange	yes	no	Uint64	Time period during which brute-force attack events occurred. Unit: seconds. Example: 5
TimeRangeDefault	yes	no	Uint64	Time period during which brute force attack events occur. Unit: seconds. This parameter applies to the default rule. Example: 1

JavaMemShellPluginSetting

Configuration of the Java memory trojan plug-in.

Referenced by the following interfaces: DescribeJavaMemShellPluginList

name	required	NULL allowed	type	description
Alias	yes	no	String	Server name. Example: redis_node_cvm
CreateTime	yes	no	String	Creation time. Example: 2021-01-20 16:17:11
Exception	yes	no	Uint64	Whether the plug-in is abnormal. 0: normal. 1: exceptional. Example: 0
HostIp	yes	no	String	Server IP address. Example: 192.168.255.10
JavaShellStatus	yes	no	Uint64	Status of the Java shell plug-in. 0: disabled. 1: enabled. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information Example:View
ModifyTime	yes	no	String	Modification time. Example: 2021-01-20 16:17:1
Quuid	yes	no	String	QUUID of the container. Example: e1f081aa-7777-4fdf-a2f7-88f3faa3d302
Uuid	no	yes	String	UUID of the server. Example: e1f081aa-7777-4fdf-a2f7-88f3faa3d302

WarningObject

Parameters for updating or inserting alarms.

Referenced by the following interfaces: DescribeSaveOrUpdateWarnings, ModifyWarningSetting

name	required	NULL allowed	type	description
BeginTime	no	no	String	Start time. Format: HH:mm Example: 19:17:28
ControlBits	no	no	String	Binary control bit of the vulnerability severity. Each bit corresponds to the enabling status of each vulnerability severity: low, medium, and high (0: disabled. 1: enabled). For example, a value of 101 indicates that both the low and high severities are selected, and a value of 01 indicates that no alarms are generated for suspicious events and alarms are generated for high-risk events (login audits). Example: 101
DisablePhoneWarning	no	no	Uint64	1: disables alarming. 0: enables alarming. Example: 1
EndTime	no	no	String	End time. Format: HH:mm Example: 19:17
HostRange	no	yes	Int64	Alarm host range type: 0: all hosts; 1: by project; 2: by cloud tag; 3: by CWP tag; 4: custom hosts. Example: 0
Type	no	no	Uint64	Event Alarm Type. 1: Offline; 2: Trojan; 3: Exceptional login; 4: Brute force; 5: Vulnerability (split into four types ranging from 9 to 12); 6: High-risk command; 7: Reverse sell; 8: Local privilege escalation;. 9: System component vulnerabilities; 10: Web application vulnerabilities; 11: Emergency vulnerabilities; 12: Security baseline; 14: Malicious request; 15: Network attack; 16: Windows system vulnerabilities; 17: Linux software vulnerabilities Example: 2

LoginWhiteLists

Login allowlist

Referenced by the following interfaces: DescribeLoginWhiteList

name	required	NULL allowed	type	description
CreateTime	yes	no	Datetime	Time when the blocklist was created. Example: 2020-10-01 00:00:01
EndTime	yes	no	String	End time. Example: 2020-10-01 00:00:02
HostIp	yes	no	String	Server IP address. Example: 10.20.30.40
Id	yes	no	Uint64	The record ID. Example: 1
IsGlobal	yes	no	Bool	Whether it is a global rule. Example: false
MachineName	yes	no	String	The host name. Example: stone
ModifyTime	yes	no	Datetime	Time when the blocklist was modified. Example: 2020-10-01 00:00:02
Places	yes	no	Array of Place	Region of the allowlist. Example:View
SrcIp	yes	no	String	IP addresses in the allowlist. Multiple IP addresses are separated with commas (,). Example: 1.2.2.3
StartTime	yes	no	String	The start time. Example: 2020-10-01 00:00:01
UserName	yes	no	String	Users in the allowlist. Separate multiple usernames with commas (,). Example: user
Uuid	yes	no	String	UUID of the CWP agent. Example: 8c09e1b1-5611-45b1-9c02-737996011b81

DuplicateHosts

Duplicated servers during batching adding servers to the allowlist.

Referenced by the following interfaces: AddLoginWhiteLists, CreateBanWhiteList

name	required	NULL allowed	type	description
Id	yes	no	Uint64	Id Example: 1
Quuid	yes	yes	String	Quuid Example: 0590bcab-726c-4ea4-8109-bcd03d559bf7
Uuid	yes	yes	String	Uuid Example: 0590bcab-726c-4ea4-8109-bcd03d559bf7

ScreenAttackHotspot

Attack hotspot on the entire network in the dashboard.

Referenced by the following interfaces: DescribeScreenAttackHotspot

name	required	NULL allowed	type	description
CreatedTime	yes	no	String	Time. Example: 2021-03-30
DstIp	yes	no	String	IP address of the victim server. Example: 12.23.252.2

name	required	NULL allowed	type	description
EventName	yes	no	String	Event name. Example: Command injection attack
Region	yes	no	String	Region. Example: region1
SrcIp	yes	no	String	IP address of the attacker. Example: 12.23.212.2

VulInfoHostInfo

Pop-up information displayed for batch vulnerability fixing.

Referenced by the following interfaces: DescribeCanFixVulMachine

name	required	NULL allowed	type	description
HostIp	yes	yes	String	IP address of the server. Example: 10.13.45.12
HostName	yes	yes	String	Server name. Example: redis_node_cvm
InstanceId	yes	yes	String	Instance ID of the server. Example: ins-dhuahsd
IsSupportAutoFix	yes	yes	Uint64	0: the vulnerability cannot be automatically fixed. 1: the vulnerability can be automatically fixed. 2: the agent is offline. 3: the server is not associated with a CWP Ultimate license, and the vulnerability can only be manually fixed. 4: automatic vulnerability fixing is not supported for this device model. 5: the vulnerability is being fixed. 6: the vulnerability has been fixed. 7: the vulnerability is being checked. 10: the vulnerability has failed to be fixed. 10: the vulnerability has been ignored. 11: or Example: 1
Quuid	yes	yes	String	QUUID of the server. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
Tags	yes	yes	Array of String	Server tags. Example: ["tag1","tag2"]
Uuid	yes	yes	String	Host UUID. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0

RansomDefenseStrategyDetail

Tag information of a server returned from the server list query API.

Referenced by the following interfaces: DescribeRansomDefenseStrategyDetail

name	required	NULL allowed	type	description
BackupType	yes	yes	Uint64	Backup pattern: 0 weekly, 1 daily Example: 0
CreateTime	yes	yes	String	Creation time. Example: 2022-12-12 12:12:12
Description	yes	yes	String	Policy Remarks Example: subtitle
EventCount	yes	yes	Uint64	Policy Associated Event Count Example: 11
ExcludeDir	yes	yes	String	Includes directories, separated by semicolons (;). Example: /usr
Hour	yes	no	String	Backup Execution Time Point (0-23): 11:00; 12:00 Example: 11:00
Id	yes	no	Int64	Policy ID. Example: 666
IncludeDir	yes	yes	String	Includes directories, separated by semicolons (;). Example: /root
IsAll	yes	no	Uint64	Whether it takes effect for all hosts. Example: 1
MachineCount	yes	yes	Uint64	Number of Bound Machines Example: 12
ModifyTime	yes	yes	String	The point in time when the namespace was last modified. Example: 2022-12-12 12:12:12
Name	yes	no	String	Policy name. Example: policy-1
SaveDay	yes	no	Uint64	Storage Days, 0 for Permanent Example: 5
Status	yes	no	Uint64	Enabling Status: 0 Disabled, 1 Enabled. Example: 1
Uin	yes	yes	String	Operating UIN Example: 666
Weekday	yes	yes	String	Backup days in a week (1-7): 1; 2; 3; 4. Example: 1;2;3

MalwareInfo

Malicious file details.

Referenced by the following interfaces: DescribeMalwareInfo

name	required	NULL allowed	type	description
Breadth	no	yes	String	Width of the impact. This parameter is currently unavailable. Example: Breadth
CheckPlatform	no	yes	String	Trojan detection platforms. Multiple platforms are separated with commas (,). 1: cloud scanning and cleaning engine. 2: TAV. 3: binaryAI. 4: suspicious behavior. 5: threat intelligence. Example: 1
CreateTime	no	no	String	First time when it was found. Example: 2021-04-26 15:19:04
FileCreateTime	no	no	String	Time when the file was first run. Example: 2021-04-26 15:19:04
FileExists	no	yes	Bool	Whether any Trojan file exists. Example: true
FileModifierTime	no	no	String	Time when the file was last run. Example: 2021-04-26 15:19:04
FileName	no	no	String	The file name. Example: FileName
FilePath	no	no	String	File path. Example: /usr/local/services/tmgins_1_0_0-1.0/lib/luajit/lib
FileSize	no	no	Int64	File size. Example: 1024
FirstDetectionMethod	no	yes	Uint64	Method by which the file was detected for the first time. 0: scanning; 1: real-time monitoring. Example: 0
HarmDescribe	no	no	String	Risk description. Example: This is a description.
Heat	no	yes	String	Query heat. This parameter is currently unavailable. Example: Heat
HostIp	no	no	String	Server IP. Example: 15.2.3.442
Id	no	no	Uint64	Unique ID. Example: 1
LatestScanTime	no	no	String	Last scan time. Example: 2021-04-26 15:19:04
Level	no	yes	Uint64	Risk severity. 0: informational. 1: low. 2: medium. 3: high. 4: critical. Example: 1
MD5	no	no	String	File MD5. Example: e10adc3949ba59abbe56e057f20f883e
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineStatus	no	yes	String	Connection status of the server. Valid values: OFFLINE and ONLINE. Example: OFFLINE
MachineWanIp	no	yes	String	Public IP. Example: 15.2.3.442
ModifyTime	no	yes	String	The point in time when the namespace was last modified. Example: 2021-04-26 15:19:04
ProcessExists	no	yes	Bool	Whether any Trojan process exists. Example: true
ProcessID	no	no	String	Process ID. Example: 116
ProcessName	no	no	String	Process name. Example: nginx
PsTree	no	yes	String	Process tree in the JSON format. pid: process ID. exe: file path. account: user group and user to which the process belongs. cmdline: command to be run. ssh_service: SSH service. ssh_sousrce: login source. Example: [{"pid":"13"}]
Reference	no	no	String	Reference link. Example: http://www.vojump.net/files/virus_analysis/virut%20botnet%20anal
References	no	yes	Array of String	Reference link. Example: ["https://domain.com"]
ServersName	no	no	String	Server name. Example: nginx
Status	no	yes	Uint64	Status. 4: to be handled. 5: trusted. 6: quarantined. Example: 1
StrFileAccessTime	no	yes	String	Last access time. Example: 2021-04-26 15:19:04
SuggestScheme	no	no	String	Suggestion scheme. Example: 1. Check for malicious processes and invalid ports, and delete suspicious startup items and scheduled tasks. 2. Isolate or delete relevant Trojan files.
Tags	no	no	Array of String	Tags. Example: ["tanat","wekk"]
Uuid	no	yes	String	Host UUID. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
VirusName	no	no	String	Virus name. Example: Linux.Trojan.Downloader.Snkl

AssetJarDetail

JAR package details in the asset management module.

Referenced by the following interfaces: DescribeAssetJarInfo

name	required	NULL allowed	type	description
MachineIp	yes	no	String	Server IP. Example: 10.0.0.11
MachineName	yes	no	String	Server name. Example: redis_node_cvm
Md5	yes	yes	String	MD5 value of the JAR package. Example: fc702c8398073ea35970449c2b894dae
Name	yes	no	String	Name. Example: com.apple.utils
OsInfo	yes	no	String	Operating system. Example: 1
Path	yes	no	String	Path Example: /root
Process	yes	yes	Array of AssetAppProcessInfo	List of referenced processes. Example:View
Status	yes	no	Uint64	Whether it can be executed. 0: unknown. 1: yes. 2: no. Example: 1
Type	yes	no	Int64	Type. 1: application program. 1: system library. 3: built-in library of a web service. 8: others. Example: 1
UpdateTime	yes	yes	String	Data update time. Example: 2011-11-11 12:12:12

name	required	NULL allowed	type	description
Version	yes	no	String	Version. Example: 1.0.0

VulFixStatusHostInfo

Vulnerability fixing details, including the fixing status of each vulnerability on each server.

Referenced by the following interfaces: DescribeVulFixStatus

name	required	NULL allowed	type	description
FailReason	yes	yes	String	Reason for the fix failure. Example: Fixing timeout
HostIp	yes	no	String	IP address of the server. Example: 10.13.45.12
HostName	yes	no	String	Server name. Example: redis_node_cvm
ModifyTime	yes	no	String	Time when it was fixed. Example: 2021-03-30 19:17:28
Quuid	yes	no	String	QUUID of the server. Example: e5b4724c-49af-46ab-bc84-cdbad97e7e0
Status	yes	no	Uint64	Status. 0: initial status. 1: task delivered (fixing). 2: completed (successful). 3: fix failed (failed). 4: fix failed due to the failure to create a snapshot (not fixed). Example: 1

VulDefenceEventDetail

Vulnerability details.

Referenced by the following interfaces: DescribeDefenceEventDetail

name	required	NULL allowed	type	description
Alias	no	no	String	Server name. Example: redis_node_cvm
City	no	no	String	City where the attack source IP address resides. Example: city1
Count	no	no	Int64	Number of occurrences of the event. Example: 1
CreateTime	no	no	String	Time when the event was created. Example: 2021-01-20 16:17:11
CveId	no	no	String	CVE ID. Example: cve-ay
Description	no	no	String	Description of the vulnerability. Example: Description
EventDetail	no	no	String	Event details related to the vulnerability ID in the JSON Array format. This parameter is available only for RASP. Example: [{ "name": "jndiurl", "value": "http://whoa
EventType	no	no	Uint64	0: attempted attack (available for WeDetect). 1: successful attack attempt (available for WeDetect). 2: RASP defense event. Example: 1
ExceptionPstree	no	no	String	Process tree of the server compromising event in the JSON format. This parameter is available only for WeDetect. Example: ppid ssh
Fix	no	no	String	Fix suggestions. Example: Suggestions
Id	no	no	Int64	ID of the vulnerability event. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information Example:View
MachineStatus	no	no	String	ONLINE OFFLINE Example: ONLINE
MainClass	no	no	String	Main class name of the associated process. Example: sfclass
MergeTime	no	no	String	Time when the event was updated. Example: 2021-01-20 16:17:11
NetworkPayload	no	no	String	Attack payload. Example: GET /$%7BClass.forName%22com.opensymphony.webwork.ServletActionContext%22).getMethod
Pid	no	no	Int64	ID of the associated process. Example: 116
PrivateIp	no	no	String	Private IP address. Example: 10.2.3.1
PublicIp	no	no	String	Public IP address. Example: 111.2.3.1
Quuid	no	no	String	QUUID of the server. Example: d92d723e-4aac-4f4a-bbf9-e5430e29d289
SourceIp	no	no	String	Attack source IP address. Example: 11.2.3.1
SourcePort	no	yes	Array of Uint64	Attack source port. Example: [1,3]
StackTrace	no	no	String	Stack information. This parameter is available only for RASP. Example: at org.javaui8
Status	no	no	Int64	Status. 0: to be handled. 1: prevented. 2: handled. 3: ignored. 4: deleted. Example: 1
VulName	no	no	String	Vulnerability name. Example: Vulnerability

ProtectMachineInfo

Licensed server information.

Referenced by the following interfaces: DescribeWebPageServiceInfo

name	required	NULL allowed	type	description
CreateTime	yes	no	String	Point in time when it was enabled. Example: 2020-11-21 15:16:00
ExpireTime	yes	no	String	The point in time when it expires. Example: 2020-11-21 15:16:00
HostIp	yes	no	String	Server IP address. Example: 10.0.1.92
HostName	yes	no	String	The instance name Example: host1

DefendAttackLog

Cyberattack log.

Referenced by the following interfaces: DescribeAttackLogs

name	required	NULL allowed	type	description
CreatedAt	no	no	String	Attack time. Example: 2020-01-01 00:00:00
DstIp	no	no	String	Target IP address. Example: 1.1.1.1
DstPort	no	no	Uint64	Target port. Example: 8080
HttpCgi	no	no	String	Attack description. Example: any attack msg
HttpContent	no	no	String	Attack content. Example: content
HttpMethod	no	no	String	Attack method. Example: POST
HttpParam	no	no	String	Attack parameter. Example: POST /demo3-1/baseServlet HTTP/1.1
Id	no	no	Uint64	Log ID. Example: 10001
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information Example:View
MachineIp	no	no	String	IP address of the target server. Example: 1.1.1.1
MachineName	no	no	String	Name of the target server. Example: 1.1.1.1
SrcIp	no	no	String	Source IP address. Example: 1.1.1.1
SrcPort	no	no	Uint64	Source port. Example: 32456
Uuid	no	no	String	Client ID Example: 93b5fa8f-f5bc-4cf9-8253-d2719e5aa484
VulType	no	no	String	Threat type. Example: tcp

PriceDetail

Quotation Parameters

Referenced by the following interfaces: DescribePrice

name	required	NULL allowed	type	description
GoodsCategoryId	yes	no	Uint64	Order Classification Example: 1
GoodsDetail	yes	no	String	Order Details Parameters Example: {"pid":1004928,"license":3,"productCode":"p_yunjing","subProductCode":"sp_yunjing_vip","w_yunjing_protection_vip":"3","timeSpan":1,"timeUnit":"d","yunjing_pro":1}
GoodsNum	yes	no	Uint64	Order Count Example: 1
PayMode	yes	no	Uint64	Billing Pattern: 0 Postpaid, 1 Prepaid Example: 1
RegionId	yes	no	Uint64	Region. Example: 1
ZoneId	yes	no	Uint64	Availability zone. Example: 1

ScanTaskDetails

Scan task details.

Referenced by the following interfaces: DescribeScanTaskDetails

name	required	NULL allowed	type	description
Description	no	no	String	Description. Example: Failed
FailType	no	no	Uint64	Failure type. 3: offline; 4: timeout; 5: failed; 8: early agent version. Example: 4
HostIp	no	no	String	Server IP. Example: 10.0.0.1
HostName	no	no	String	Server name. Example: any-agent
Id	no	no	Uint64	Unique ID. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineWanIp	no	no	String	Public IP. Example: 172.22.11.12

name	required	NULL allowed	type	description
OsName	no	no	String	Operating system. Example: win64
Quuid	no	no	String	QUUID. Example: badea25d-d702-4f68-8906-0580c0a13170
RiskNum	no	no	Uint64	Number of risks. Example: 1
ScanBeginTime	no	no	String	Start time of the scan. Example: 2024-10-29 10:35:50
ScanEndTime	no	no	String	Time when the scan ends. Example: 2024-10-29 10:39:50
Status	no	no	String	Status code: Scanning; Ok; Fail. Example: Fail
Uuid	no	no	String	Unique user ID. Example: badea25d-d702-4f68-8906-0580c0a13170

BaselineFix

Baseline password fixing.

Referenced by the following interfaces: DescribeBaselineFixList

name	required	NULL allowed	type	description
CreateTime	no	no	String	First scan time. Example: 2021-02-01 12:00:00
FixTime	no	no	String	Time when it was fixed. Example: 2021-02-01 12:00:00
HostIp	no	no	String	IP address of the server. Example: 192.168.0.204
Id	no	no	Int64	Result ID of the baseline check item. Example: 1
ItemName	no	no	String	Name of the fix item. Example: Ensure the SSH idle timeout time.
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information Example:View
ModifyTime	no	no	String	Last detection time. Example: 2021-02-01 12:00:00

AssetType

Description of an asset fingerprint type.

Referenced by the following interfaces: DescribeAssetTypes

name	required	NULL allowed	type	description
Id	yes	no	Uint64	Type ID. Example: 1
Name	yes	no	String	Type name. Example: Accounts

CanNotSeparateInfo

Information about servers on which trojans cannot be quarantined.

Referenced by the following interfaces: DescribeCanNotSeparateMachine

name	required	NULL allowed	type	description
Alias	yes	no	String	Server name. Example: redis_node_cvm
PrivateIp	yes	no	String	Private IP address. Example: 127.12.1.1
PublicIp	yes	no	String	Public IP. Example: 192.2.23.1
Quuid	yes	no	String	QUUID of the server. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
Reason	yes	no	Uint64	Cause of the quarantine failure. 1: the agent is offline. Example: 1
Uuid	yes	no	String	Host UUID. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0

MachineLicenseDetail

License binding information of a server.

Referenced by the following interfaces: DescribeMachineLicenseDetail

name	required	NULL allowed	type	description
InquireKey	yes	no	String	This field has been deprecated. Example: xv_yunjing_se_x
PayMode	yes	no	Uint64	Billing mode. 0: pay-as-you-go; 1: prepaid. Example: 1
Quuid	yes	no	String	QUUID of the server. Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0
ResourceId	yes	no	String	Resource ID. Example: any1d
SourceType	yes	no	Uint64	Order type. 0: default billing order; 1: trial order; 2: gift; 3: experience. Example: 1

MaWhitelist

Referenced by the following interfaces: DescribeMaWhitelist, ModifyMaWhitelist

name	required	NULL allowed	type	description
CreateTime	no	yes	String	Creation time. Example: 2023-10-10 00:00:00
Dest	yes	yes	String	Access target, which supports IPs/IP ranges. Multiple entries are separated by semicolons. The default is All. Example: 1.1.1.1-1.1.1.2
DestPort	no	yes	String	Target port. Multiple entries are separated by semicolons. If not specified, it indicates all. Example: 80;8080
Enable	yes	yes	Uint64	Whether it is enabled. • 0: Not enabled. • 1: Enabled. Example: 1
From	yes	yes	Uint64	Configuration source of the allowlist. • 1: Tenant console. • 0: CMGT console. The tenant console cannot delete or disable global configuration allowlists from the CMGT console. Example: 1
Id	no	yes	Uint64	ID of the allowlist configuration item. Example: 1
ModifyTime	no	yes	String	Update time. Example: 2023-10-10 00:00:00
Name	yes	yes	String	Allowlist name. Example: Allowlist 1
Source	yes	yes	String	Access source, which supports IPs/IP ranges. Multiple entries are separated by semicolons. The default is All. Example: 1.1.1.1/24
Updater	yes	yes	String	Allowlist creator/updater. Example: Alice

HostLoginList

Login audit list.

Referenced by the following interfaces: DescribeHostLoginList

name	required	NULL allowed	type	description
City	no	yes	Uint64	City ID. Example: 23
Country	no	yes	Uint64	Country ID. Example: 1
Desc	no	yes	String	High-risk Information Explanation: ABROAD - Overseas IP; XTI – Threat Intelligence. Example: ABROAD
Id	no	no	Uint64	Record ID. Example: 10001
IsRiskArea	no	yes	Uint64	Whether it is determined as a login from an unusual location. 1: yes. 0: no. Example: 1
IsRiskSrcIp	no	yes	Uint64	Whether it is determined as a suspicious IP address. 1: yes. 0: no. Example: 1
IsRiskTime	no	yes	Uint64	Whether it is determined as a suspicious login time. 1: yes. 0: no. Example: 1
IsRiskUser	no	yes	Uint64	Whether it is determined as a suspicious user. 1: yes. 0: no. Example: 1
Location	no	yes	String	Location name. Example: location1,location2,location3
LoginTime	no	yes	String	Login time. Example: 2024-10-30 15:58:43
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	no	yes	String	IP address of the server. Example: 192.168.0.204
MachineName	no	yes	String	Server name. Example: redis_node_cvm
ModifyTime	no	yes	String	Modification time. Example: 2024-10-30 15:58:43
Port	no	yes	Int64	Request destination port. Example: 3306
Province	no	yes	Uint64	Province ID. Example: 101
Quuid	no	yes	String	QUUID of the server. Example: 935e27b1-d675-4509-80bf-96fbf0764237
RiskLevel	no	yes	Uint64	Risk severity. 0: high. 1: suspicious. Example: 1
SrcIp	no	yes	String	Source IP. Example: 192.168.0.204
Status	no	no	Uint64	1: usual login. 2: login from an unusual location. 5: added to the allowlist. 14: handled. 15: ignored. Example: 1
UserName	no	yes	String	User name. Example: root
Uuid	no	yes	String	Host UUID. Example: 380add75-bb06-4cc4-84c5-c806d102fbba

BaselinePolicyDetect

Baseline check policy.

Referenced by the following interfaces: DescribeBaselineDetectList

name	required	NULL allowed	type	description
FailedCount	yes	no	Int64	Number of servers that failed the check due to timeouts. Example: 1
FinishTime	yes	no	String	End time. Example: 2021-02-01 12:00:00
HostCount	yes	no	Int64	Number of associated servers. Example: 52
PolicyDetectStatus	yes	yes	Int64	1: checking. 2: check completed. Example: 1
PolicyId	yes	no	Int64	Policy ID. Example: 1523
PolicyName	yes	no	String	Policy name. Example: Unauthorized access
StartTime	yes	no	String	Start time. Example: 2021-02-01 12:00:00
SuccessCount	yes	no	Int64	Number of servers that passed the check. Example: 1
TaskId	yes	no	Int64	ID of the check task. Example: 18644956
TimeoutCount	yes	no	Int64	Number of servers that failed the check due to timeouts. Example: 1

RansomDefenseStrategyMachineBackupInfo

Details of Host Backup Bound to Anti-Ransomware Policy

Referenced by the following interfaces: DescribeRansomDefenseMachineList

name	required	NULL allowed	type	description
BackupCount	yes	yes	Uint64	Number of Backups Example: 1
BackupSuccessCount	yes	yes	Uint64	Backup Success Count Example: 1
CloudTags	yes	yes	Array of Tag	Cloud tag Example:View
DiskInfo	yes	yes	String	Hard Disk Information, effective for all disks when empty: disk1
InstanceId	yes	no	String	Host Instance ID Example: cvm-dwcs
LastBackupMessage	yes	yes	String	Reason for the Last Backup Failure Example: fail
LastBackupStatus	yes	yes	Uint64	Latest Backup Status: 0 - Backing Up, 1 - Normal, 2 - Failed, 9 - No Backup Yet Example: 1
LastBackupTime	yes	yes	String	Last Backup Time Example: 2022-11-11 11:11:11
MachineIp	yes	no	String	Private IP address. Example: 10.0.0.22
MachineName	yes	no	String	Server name. Example: redis_node_cvm
MachineWanIp	yes	yes	String	Public IP. Example: 112.11.33.22
Quuid	yes	no	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
RegionInfo	yes	yes	RegionInfo	Information on availability zones. Example:View
RollBackPercent	yes	yes	Uint64	Latest Rollback Progress Percentage Example: 1
RollBackStatus	yes	yes	Uint64	Latest Rollback Status: 0 - In Progress, 1 - Succeeded, 2 - Failed Example: 1
Status	yes	yes	Uint64	Protection status: 0 Disabled, 1 Enabled. Example: 0
StrategyId	yes	yes	Uint64	Policy ID. 0 indicates no binding to any policy. Example: 0
StrategyName	yes	yes	String	Policy name. Example: any1
Tag	yes	yes	Array of MachineTag	Host Security Tag Example:View
Uuid	yes	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

JavaMemShellDetail

Details of a Java memory trojan event.

Referenced by the following interfaces: DescribeJavaMemShellInfo

name	required	NULL allowed	type	description
Annotations	no	no	String	Comment. Example: Note
Args	no	no	String	Parameters of the Java process command. Example: org.apache.jasper.servlet.JasperLoader
ClassContent	no	no	String	Base64 encoded binary code of the Java memory trojan. Example: yGFjaXFmZSBjb20uYZ9lcGFuaTkgHIB1YmxpYyBjbGFzcyBNYWluIHtgICAgICBwdWJsaWMgc3RhdGljIHZvaQ==
ClassContentPretty	no	no	String	Decompiled Java memory trojan code. Example: package com.company; public class Main { public static voi
ClassLoaderName	no	no	String	Java loader class name. Example: org.apache.jasper.servlet.JasperLoader
ClassName	no	no	String	Class name. Example: main.class
CreateTime	no	no	String	First time when it was found. Example: 2021-01-20 16:17:11
Description	no	no	String	Help. Example: Trojan is detected in the org.apache.catalina.startup.Bootstrap class of the Java process (PID: 1128220).
EventDescription	no	no	String	Event description. Example: A Webshell is detected in Java service processes. Java Webshell can reside in the memory for a long time and receive input submitted by attackers for long-term remote control of servers.
Exe	no	no	String	Path of the Java process. Example: /usr/lib/jvm/java-6-openjdk-amd64/jre/bin/java
InstanceName	no	no	String	Container name. Example: redis_node_cvm
InstanceState	no	no	String	Instance status. Valid values: RUNNING, STOPPED, and SHUTDOWN. Example: RUNNING
Interfaces	no	no	String	Inherited interfaces. Example: java.IO.Writer,java.IO.Reader
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information Example:View
MachineState	no	no	String	Agent status: OFFLINE, ONLINE. Example: OFFLINE
Md5	no	no	String	MD5 value of the class file. Example: 37e54fce603f1ca6c82927caf7aa1c412
Pid	no	no	Uint64	Process pid. Example: 1
PrivateIp	no	no	String	Private IP Example: 192.168.255.10
PublicIp	no	no	String	Public IP Example: 110.40.207.98
RecentFoundTime	no	no	String	Last detection time. Example: 2021-01-20 16:17:11
SecurityAdvice	no	no	String	Security suggestion. Example: Check Java service access logs and assess whether memory shells have been accessed. Check for high-risk vulnerabilities on the host, fix the high-risk vulnerabilities, and restart the Java service.
Status	no	no	Uint64	Handling status. 0: to be handled. 1: added to the allowlist. 2: deleted. 3: ignored. 4: manually handled. Example: 0
SuperClassName	no	no	String	Parent class name. Example: java.lang.Object
Type	no	no	Uint64	Trojan memory type. 0: Filter. 1: Listener. 2: Servlet. 3: Interceptors. 4: Agent. 5: others. Example: 1

EventStat

Statistics about pending security events.

Referenced by the following interfaces: DescribeSecurityEventStat

name	required	NULL allowed	type	description
EventsNum	yes	no	Uint64	Number of events. Example: 0
MachineAffectNum	yes	no	Uint64	Number of affected servers. Example: 0

JavaMemShellInfo

Java memory trojan event information.

Referenced by the following interfaces: DescribeJavaMemShellList

name	required	NULL allowed	type	description
Alias	no	yes	String	Server name. Example: dev-centos8
Annotations	no	yes	String	Comment. Example: @Override
ClassName	no	yes	String	Class name. Example: org.apache.catalina.startup.Bootstrap
CreateTime	no	no	String	First time when it was found. Example: 2021-01-20 16:17:11
Description	no	no	String	Help. Example: Trojan is detected in the org.apache.catalina.startup.Bootstrap class of the Java process (PID: 1128220).
HostIp	no	yes	String	Server IP. Example: 192.168.255.10
Id	no	no	Uint64	Event ID. Example: 142
Interfaces	no	yes	String	Inherited interfaces. Example: org.apache.catalina.startup.Bootstrap
LoaderClassName	no	yes	String	Associated class loader. Example: org.apache.catalina.startup.Bootstrap
MachineExtraInfo	no	yes	MachineExtraInfo	Host Additional Information Example:View
Quuid	no	no	String	QUUID of the server. Example: e1081ae-7777-4fd1-a2f7-88f3faa3d302
RecentFoundTime	no	no	String	Last detection time. Example: 2021-01-20 16:17:11
Status	no	no	Uint64	Handling status. 0: to be handled. 1: added to the allowlist. 2: deleted. 3: ignored. 4: manually handled. Example: 0
SuperClassName	no	yes	String	Parent class name. Example: org.apache.catalina.startup.Bootstrap

name	required	NULL allowed	type	description
Type	no	no	Uint64	Trojan memory type. 0: Filter. 1: Listener. 2: Servlet. 3: Interceptors. 4: Agent. 5: others. Example: 1
Uuid	no	yes	String	UUID of the server. Example: e1081aa-7777-46df-a2f7-88f3faa3d302

VulFixStatusSnapshotInfo

Snapshot information of a server.

Referenced by the following interfaces: DescribeVulFixStatus

name	required	NULL allowed	type	description
FailReason	yes	yes	String	Reason for failed snapshot creation. Example: Failed to get authorization
HostIp	yes	yes	String	IP address of the server. Example: 145.12.3.12
HostName	yes	yes	String	Server name. Example: redis_node_cvm
Id	yes	no	Uint64	Unique ID of the record. Example: 12
ModifyTime	yes	yes	String	Time when the snapshot was created. Example: 2021-03-11 18:15:17
Quuid	yes	no	String	cvm id Example: 380add75-bb06-4cc4-84c5-c1806d102fba
SnapshotId	yes	yes	String	Snapshot ID. Example: snp-dhussaxy
SnapshotName	yes	yes	String	Name of the snapshot. Example: Backup on 2021-03-01
Status	yes	no	Uint64	Snapshot status. 0: initial status. 1: the snapshot was created successfully. 2: the snapshot failed to be created. Example: 1

MalwareWhiteListInfo

Component list data.

Referenced by the following interfaces: DescribeMalwareWhiteList

name	required	NULL allowed	type	description
CreateTime	yes	no	String	The point in time when the rule was created. Example: 2024-10-30 09:12:21
EventsCount	yes	no	Uint64	Number of event records. Example: 1
FileDirectory	yes	no	String	File directory. Multiple file directories are separated with commas (,). Example: /tmp
FileExtension	yes	no	String	File extension. Multiple file extensions are separated with commas (,). Example: php
FileName	yes	no	String	File name. Multiple file names are separated with commas (,). Example: run.sh
Id	yes	no	Uint64	Unique ID. Example: 1
IsGlobal	yes	no	Uint64	Whether the allowlist takes effect on all servers. 0: no. 1: yes. Example: 1
MatchType	yes	no	Uint64	Match mode. 0: exact match. 1: fuzzy match. Example: 1
Md5List	yes	no	String	List of MD5 values. Multiple MD5 values are separated with commas (,). Example: 708cae4cf814c3deda4208da228fad4e
Mode	yes	no	Uint64	Allowlist mode. 1: MD5 allowlist. 1: custom allowlist. Example: 1
ModifyTime	no	no	String	Rule modification time. Example: 2024-10-30 09:12:21
QuuidList	yes	no	String	QUUIDs of servers. Multiple QUUIDs are separated with commas (,). Example: e5b4724c-49af-46ab-bd84-cdbae897e7e0

MachineExtraInfo

Server Basic Information

Referenced by the following interfaces: DescribeAssetAppList, DescribeAssetCoreModuleList, DescribeAssetDatabaseList, DescribeAssetEmList, 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, DescribeIgnoreHostAttemConfig, DescribeJavaMemShellInfo, DescribeJavaMemShellList, DescribeJavaMemShellPluginList, DescribeLicenseBindList, DescribeLicenseBindSchedule, DescribeMachineList, DescribeMachines, DescribeMalWareList, DescribeMalwareInfo, DescribePrivilegeEvents, DescribeProtectDirRelatedServer, DescribeReverseShellEvents, DescribeRiskDnsEventInfo, DescribeRiskDnsEventList, DescribeRiskProcessEvents, DescribeScanTaskDetails, DescribeScreenMachines, DescribeVulDefenceEvent, DescribeVulEffectHostList, DescribeWebPageEventList

name	required	NULL allowed	type	description
HostName	no	yes	String	Server name. Example: redis_node_cvm
InstanceID	no	yes	String	Instance ID. Example: ins-1s7mkggc
NetworkName	no	yes	String	Network Name, returns vpc_id in the case of a VPC network Example: vpc-9m7hl6w
NetworkType	no	yes	Int64	Network type: 1: VPC network; 2: basic network; 3: non-cloud network. Example: 1
PrivateIP	no	yes	String	Private IP. Example: 1.1.1.1
WanIP	no	yes	String	Public IP Example: 1.1.1.1

MaCustomPolicy

Referenced by the following interfaces: DescribeMaCustomPolicyList, ModifyMaCustomPolicy

name	required	NULL allowed	type	description
ActionType	no	yes	Uint64	Policy action, currently only 0. • 0: Allow • 1: Alarm Example: 0
ConEventId	no	yes	Array of Uint64	ID of the historical event when added into the allowlist. Example: [201]
CreateTime	no	yes	String	Creation time. Example: 2023-10-10 00:00:00
DestHostWorkloadNum	no	yes	Uint64	Number of the target server workloads. Example: 1
DestIPs	no	yes	Array of String	Target IP configuration. Example: ["192.168.0.204"]
DestLabels	no	yes	Array of MaLabel	Target tag configuration. Example:View
DestPodWorkloadNum	no	yes	Uint64	Number of the target pod workloads. Example: 1
DestPorts	no	yes	Array of String	Target port, which defaults to All if not specified, indicating all. Example: ["80"]
DestType	yes	yes	Uint64	Target configuration type. • 0: Tag • 1: IP • 2: Workload • 3: All Example: 1
DestWorkloads	no	yes	Array of MaCustomPolicyWorkload	Target workload configuration. Example:View
Enable	yes	yes	Uint64	Custom allowlist status. • 0: Disabled • 1: Enabled Example: 1
HandleHistory	no	yes	Int64	Whether to process historical events. • 0: Do not process • 1: Process Example: 0
Id	no	yes	Uint64	Custom allowlist rule ID. Example: 1
ModifyTime	no	yes	String	Update time. Example: 2023-10-10 00:00:00
Name	yes	yes	String	Name of the custom allowlist rule. Example: policy1
SrcHostWorkloadNum	no	yes	Uint64	Number of the source server workloads. Example: 1
SrcIPs	no	yes	Array of String	Source IP configuration. Example: ["192.168.0.1"]
SrcLabels	no	yes	Array of MaLabel	Source tag configuration. Example:View
SrcPodWorkloadNum	no	yes	Uint64	Number of the source pod workloads. Example: 1
SrcType	yes	yes	Uint64	Source configuration type. • 0: Tag • 1: IP • 2: Workload • 3: All Example: 1
SrcWorkloads	no	yes	Array of MaCustomPolicyWorkload	Source workload configuration. Example:View
Updater	yes	yes	String	Creator/updater. Example: user1

OrderModifyConfig

Order configuration adjustment object.

Referenced by the following interfaces: ModifyOrder

name	required	NULL allowed	type	description
InquireKey	yes	yes	String	Billable item name, which starts with sv. Example: sv_yunjing_ue_x
InquireNum	yes	yes	Uint64	Purchase Quantity Example: 10
SubProductCode	yes	yes	String	Subproduct SP_ Example: sp_yunjing_0014

SearchTemplate

Quick search template.

Referenced by the following interfaces: CreateSearchTemplate, DescribeSearchTemplates

name	required	NULL allowed	type	description
Condition	yes	no	String	Search statement. Example: count is_one_of 200
DisplayData	yes	no	String	Data displayed. Example: [{"id":1652667748318,"patternsField":"count","selectedtype":"is"}]
Flag	yes	no	String	Search method. Valid values for searches in a search box: standard and filter. Valid value for simple searches: simple. Example: simple

name	required	NULL allowed	type	description
Id	no	no	Uint64	Rule ID. Example: 198
LogType	yes	no	String	Search index type. Example: userlog-vul
Name	yes	no	String	Search name. Example: nOqBFVMNgONSs4Gm5GYZpwkKdZ1KFMtuGysMcJeioNvGEISsvXaDcpSFuzHkTiEjqkGWameNFwmtVR9kEbdsDG@Uayay
Query	yes	no	String	Query statement after conversion. Example: {"index":["userlog-vul"], "body":{"query":{}, "sort":[{"create_time":"desc"}]}
TimeRange	yes	no	String	Time range. Example: From 2021-11-11 00:00:00 to 2022-02-01 12:00:00

AssetLoadSummary

Resource load overview.

Referenced by the following interfaces: DescribeAssetLoadInfo

name	required	NULL allowed	type	description
Counts	yes	no	Array of Uint64	Load counts. [0% or an unknown number. 0% to 20%. 20% to 50%. 50% to 80%. 80% to 100%.] Example: [0,1,1,2,3,1]
Top5	yes	yes	Array of AssetLoadDetail	Top 5 loads. Example:View

BaselinePolicy

Baseline policy information.

Referenced by the following interfaces: DescribeBaselinePolicyList, ModifyBaselinePolicy

name	required	NULL allowed	type	description
AssetType	yes	no	Int64	Asset type. 0: all servers with CWP Pro and all servers with CWP Ultimate. 1: server ID. 2: server IP address. Example: 0
DetectInterval	yes	no	Int64	Check interval. 1: 1 day. 3: 3 days. 5: 5 days. 7: 7 days. Example: 7
DetectTime	yes	no	String	Scan time. Example: 09:00:00
HostCount	no	no	Int64	Number of servers associated with the baseline. Example: 0
HostIds	no	no	Array of String	Server ID. Example: ["116d84e9-22d1-4fa1-a11b-a1e58f2bayay"]
HostIps	no	no	Array of String	IP address of the server. Example: ["1.1.1.1"]
IsDefault	no	no	Int64	Whether it is the system default policy. Example: 0
IsEnabled	yes	no	Int64	Whether it is enabled. 0: not enabled. 1: enabled. Example: 0
ItemCount	no	no	Int64	Number of associated baseline items. Example: 1419
PolicyId	no	no	Int64	Policy ID. Example: 902471
PolicyName	yes	no	String	Policy name. The maximum length is 128 characters. Example: International standard baseline
RuleCount	no	no	Int64	Number of associated baseline items. Example: 12
RuleIds	no	no	Array of Int64	Rule ID. Example: [11]

AssetEnvBaseInfo

List of environment variables in the asset management module.

Referenced by the following interfaces: DescribeAssetEnvList

name	required	NULL allowed	type	description
FirstTime	no	no	String	First collection time. Example: 2022-07-15 11:27:01
IsNew	no	no	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	no	no	String	Server IP. Example: 1.1.1.1
MachineName	no	no	String	Server name. Example: hname
MachineWanIp	no	no	String	Public IP address of a server. Example: 1.1.1.1
Name	no	no	String	Name. Example: BASHOPTS
OsInfo	no	no	String	Operating system. Example: Linux
Quuid	no	no	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Type	no	no	Uint64	The attribute type. Valid values: 0: user variable 1: system variable Example: 1
UpdateTime	no	yes	String	Data update time. Example: 2011-11-11 12:12:12
User	no	no	String	User who triggers initialization. Example: root
Uuid	no	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Value	no	no	String	The environment variable value. Example: checkwinsize:cmdhist:complete_fullquote:extquote:force_fignore:globascii:ranges:hostcomplete:interactive_comments:login_shell:progcomp:promptvars:sourcepath

Place

Login location information

Referenced by the following interfaces: AddLoginWhiteLists, DescribeLoginWhiteCombinedList, DescribeLoginWhiteList, DescribeLoginWhiteListNew, ModifyLoginWhiteInfo, ModifyLoginWhiteRecord

name	required	NULL allowed	type	description
CityId	yes	no	Uint64	City ID. Example: 99
CountryId	yes	no	Uint64	Country ID Example: 1
Location	no	no	String	Location name. Example: location1|location2|location3
ProvinceId	yes	no	Uint64	Province ID. Example: 23

VulLevelCountInfo

Number of vulnerabilities at each severity level.

Referenced by the following interfaces: DescribeVulHostTop

name	required	NULL allowed	type	description
VulCount	yes	no	Uint64	Number of vulnerabilities. Example: 10
VulLevel	yes	no	Uint64	Vulnerability severity. 1: low. 2: medium. 3: high. 4: critical. Example: 3

SecurityEventInfo

Security event statistics.

Referenced by the following interfaces: DescribeSecurityEventsCnt

name	required	NULL allowed	type	description
EventCnt	yes	no	Uint64	Number of security events. Example: 17
UuidCnt	yes	no	Uint64	Number of affected servers. Example: 6

AssetUserBaseInfo

Basic account information in the asset management module.

Referenced by the following interfaces: DescribeAssetUserList

name	required	NULL allowed	type	description
FirstTime	no	no	String	First collection time. Example: 2011-11-11 12:12:12
Gid	no	no	String	Account GID. Example: 16
HomePath	no	no	String	Home directory. Example: /var/lib/sgprofile
IsDomain	no	no	Uint64	Whether a domain account: 0: no; 1: yes; 2: no; 999: null (Windows only). Example: 1
IsNew	no	no	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
IsRoot	no	no	Uint64	Whether it is granted the root permissions. 0: no. 1: yes. 999: empty string. This parameter is applicable only to Linux systems. Example: 1
IsSshLogin	no	no	Uint64	Whether SSH logins are allowed. 1: allowed. 0: not allowed. 999: empty string. This parameter is applicable only to Linux systems. Example: 1
IsSudo	no	no	Uint64	Whether it is granted the sudo permissions. 1: yes. 0: no. 999: empty string. This parameter is applicable only to Linux systems. Example: 1
LastLoginTime	no	no	String	Last login time. Example: 1
LoginType	no	no	Uint64	Login type. 0: logins are not allowed. 1: only logins with keys are allowed. 2: only logins with passwords are allowed. 3: logins with keys or passwords are allowed. 999: empty string. This parameter is applicable only to Linux systems. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Host information Example:View
MachineIp	no	no	String	Private IP address of the server. Example: 10.0.0.11
MachineName	no	no	String	Server name. Example: redis_node_cvm
MachineWanIp	no	no	String	Public IP address of the server. Example: 112.65.22.19
Name	no	no	String	The username. Example: admin

name	required	NULL allowed	type	description
OsInfo	no	no	String	OS information. Example: Centos 64bit
PasswordChangeTime	no	no	String	Password reset time. Example: 2024-10-22 19:40:38
PasswordDueTime	no	no	String	Time when the password expires. This parameter is applicable only to Linux systems. Example: 2024-10-22 19:40:38
PasswordLockDays	no	no	Int64	Number of days for which the password is locked. -1: never locked. 999: empty string. This parameter is applicable only to Linux systems. Example: 1
PasswordStatus	no	no	Int64	Password status. 1: normal. 2: expire soon. 3: expired. 4: locked. 999: empty string. This parameter is applicable only to Linux systems. Example: 1
ProjectId	no	no	Uint64	ID of the project to which the server belongs. Example: 1
Quuid	no	no	String	Host QUUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Shell	no	no	String	Path of the shell. This parameter is applicable only to Linux systems. Example: /bin/bash
ShellLoginStatus	no	no	Uint64	Whether it is a shell login. 0: no. 1: yes. This parameter is applicable only to Linux systems. Example: 1
Status	no	no	Uint64	Account status. 0: disabled. 1: enabled. Example: 1
Uid	no	no	String	Account UID. Example: 16
UpdateTime	no	yes	String	Update time. Example: 2011-11-11 12:12:12
UserType	no	no	Uint64	Account type: 0: guest user; 1: standard user; 2: administrator user; 999: null (Windows only). Example: 1
Uuid	no	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

ScreenBroadcasts

Security notice information in the dashboard visualization module.

Referenced by the following interfaces: DescribeScreenBroadcasts

name	required	NULL allowed	type	description
Id	yes	no	Uint64	Notice ID. Example: 10003
Level	yes	no	Uint64	Severity of the notice. 0: no risk. 1: critical. 2: high. 3: medium. 4: low. Example: 1
Time	yes	no	String	Release time. Example: 2021-03-30 19:17:28
Title	yes	no	String	Title of the notice. Example: The Apache HTTP/2 DoS vulnerability (CVE-2023-44487) has been detected.

ScreenProtection

Attack defense status in the dashboard visualization module.

Referenced by the following interfaces: DescribeScreenProtectionStat

name	required	NULL allowed	type	description
Name	yes	no	String	Type value, which includes file scanning and cleaning, brute force attack, vulnerability scanning, and baseline check. Example: Virus Scanning
Status	yes	no	Uint64	File scanning and cleaning: 0: never checked or no paid asset found. 1: checked and malicious files detected. 2: checked and quarantine protection not enabled. 3: checked, protection enabled, and no risks detected. Brute force attack: 0: protection not enabled and no paid asset found. 1: automatic blocking enabled. Vulnerability scanning: 0: never checked or no paid asset found. 1: vulnerability risks detected. 2: no risks detected. Baseline check: 0: never checked or no paid asset found. 1: baseline risks detected. 2: no risks detected. Example: 1

AttackSource

Attack backtracking information.

Referenced by the following interfaces: DescribeAttackSource

name	required	NULL allowed	type	description
Edges	yes	yes	Array of AttackSourceEdge	Node paths. Example:View
EventInfoParam	yes	yes	String	Event details parameters related to request nodes. Example: params
Nodes	yes	yes	Array of AttackSourceNode	Node description. Example:View

BashEventsInfo

High-risk command details.

Referenced by the following interfaces: DescribeBashEventsInfo

name	required	NULL allowed	type	description
BashCmd	yes	no	String	Command to run. Example: rm
CreateTime	yes	no	String	Event time. Example: 2021-03-30 19:17:28
DetectBy	no	yes	Int64	Data Source Example: agent
Exe	yes	yes	String	Process name. Example: l.exe
HarmDescribe	yes	yes	String	Description. Example: desc of event
HostIp	yes	no	String	Private IP address of the server. Example: 127.0.0.1
Id	yes	no	Uint64	Data ID. Example: 1001
MachineName	yes	no	String	Server name. Example: redis_node_cvm
MachineStatus	yes	yes	String	Connection status of the server. Valid values: OFFLINE and ONLINE. Example: ONLINE
MachineWanIp	yes	yes	String	Public IP address of the server. Example: 124.2.4.55
ModifyTime	yes	yes	String	Handling time. Example: 2021-03-30 19:17:28
Pid	yes	yes	String	Process ID. Example: 1
Platform	yes	no	Uint64	System type. 2: Windows. 4: Linux. Example: 1
PsTree	yes	yes	String	Process tree in the JSON format. pid: process ID. exe: file path. account: user group and user to which the process belongs. cmdline: command to be run. ssh_service: SSH service. ssh_source: login source. Example: "{\"pid\":1,54,\"exe\":\"/usr/bin/bash\",\"account\":\"root:root\",\"cmdl"
Quuid	yes	no	String	Server ID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
References	yes	yes	Array of String	Reference link. Example: ["http://www.domain.com"]
RegexBashCmd	yes	yes	String	Auto-generated regular expression. Example: rm -rf /tmp/t*
RuleCategory	yes	yes	Uint64	Rule type. 0: system rule. 1: custom rule. Example: 0
RuleId	yes	no	Uint64	Rule ID. A value of 0 indicates that the rule has been deleted or the effective scope has been modified. Example: 1
RuleLevel	yes	no	Uint64	Rule severity. 1: high. 2: medium. 3: low. Example: 1
RuleName	yes	no	String	Rule Name Example: redis_node_use
Status	yes	no	Uint64	Handling status. 0: to be handled. 1: handled. 2: added to the allowlist. 3: ignored. Example: 1
SuggestScheme	yes	yes	String	Suggestion scheme. Example: attempt to repair
Tags	yes	yes	Array of String	Tag. Example: ["tag-redis","tag-nginx"]
User	yes	yes	String	Login user. Example: root
Uuid	yes	no	String	Host UUID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

RiskMainClass

Risk service during Java Webshell and RASP injection.

Referenced by the following interfaces: DescribeInjectRiskyServiceSwitch

name	required	NULL allowed	type	description
ServiceName	no	yes	String	Risk service during RASP injection. Example: 1

AssetMachineBaseInfo

Basic server information in the asset fingerprint module.

Referenced by the following interfaces: DescribeAssetMachineList

name	required	NULL allowed	type	description
Cpu	no	no	String	CPU information. Example: Intel(R) Xeon(R) Gold 6148 CPU @ 2.40GHz
CpuLoad	no	no	String	CPU utilization in percentage. Example: 54.2
CpuLoadNum	no	yes	String	CPU load readings (only valid for Linux systems). Example: 0
CpuSize	no	no	Uint64	Number of CPU cores. Example: 1
DiskLoad	no	no	String	Disk usage in percentage. Example: 22.4
DiskSize	no	no	Uint64	Disk capacity. Unit: GB. Example: 100
FirstTime	no	no	String	First collection time. Example: 2022-07-15 11:27:01
IsNew	no	no	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	no	no	String	Server private IP address. Example: 10.0.0.11
MachineName	no	no	String	Server name. Example: any-machine
MachineWanIp	no	no	String	Public IP address of the server. Example: 112.22.662.11
MemLoad	no	no	String	Memory utilization in percentage. Example: 22.5

name	required	NULL allowed	type	description
MemSize	no	no	Uint64	Memory capacity. Unit: GB. Example: 1024
OsInfo	no	no	String	OS name. Example: windows
PartitionCount	no	no	Uint64	Number of partitions Example: 1
ProjectId	no	no	Uint64	Project ID. Example: 1
Quuid	no	no	String	QUUID of the server. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
Tag	no	yes	Array of MachineTag	Tag. Example:View
UpdateTime	no	yes	String	Data update time. Example: 2011-11-11 12:12:12
Uuid	no	no	String	UUID of the server. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

PrivilegeEventInfo

Local privilege escalation data.

Referenced by the following interfaces: DescribePrivilegeEventInfo

name	required	NULL allowed	type	description
CmdLine	yes	no	String	Command to run. Example: /bin/nginx
CreateTime	yes	no	String	Event time. Example: 2024-10-30 02:19:08
FullPath	yes	no	String	Process path. Example: /bin/nginx
HarmDescribe	yes	no	String	Risk description. Example: After hacking a server, hackers may perform operations such as downloading malicious files, connecting to a mining pool, adding public keys, and viewing sensitive files for further malicious actions.
HostIp	yes	no	String	Private IP address of the server. Example: 10.0.0.1
Id	yes	no	Uint64	Data ID. Example: 1
MachineName	yes	no	String	The host name. Example: ims-agent
MachineStatus	yes	no	String	Connection status of the server. Valid values: OFFLINE and ONLINE. Example: ONLINE
MachineWanIp	yes	no	String	Public IP address of the server. Example: 124.2.4.55
ModifyTime	yes	no	String	Handling time. Example: 2021-03-30 19:17:28
NewCaps	yes	no	String	List of permissions. Multiple permissions are separated with vertical lines (
ParentProcGroup	yes	no	String	User group of the parent process. Example: root
ParentProcName	yes	no	String	Parent process name. Example: /bin/ssh
ParentProcPath	yes	no	String	Path of the parent process. Example: /bin/ssh
ParentProcUser	yes	no	String	Username of the parent process. Example: root
ProcFilePrivilege	yes	no	String	Permissions on the process file. Example: rwx
ProcessName	yes	no	String	Process name. Example: nginx
PsTree	yes	no	String	Process tree in the JSON format. pid: process ID. exe: file path. account: user group and user to which the process belongs. cmdline: command to be run. ssh_service: SSH service. ssh_source: login source. Example: {"pid":"143","account":"root","exe":"/tmp"}
Quuid	yes	no	String	Host UUID. Example: e5b4724c-49af-46ab-bd84-cdbaa897e7e0
References	yes	no	Array of String	Reference link. Example: ["http://www.domain.com"]
Status	yes	no	Uint64	Handling status. 0: to be handled. 2: added to the allowlist. 3: handled. 4: ignored. Example: 0
SuggestScheme	yes	no	String	Suggestion scheme. Example: 1. Check for malicious processes and invalid ports, and delete suspicious startup items and scheduled tasks. 2. Isolate or delete relevant Trojan files.
Tags	yes	no	Array of String	Tag. Example: ["redis_use","nginx_use"]
UserGroup	yes	no	String	User Group Example: root
UserName	yes	no	String	User name. Example: root
Uuid	yes	no	String	UUID of the CWP agent. Example: e5b4724c-49af-46ab-bd84-cdbaa897e7e0

ComponentStatistics

Component statistics.

Referenced by the following interfaces: DescribeComponentStatistics

name	required	NULL allowed	type	description
ComponentName	yes	no	String	Component name. Example: nginx
ComponentType	yes	no	String	Component type. • WEB: web component. • SYSTEM: system component Example: WEB
Description	yes	no	String	Description of the component. Example: nginx web
Id	yes	no	Uint64	Component ID. Example: 100010
MachineNum	yes	no	Uint64	Number of servers. Example: 10

BashEventsInfoNew

High-risk command details (new).

Referenced by the following interfaces: DescribeBashEventsInfoNew

name	required	NULL allowed	type	description
BashCmd	yes	no	String	Command to run. Example: rm
CreateTime	yes	no	String	Event time. Example: 2021-03-30 19:17:28
DetectBy	yes	yes	Int64	Detection source. 0: bash command. 1: real-time monitoring. Example: 0
Exe	yes	yes	String	Process name. Example: 1.exe
HarmDescribe	yes	yes	String	Description. Example: desc of event
HostIp	yes	no	String	Private IP address of the server. Example: 127.0.0.1
Id	yes	no	Uint64	Data ID. Example: 1
MachineName	yes	no	String	Server name. Example: redis_node_cvm
MachineStatus	yes	yes	String	Connection status of the server. Valid values: OFFLINE and ONLINE. Example: ONLINE
MachineType	yes	yes	Int64	0: Basic Edition. 1: Professional Edition. 2: Ultimate Edition. Example: 1
MachineWanIp	yes	yes	String	Public IP address of the server. Example: 124.2.4.55
ModifyTime	yes	yes	String	Handling time. Example: 2021-03-30 19:17:28
Pid	yes	yes	String	Process ID. Example: 1
Platform	yes	no	Uint64	System type. 2: Windows; 4: Linux. Example: 1
PsTree	yes	yes	String	Process tree in the JSON format. pid: process ID. exe: file path. account: user group and user to which the process belongs. cmdline: command to be run. ssh_service: SSH service. ssh_source: login source. Example: "{\"pid\":134,\"exe\":\"/usr/bin/bash\",\"account\":\"root:root\",\"cmdl"
Quuid	yes	no	String	Server ID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116
References	yes	yes	Array of String	Reference link. Example: ["http://www.domain.com"]
RegexBashCmd	yes	yes	String	Auto-generated regular expression. Example: rm -rf /tmp/t*
RuleCategory	yes	yes	Uint64	Rule type. 0: system rule. 1: custom rule. Example: 0
RuleId	yes	no	Uint64	Rule ID. A value of 0 indicates that the rule has been deleted or the effective scope has been modified. Example: 1
RuleLevel	yes	no	Uint64	Rule severity. 1: high. 2: medium. 3: low. Example: 1
RuleName	yes	no	String	Rule Name Example: redis_node_use
Status	yes	no	Uint64	Handling status. 0: to be handled. 1: handled. 2: added to the allowlist. 3: ignored. Example: 1
SuggestScheme	yes	yes	String	Suggestion scheme. Example: attempt to repair
Tags	yes	yes	Array of String	Tag. Example: ["tag-redis","tag-nginx"]
User	yes	yes	String	Login user. Example: user1
Uuid	yes	no	String	CWP ID. Example: acdd5474-6360-4fd4-bfc7-843162cb8116

StandardModeConfig

Configuration of standard blocking.

Referenced by the following interfaces: DescribeBanMode

name	required	NULL allowed	type	description
Til	yes	no	Uint64	Blocking period. Unit: seconds. Example: 300

HostLoginWhiteObj

Newly added login audit allowlist.

Referenced by the following interfaces: AddLoginWhiteLists

name	required	NULL allowed	type	description
EndTime	no	no	String	End time. Example: 2024-11-03 18:37:03
HostInfos	yes	no	Array of HostInfo	Information about the servers on which an allowlist takes effect. Example:View
IsGlobal	yes	no	Uint64	Whether it takes effect globally. 1: globally effective. 0: effective only on a single server. Example: false
Places	no	no	Array of Place	Regions in the allowlist. Example:View
Remark	no	no	String	Description. Example: Internal use
SrcIp	yes	no	String	Source IP addresses or CIDR blocks in the allowlist. Multiple IP addresses or CIDR blocks are separated with commas (,). Example: 10.0.1.11
StartTime	no	no	String	Start time. Example: 2024-11-03 18:37:03
UserName	yes	no	String	Users in the allowlist. Multiple usernames are separated with commas (,). Example: root

BaselineCustomRuleIdName

ID and name of a custom baseline rule.

Referenced by the following interfaces: DescribeBaselineItemIgnoreList, DescribeBaselineItemInfo, DescribeIgnoreHostAndItemConfig

name	required	NULL allowed	type	description
RuleId	yes	yes	Int64	Custom rule ID. Example: 1
RuleName	yes	yes	String	Custom rule name. Example: Custom

AttackSourceEdge

Path description in attack backtracking.

Referenced by the following interfaces: DescribeAttackSource

name	required	NULL allowed	type	description
From	yes	no	String	Starting node. Example: node_a
To	yes	no	String	Target node. Example: node_b

DefaultStrategyInfo

Basic information about the default policy.

Referenced by the following interfaces: DescribeBaselineDefaultStrategyList

name	required	NULL allowed	type	description
StrategyId	yes	no	Uint64	Policy ID. Example: 1
StrategyName	yes	no	String	Policy name. Example: International standard baseline

MaSelfLearnPolicy

Referenced by the following interfaces: DescribeMaSelfLearnPolicyList

name	required	NULL allowed	type	description
CreateTime	no	yes	String	Creation time. Example: 2023-10-10 00:00:00
DestIP	no	yes	String	Policy IP, assigned here when DestLabels is empty. Example: 2.2.2.2
DestLabels	no	yes	Array of MaLabel	Target tags Example:View
DestPort	no	yes	Uint64	Target port. Example: 8080
Id	no	yes	Uint64	Self-Learning policy ID. Example: 1
MatchCount	no	yes	Uint64	Number of packets hit. Example: 1
ModifyTime	no	yes	String	Update time. Example: 2023-10-10 00:00:00
SrcIP	no	yes	String	Policy IP, assigned here when SrcLabels is empty. Example: 1.1.1.1
SrcLabels	no	yes	Array of MaLabel	Source label Example:View
UniqueId	no	yes	String	Unique ID of the self-learning policy. Example: uniqdgs

BruteAttackRule

Standard blocking rule.

Referenced by the following interfaces: ModifyBruteAttackRules

name	required	NULL allowed	type	description
LoginFailTimes	yes	no	Uint64	Number of failed brute force attack events. Example: 6
TimeRange	yes	no	Uint64	Time period during which brute-force attack events occurred. Unit: seconds. Example: 1

KeyValueInfo

Key-Value index configuration

Referenced by the following interfaces: DescribeLogIndex

name	required	NULL allowed	type	description
CaseSensitive	yes	no	Bool	Whether it is case-sensitive. Example: false
KeyValues	yes	yes	Array of KeyValueArrayInfo	Key-value pair information for which you want to create an index. Example:View

MalwareRisk

Risk notifications for malicious files.

Referenced by the following interfaces: DescribeMalwareRiskWarning

name	required	NULL allowed	type	description
CreateTime	yes	no	String	Detection time. Example: 2022-01-01 00:00:00
Id	yes	no	Uint64	Unique ID. Example: 10001
MachineIp	yes	no	String	Server IP address. Example: 1.1.1.1
VirusName	yes	no	String	Virus name. Example: Linux.Trojan.Downloader.Snkl

CKafkaTopicInfo

Name of the CKafka topic.

Referenced by the following interfaces: DescribeLogDeliveryKafkaOptions

name	required	NULL allowed	type	description
TopicID	yes	no	String	Topic ID. Example: topic_gsyds
TopicName	yes	no	String	Topic name. Example: topic_dsyg

SecurityTrend

Security trend statistics.

Referenced by the following interfaces: DescribeSecurityTrends

name	required	NULL allowed	type	description
Date	yes	no	Date	Time when the event occurred. Example: 2021-07-11
EventNum	yes	no	Uint64	Number of events. Example: 10

BroadcastInfo

Security notice details.

Referenced by the following interfaces: DescribeSecurityBroadcastInfo

name	required	NULL allowed	type	description
Content	yes	no	String	Rich text. Example: Vulnerability details
CreateTime	yes	no	String	Release time. Example: 2021-03-30 19:17:28
GotoType	yes	yes	Uint64	Location to redirect to. 0: no redirection. 1: file scanning and cleaning. 2: vulnerability scanning. 3: baseline check. Example: 1
Id	yes	no	Uint64	Unique ID of the notice. Example: 12
Subtitle	yes	no	String	Subtitle of the notice. Example: The new version supports vulnerability fixing.
Title	yes	yes	String	Title of the notice. Example: Vulnerability outbreak
Type	yes	no	Uint64	Type. 0: emergent notification. 1: feature update. 2: industrial honor. 3: version release. Example: 1

AssetDiskPartitionInfo

Information about asset management disk partitions.

Referenced by the following interfaces: DescribeAssetDiskList, DescribeAssetMachineDetail

name	required	NULL allowed	type	description
Name	yes	no	String	Partition name. Example: /dev/vda1
Path	yes	no	String	Mount directory. Example: /data
Percent	yes	no	Float	Partition usage rate. Example: 78.81294
Size	yes	no	Uint64	Partition size in GB. Example: 50

name	required	NULL allowed	type	description
Type	yes	no	String	File system type. Example: ext4
Used	yes	no	Uint64	Used space size in GB. Example: 26

AssetAppBaseInfo

Basic resource information in the asset management module.

Referenced by the following interfaces: DescribeAssetAppList

name	required	NULL allowed	type	description
BinPath	no	no	String	Binary path. Example: /root
ConfigPath	no	no	String	Path of the configuration file. Example: /root
Desc	no	no	String	The description of the application. Example: app info
FirstTime	no	no	String	First collection time. Example: 2022-07-15 11:27:01
IsNew	no	yes	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	no	no	String	Private IP address of the server. Example: 10.0.0.11
MachineName	no	no	String	Server name. Example: agentyo
MachineWanIp	no	no	String	Public IP address of the server. Example: 192.168.0.204
Name	no	no	String	Application name. Example: php
OsInfo	no	no	String	OS information. Example: centos 64bit
ProcessCount	no	no	Uint64	Number of associated processes. Example: 1
ProjectId	no	no	Uint64	ID of the project to which the server belongs. Example: 1
Quuid	no	no	String	Host QUUID. Example: acdd5474-6360-46d4-bfc7-843162cb8116
Tag	no	yes	Array of MachineTag	Server tags. Example:View
Type	no	no	Uint64	Application type. 1: DPS. 2: database 3: security 4: suspicious application 5: system architecture 6: system application 7: web service 99: others Example: 1
UpdateTime	no	yes	String	Data update time. Example: 2011-11-11 12:12:12
Uuid	no	no	String	Host UUID. Example: acdd5474-6360-46d4-bfc7-843162cb8116
Version	no	no	String	Version number. Example: 1.0

AgentInstallResult

Agent installation result of a host.

Referenced by the following interfaces: DescribeAgentInstallResult, DescribeAgentInstallTaskResult, ModifyAssetsProtectionStatus

name	required	NULL allowed	type	description
AppId	no	yes	Uint64	App ID information Example: 1255080011
AssetId	no	yes	String	Asset ID Example: ins-figuhjbf
Code	no	yes	String	Error code. Empty: Successful. ErrLicenseNotEnough: Insufficient license. ErrStarNetOnline: TAT client not online. ErrStrAgentInstallTimeout: Task timeout. ErrStrLicenseLocked: Authorization operation in progress. Example: ErrStrLicenseLocked
MemberId	no	yes	String	member-id Example: member-jdkaghdjag
Message	no	yes	String	Error message. Example: PayResourceChangingQuota
Region	no	yes	String	Region. Example: ap-region1

AssetWebLocationPath

Virtual directory of a website in the asset management module.

Referenced by the following interfaces: DescribeAssetWebLocationPathList

name	required	NULL allowed	type	description
Group	yes	no	String	Group to which the file belongs. Example: root
Permission	yes	no	String	File permissions. Example: rwxay
RealPath	yes	no	String	Physical path. Example: /var/www/html
User	yes	no	String	File owner. Example: root
VirtualPath	yes	no	String	Virtual path. Example: /var/www/html

CreateVulFixTaskQuuids

QUUIDs of the servers for which the fix task is created.

Referenced by the following interfaces: CreateVulFix

name	required	NULL allowed	type	description
FixMethod	no	yes	Uint64	Repair method. 0: Update components or install patches. 1: Disable service. Example: 0
Quuids	yes	no	Array of String	Servers for which you want to fix the vulnerability. The vulnerability specified by VulId must be detected and in the To Be Fixed state on all specified servers. Example: ["e5b4724c-49ef-46ab-bd84-cdbad897e7e0"]
VulId	yes	no	Uint64	Vulnerability ID. Example: 1089

RegionListDetail

Details of the region list

Referenced by the following interfaces: DescribeMachineRegionList

name	required	NULL allowed	type	description
CloudFrom	no	yes	Uint64	0: cloud. 1: IDC. 2: Alibaba Cloud. 3: Huawei Cloud. 4: Amazon. 5: Microsoft. 6: Google. 7: Oracle. 8: Digital Ocean. Example: 0
MachineType	no	yes	String	Machine type. CVM: CVM. LH: Cloud Platform Lighthouse. ECM: Edge Computing Machine. BM: Bare Metal Service 1.0 Server. Other: Other servers (non-cloud servers). Example: CVM
RegionList	no	yes	Array of RegionInfo	Region List Example:View

AssetJarBaseInfo

List of JAR packages in the asset management module.

Referenced by the following interfaces: DescribeAssetJarList

name	required	NULL allowed	type	description
FirstTime	no	no	String	First collection time. Example: 2022-07-15 11:27:01
Id	no	no	String	ID of the JAR package. Example: 1024
IsNew	no	no	Int64	Whether it is newly added. 0: no. 1: yes. Example: 1
MachineExtraInfo	no	yes	MachineExtraInfo	Supplementary Information Example:View
MachineIp	no	no	String	Server IP. Example: 10.0.0.11
MachineName	no	no	String	Server name. Example: any-instance
MachineWanIp	no	no	String	Public IP address of a server. Example: 1.1.1.1
Md5	no	no	String	MD5 value of the JAR package. Example: fc702c8398075ea36970449c2b894dae
Name	no	no	String	Name. Example: com.apple.util
OsInfo	no	no	String	Operating system. Example: centos 64bit
Path	no	no	String	Path Example: /root
Quuid	no	no	String	Host QUUID. Example: acdd5474-6360-46d4-bfc7-843162cb8116
Status	no	no	Uint64	Whether it can be executed. 0: unknown. 1: yes. 2: no. Example: 1
Type	no	no	Int64	Type. 1: application program. 1: system library. 3: built-in library of a web service. 8: others. Example: 1
UpdateTime	no	yes	String	Data update time. Example: 2011-11-11 12:12:12
Uuid	no	no	String	Host UUID. Example: acdd5474-6360-46d4-bfc7-843162cb8116
Version	no	no	String	Version. Example: 1.0.1

ClsLogsetInfo

CLS Log Set Information

Referenced by the following interfaces: DescribeClsLogsets

name	required	NULL allowed	type	description
AssumerName	no	yes	String	Cloud Product Identifier Example: CWP
CreateTime	no	yes	String	Creation Time Example: 2021-04-01 08:00:00
LogsetId	no	yes	String	Logset ID Example: 25425
LogsetName	no	yes	String	Logset Name Example: redis_node_log
TopicCount	no	yes	Uint64	Total number of log topics. Example: 10

BaselineDownload

Parameters used to download exported baseline results.

Referenced by the following interfaces: DescribeBaselineDownloadList

name	required	NULL allowed	type	description
DownloadUrl	yes	no	String	The download URL. Example: https://cwp-1258144699.cos.ap-region1.mydomain.com/baseline-rule-view-result-20220823-095a9c44-7cc5-49c0-a02b-9a3e3442d5d6.csv?q-sign-algorithm=sha1
EndTime	yes	no	String	Completion time. Example: 2021-02-01 12:00:00
StartTime	yes	no	String	Start time. Example: 2021-02-01 12:00:00
Status	yes	no	Int64	Status. 0: not completed. 1: completed. Example: [0: not completed
TaskId	yes	no	Int64	Task ID. Example: 1661258891
TaskName	yes	no	String	Task Name. Example: baseline_rule_view_result_2021-02-01 12:00:00

AttackSourceNode

Attack backtracking node.

Referenced by the following interfaces: DescribeAttackSource

name	required	NULL allowed	type	description
EndTime	yes	no	String	End time. Example: 2021-03-30 19:17:28
EventId	yes	no	Uint64	Event ID. If no value is returned, no corresponding event is queried. Example: 1
EventType	yes	no	String	BRUTEFORCE: password cracking. MALWARE: trojan attack. BASH: high-risk command. RISK_DNS: malicious request. LOGIN: login from an unusual location. HOST: server node. TIME_ORDER: general node. Example: BRUTEFORCE
Ip	yes	no	String	Node IP address. This parameter is available when the value of EventType is HOST. Example: 10.0.0.1
Level	yes	no	Uint64	Severity. 0: informational. 1: low-risk. 2: medium-risk. 3: high-risk. 4: critical. Example: 0
NodeDesc	yes	no	String	Description of the general node. Example: desc
NodeDetail	yes	no	String	Node details. Example: detail
NodeId	yes	no	String	Node ID. Example: node-uniqueid
StartTime	yes	no	String	Start time. Example: 2021-03-30 19:17:28
TimeLineNum	yes	no	Uint64	Timeline ID. Nodes with the same timeline ID belong to the same timeline. Example: 1

DeliverTypeDetails

Details of a log shipping type.

Referenced by the following interfaces: DescribeLogClsDeliverInfo, DescribeLogKafkaDeliverInfo, ModifyLogKafkaAccess

name	required	NULL allowed	type	description
ErrInfo	no	no	String	Error message. Example: kafka: client has run out of available brokers to talk to: dial tcp 9.151.101.93:6232: i/o timeyay
LogName	no	yes	String	Logset name Example: web_logs
LogSetId	no	yes	String	Logset ID Example: 269e5897-009a-4c5e-9350-5898964eyayay
LogType	yes	no	Array of Int64	Log type of the security module. Valid values when the security module type is "1: virus scanning": 1: file scan; 2: abnormal login; 3: password cracking; 4: malicious request; 5: high-risk command; 6: local privilege escalation; 7: reverse shell; 8: abnormal process.\nValid values when the security module type is "2: vulnerability management": 1: emergency vulnerability; 2: Linux software vulnerability; 3: Windows system vulnerability; 4: Web-CMS vulnerability; 5: application vulnerability; 6: vulnerability defense. \nValid values when the security module type is "3: baseline management": 1: security baseline.\nValid values when the security module type is "4: advanced defense": 1: Java Webshell; 2: core file monitoring; 3: attack detection; 4: webpage tampering prevention.\nValid values when the security module type is "5: client-related": 1: client offline; 2: client uninstalled. \nValid values when the security module type is "6: asset fingerprint": 1: resource monitoring; 2: account; 3: port; 4: process; 5: software application; 6: database; 7: web application; 8: web service; 9: web framework; 10: website; 11: JAR package; 12: startup service; 13: scheduled task; 14: environment variable; 15: kernel module.\nValid values when the security module type is "7: host list": 1: host list. \nValid values when the security module type is "8: client log": 1: client log; 2: DNS log; 3: process snapshot; 4: network 5-tuple; 5: file write; 6: login record. Example: [1,2]
Region	no	yes	String	Logset region Example: ap-region1
SecurityType	yes	no	Uint64	Security module type. 1: intrusion detection; 2: vulnerability management; 3: baseline management; 4: advanced defense; 5: client security; 6: asset fingerprint; 7: host list; 8: client reporting. Example: 1
Status	no	no	Uint64	Log shipping status. 1: not enabled. 1: normal. 2: abnormal. Example: 1
StatusTime	no	no	Int64	Timestamp of last status reporting. Example: 1
Switch	yes	no	Uint64	Log shipping status. 0: disabled. 1: enabled. Example: 1
TopicId	yes	no	String	Topic ID. Example: topic-70s2ayay
TopicName	yes	no	String	Topic Name Example: log-recive

RegionSet

Region information.

Referenced by the following interfaces: DescribeBanRegions

name	required	NULL allowed	type	description
RegionName	yes	no	String	The region name. Example: region1
ZoneSet	yes	no	Array of ZoneInfo	Information on availability zones. Example:View

PushTaskResult

Scan result of a task delivered for quick protection.

Referenced by the following interfaces: CreateQuickProtectSetting

name	required	NULL allowed	type	description
FailureReason	yes	no	String	Reason for the delivery failure. Example: Checking...
IsSuccess	yes	no	Bool	Whether the task is successfully delivered. Example: true
TaskId	yes	no	Uint64	Task ID. Example: 1
TaskType	yes	no	String	Task type. Vul: vulnerability detection. Malware: file scanning and cleaning. Baseline: baseline check. AutoBan: automatic blocking. Example: Vul

MaPod

Referenced by the following interfaces: DescribeMaPodList

name	required	NULL allowed	type	description
AlarmCount	no	yes	Int64	Number of workload alarms. Example: 10
ClusterId	no	yes	String	cluster ID Example: cls-ogbbasz4
ClusterName	no	yes	String	Cluster Name Example: any_dev1
Id	no	yes	Int64	ID Example: 1
IsEnabled	no	yes	Int64	Whether monitoring is enabled (1: Enabled; 0: Disabled). Example: 1
IsNew	no	yes	Int64	Whether it is added in 15 days (1: Yes; 0: No). Example: 1
IsSupportMa	no	yes	Int64	Whether to support micro-alarms (1: Yes; 0: No). Example: 0
Labels	no	yes	Array of MaLabel	Tag. Example:View
LearnEndTime	no	yes	String	End time of learning for a single workload. Example: 2024-01-01 00:00:00
LearnStartTime	no	yes	String	Start time of learning for a single workload. Example: 2024-01-01 00:00:00
Name	no	yes	String	Server name. Example: redis_node_cvm
Namespace	no	yes	String	Namespace of the pod. Example: system
NotSupportMaCode	no	yes	Int64	Reason for not supporting micro-alarms [0: Supported; 1: Low client version; 2: Not premium edition; 3: Client not installed]. Example: 0
PodIp	no	yes	String	Pod IP Example: 10.0.0.1
Status	no	yes	String	Pod status Example: Running

ErrorCode

Feature Description

If there is an Error field in the response, it means that the API call failed. For example:

```
{
    "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"
    }
}
```

Code in Error indicates the error code, and Message indicates the specific information of the error.

Error Code List

Common Error Codes

Error codes	Description
AuthFailure.InvalidSecretId	Invalid key (not a Cloud API key type).
AuthFailure.MFAFailure	MFA failed.
AuthFailure.SecretIdNotFound	Key does not exist. Check if the key has been deleted or disabled in the console, and if not, check if the key is correctly entered. Note that whitespaces should not exist before or after the key.
AuthFailure.SignatureExpire	Signature expired. Timestamp and server time cannot differ by more than five minutes. Please ensure your current local time matches the standard time.
AuthFailure.SignatureFailure	Invalid signature. Signature calculation error. Please ensure you've followed the signature calculation process described in the Signature API documentation.
AuthFailure.TokenFailure	Token error.

Error codes	Description
AuthFailure.UnauthorizedOperation	The request does not have CAM authorization.
DryRunOperation	DryRun Operation. It means that the request would have succeeded, but the DryRun parameter was used.
FailedOperation	Operation failed.
InternalError	Internal error.
InvalidAction	The API does not exist.
InvalidParameter	Incorrect parameter.
InvalidParameterValue	Invalid parameter value.
LimitExceeded	Quota limit exceeded.
MissingParameter	A parameter is missing.
NoSuchVersion	The API version does not exist.
RequestLimitExceeded	The number of requests exceeds the frequency limit.
ResourceInUse	Resource is in use.
ResourceInsufficient	Insufficient resource.
ResourceNotFound	The resource does not exist.
ResourceUnavailable	Resource is unavailable.
UnauthorizedOperation	Unauthorized operation.
UnknownParameter	Unknown parameter.
UnsupportedOperation	Unsupported operation.
UnsupportedProtocol	HTTPS request method error. Only GET and POST requests are supported.
UnsupportedRegion	API does not support the requested region.

Service Error Codes

Error codes	Description
FailedOperation.PartSeparate	Failed to isolate all or part of servers.

Error codes	Description
FailedOperation.AgentOffline	The agent is offline.
FailedOperation.APIServerFail	Failed to call the API service.
InvalidParameter.ReverShellKeyFieldAllEmpty	The process name, target IP address, and target port cannot be left empty at the same time.
FailedOperation.CloseProVersion	Failed to deactivate CWP Pro.
InvalidParameterValue	The parameter value is invalid.
FailedOperation.MachineDelete	The server was uninstalled.
InvalidParameter.RegexRuleError	The format of the regular expression parameter is invalid.
InvalidParameter.IllegalRequest	Invalid request.
LimitExceeded.AreaQuota	The maximum number of entries to be added in batches is exceeded.
InvalidParameter.DateRange	The time range format is incorrect.
InvalidParameter.NameHasRepetition	The name already exists.
ResourceNotFound	The resource does not exist.
FailedOperation.RescanVul	Failed to scan for vulnerabilities again.
OperationDenied	Operation denied.
InternalError.MainDBFail	Failed to operate data.
ResourceInsufficient	Insufficient resource.
UnsupportedOperation	Unsupported operation.
FailedOperation.Recover	Failed to recover the trojan.
InvalidParameter.MissingParameter	Missing parameter.
InvalidParameter.InvalidFormat	Incorrect parameter format.
FailedOperation.LicenseExceeded	The number of available licenses is insufficient, and one more license is required. Please purchase a new license.
InvalidParameter.RuleHostDuplicateErr	Duplicate server for a rule API.

Error codes	Description
InvalidParameter	Invalid parameter.
FailedOperation.Export	Failed to export.
FailedOperation.TooManyStrategy	The maximum number of baseline policies is exceeded.
AuthFailure	CAM signature or authentication error.
InvalidParameter.RuleHostipErr	Incorrect server IP address for a rule API.
ResourceNotFound.MachineNotFound	The specified server to scan does not exist.
MissingParameter	Missing parameter.
InvalidParameter.ParsingError	Parameter parsing error.
FailedOperation.SingleSeparate	Failed to isolate a single server.
InvalidParameter.PortNoValid	Invalid port format.
InvalidParameterValue.TagNameLengthLimit	The tag name cannot contain more than 15 characters.
FailedOperation.OpenProVersion	Failed to activate CWP Pro.
FailedOperation.PrePayMode	Unable to disable the prepaid Pro edition. Please disable it in Billing Center.
InternalError	Internal error.
FailedOperation.ProtectStartFail	Failed to enable protection.
FailedOperation	Operation failed.
UnknownParameter	Unknown parameter error.
ResourceInUse	The resource is in use.
AuthFailure.UnauthorizedOperation	The user failed authentication.
ResourceUnavailable	The resource is unavailable.
FailedOperation.NoProfessionHost	No servers with CWP Pro exist.
UnauthorizedOperation	Unauthorized operation.
LimitExceeded	The quota limit has been reached.
InvalidParameter.IpNoValid	Invalid IP address format.