Cloud Workload Protection Platform

Cloud Workload Protection Description

Copyright Notice

Trademark Notice

Tencent Cloud

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Cloud Workload Protection Description
Function Behavior Description

Last updated: 2025-02-27 11:17:56

Web Shell Detection

Web shells are common in hackers' attacks. The CWPP agent will scan newly created web program files on the server for suspicious risks. For a small number of files that are suspected to be web shells, CWPP reports them to Tencent Cloud, which then conducts further detection through the machine learning detection engine. After detection, the sample files will be deleted in real time. CWPP runs a full scan every day by default. No private data will be extracted in this process.

Abnormal Login Reminder

The abnormal login reminder allows you to identify abnormal admin logins. The source IP, time, login user name and login status data in the login log need to be collected for computing risks. The login log data is retained on cloud for one month.

Password Cracking Reminder

Detect password cracking attacks against your server and show you the log and result of the attacks. It collects and analyzes information in the logs, including source IP address, time, login username, and login status. The login logs will be retained in the cloud for one month.

Malicious Trojans and Virus Detection

Malicious Trojans and virus programs usually steal user data or launch attacks, consuming a large amount of system resources and causing business disruptions. The client will collect the hash fingerprints of suspicious malicious programs to the cloud, where the Cloud Scan module will inspect the hash fingerprints. If the cloud hash library does not have a record of the file, the executable file will be reported to the cloud and inspected by the cloud antivirus engine. After inspection, the sample file will be deleted in real time. The host security system provides a full-disk scan service every day by default, and no user privacy data will be extracted during the detection process.

Vulnerability Alert

The current CWPP supports detecting Linux and Windows vulnerabilities and security baselines complying with Tencent Cloud requirements.

Upgrade and Maintenance

The upgrade and maintenance feature mainly informs users to upgrade the client to obtain the latest security protection services. The client software needs to collect the host security version number, OS configuration information, and security rule version number to the cloud for judgment and reminders. No private data will be extracted in this process.

Agent Process Description

Last updated: 2025-02-27 11:18:13

Name	Windows	Linux
Program installation directory	C:\program files\qcloud\yunjing\ydeyes C:\program files\qcloud\yunjing\ydlive	/usr/local/qcloud/YunJing/
Process name	YDService main service process of the host security main service YDLive daemon process YDPython vulnerability & baseline scan plug-in YDQuaraV2 Trojan isolation plugin qtflame Asset Collection Plugin	YDService main service process of the host security main service YDLive daemon process YDPython vulnerability & baseline scan plug-in YDUtils process scan plug-in YDQuaraV2 Trojan isolation plugin qtflame Asset Collection Plugin tcss-agent container baseline scan plug-in tcss-scan container mirror scan plug-in
Registered service name	YDService YDLive YDEdr	-

The port used by the agent program is randomly returned by the system, and there is no fixed port range. If the used port conflicts with the port for business, restart the agent program.

- Agent restart commands (Linux)

  1.1 Suspend the client program service.

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

  1.2 Restart the client.

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

- Agent restart commands (Windows)
  Enter the following commands or open Task Manager, locate YDService, and right-click to restart the agent.

1.1 Suspend the client program service.

```
net stop YDService
```

1.2 Restart the client.

```
net  start YDService
```

Security Baseline Detection Checklist

Last updated: 2025-02-27 11:18:30

This document will introduce the security baseline detection list of Host Security.

> **Note:**
> The security baselines will take effect immediately after the product is configured.

Name	Level	Vul_type
CouchDB unauthorized access	High	Improper configuration
Docker Daemon management port 2375 open	High	Remote code execution
Elasticsearch unauthorized access	High	Improper configuration
JavaRMI remote code execution	High	Remote code execution
Jenkins without authentication can lead to command execution	High	Remote code execution
Kubelet unauthorized access	High	Security baseline
Weak password detection in Linux system	High	Remote code execution
MongoDB unauthorized access	High	Improper configuration
MySQL weak password detection	High	Weak password
NFS misconfiguration leading to mountable sensitive directory	High	Improper configuration
Redis baseline compliance check	High	Remote code execution

Improper RPCBind configuration detection	High	Security baseline
Rsync weak password detection	High	Weak password
Rsync access without password	High	Improper configuration
Tomcat weak password detection	High	Weak password
Windows user weak password detection	High	Weak password
Xampp default FTP password	High	Information leakage
Backup files exist in the website directory	High	Information leakage
FTP anonymous login detection	Chinese	Information leakage
IIS configuration error leads to parsing vulnerability	Middle	Improper configuration
Memcached UDP port can be exploited for DDOS Amplify Attack	Middle	Information leakage
PHP-FPM misconfiguration	Middle	Security baseline
PostgreSQL compliance check	Middle	Remote code execution
Information leakage caused by .git folder in web directory	Chinese	Information leakage
Information leakage caused by .svn folder in web directory	Middle	Information leakage
Windows hidden account detection	Middle	Security baseline
Windows shadow account detection	Middle	Remote code execution
ZooKeeper unauthorized access	Chinese	Improper configuration

Hadoop unauthorized access	Low	Remote code execution
sudo no password user detection	Low	Security baseline
Tomcat example directory detection	Low	Security baseline
The phpinfo file exists in the web directory	Low	Information leakage
Status check of Windows guest account	Low	Security baseline

JSON Format Alarm Data Resolution

Last updated: 2025-02-27 11:18:55

This document will introduce the transmission fields and descriptions of various alarms that users will receive after setting to receive JSON format alarm data in Alarm Settings > **Robot Notification**.

> **Description**
> Alarm Settings > **Robot notifications** are independent of the message center's robots and are not related.

Public Field

Example

```
{
    "uin": "1000xxxxxx21",
    "nickname": "Test Account",
    "server": "172.x.x.41 [test machine]",
    "instance_id": "ins-xxxxxxxx",
    "region": "Southwest China (Chengdu)",
    "time": "2023-10-30 09:24:20"
}
```

Field description

Field Name	Description
uin	<User UIN>
nickname	User Nickname
server	Machine IP [Machine Alias]
instance_id	Machine Instance ID
region	Machine Region
time	Event Time

Abnormal Login

Example

```
{
    "event_type": "abnormal login",
    "src_ip": "43.x.x.41",
    "area": "Hong Kong (China)",
    "level": "high risk"
}
```

Field description

Field Name	Description
src_ip	Source IP
area	Source location
level	Danger Level

Password Cracking

Example

```
{
    "event_type": "password cracking",
    "src_ip": "43.x.x.41",
    "area": "Hong Kong (China)",
    "count": "3",
    "banned": "blocking successful"
}
```

Field description

Field Name	Description
src_ip	Source IP
area	Source location
count	Number of attempts
banned	Blocking Status

Malicious File Scan

Malicious File

Example

```
{
    "event_type": "malicious file",
    "file_type": "malicious",
    "path": "/root/bebinder_shell.jsp",
    "level": "Serious, your server is suspected of being hacked. It is
recommended to confirm promptly to avoid serious loss"
}
```

Field description

Field Name	Description
file_type	File Type
path	File path
level	Danger Level

Abnormal Processes

Example

```
{
    "event_type": "abnormal process",
    "pid": "5916",
    "path": "/root/2/ISHELL-v0.2/ishd"
}
```

Field description

Field Name	Description
pid	Process ID
path	Process Path

Malicious Requests

Example

```
{
    "event_type": "malicious request",
    "url": "massdns.ran6066.com",
    "count": "1"
}
```

Field description

Field Name	Description
url	Malicious Domain
count	Requests

High-Risk Commands

Example

```
{
    "event_type": "high risk command",
    "cmd": "iptables-restore -w 5 --noflush",
    "level": "high risk",
    "status": "Processing"
}
```

Field description

Field Name	Description
cmd	Command content
level	Threat Level
status	Processing Status

Local Privilege Escalation

Example

```
{
    "event_type": "local privilege escalation"
    "user": "0",
    "process": "privilege"
}
```

Field description

Field Name	Description
user	Privilege Escalation User
process	Privilege Escalation Process

Reverse Shell

Example

```
{
    "event_type": "Reverse Shell"
    "process": "mass_0",
    "dst_ip": "125.x.x.220",
    "dst_port": "8888"
}
```

Field description

Field Name	Description
process	Process name
dst_ip	Target Host
dst_port	Target Port

Java Memory Shell

Example

```
{
    "event_type": "Java Memory Shell"
```

```
    "type": "Java Memory Horse-Servlet"
    "pid": "3333",
    "argv": "masstest",
    "class_name": "massTest"
}
```

Field description

Field Name	Description
type	Java Webshell Type
pid	Process ID
argv	Process Parameters
class_name	Memory Horse Class Name

Core File Monitoring

Example

```
{
    "event_type": "core file",
    "rule_name": "adwqdadwqd",
    "exe_path": "/usr/bin/systemd-tmpfiles",
    "file_path": "/home",
    "count": "1",
    "level": "high risk"
}
```

Field description

Field Name	Description
rule_name	Hit rule name
exe_path	Process Path
file_path	File path
count	Number of Events

level	Threat Level

Network Attack

Example

```
{
    "event_type": "network attack",
    "src_ip": "129.x.x.166",
    "city": "jiangsu province - Nanjing",
    "vul_name": "showdoc File Upload Vulnerability",
    "dst_port": "80",
    "status": "attempted attack"
}
```

Field description

Field Name	Description
src_ip	Source IP
city	Source City
vul_name	Vulnerability Name
dst_port	Target Port
status	Attack status

Client Offline

Example

```
{
    "event_type": "client offline",
    "offline_hour": "1"
}
```

Field description

Field Name	Description

offline_hour	Client offline duration

Uninstalling Client

```
{
    "event_type": "client uninstall",
}
```

Vulnerability Notification

Example

```
{
    "event_type": "vulnerability",
    "category": "Linux software vulnerability",
    "vul_name": "libexpat code execution vulnerability (CVE-2022-
40674)",
    "level": "Serious"
}
```

Field description

Field Name	Description
category	Vulnerability categorization
vul_name	Vulnerability Name
level	Threat Level

Baseline Notification

Example

```
{
    "event_type": "baseline"
    "category": "Linux system weak password detection"
    "rule_name": "Linux system weak password detection"
    "level": "high risk"
}
```

Field description

Field Name	Description
category	Baseline categorization
rule_name	Rule name
level	Threat Level

Ransomware Defense

Example

```
{
    "event_type": "anti-ransomware"
    "file_path": "/usr/bin/vi"
}
```

Field description

Field Name	Description
file_path	File Directory

Webpage Anti-Tampering

Tampering Successful

Example

```
{
    "event_type": "webpage tamper-proofing (successful tampering)",
    "protect_name": "important file",
    "protect_path": "/tmp",
    "recover_type": "file creation",
    "recovered_status": "unrecovered",
}
```

Field description

Field Name	Description
protect_name	Protection name
protect_path	Protection Directory
recover_type	Event type
recovered_status	Event status

Recovery Failure

Example

```
{
    "event_type": "webpage tamper-proofing (recovery failure)",
    "protect_name": "important file",
    "protect_path": "/tmp",
    "exception": "client offline"
}
```

Field description

Field Name	Description
protect_name	Protection name
protect_path	Protection Directory
exception	Failure Reason

Log Field Data Resolution

Last updated: 2026-03-12 11:51:28

Global Standard

- The log content is in JSON format.
- The log character encoding is unified to UTF-8 format.
- The log includes public fields and type-specific fields. See field description for details.
- Logs are currently divided into three types: event logs, asset logs, and client logs.

Log Type

The log type is determined by the public field cls_event_type. Currently, the log type values are explained as follows:

Event Log

Cls_event_type	Log Type Value
malware	Malicious File Scan
risk_process	Abnormal Process
hostlogin	Unusual Login
bruteattack	Password Cracking
risk_dns	Malicious Requests
bash	High-Risk Commands
privilege_escalation	Local Privilege Escalation
reverse_shell	Reverse Shell
emergency_vul	Urgent Vulnerability
linux_app_vul	Linux System Vulnerability
windows_sys_vul	Windows System Vulnerability
Web-CMS_vul	Web-CMS Vulnerability
application_vul	Application Vulnerability

baseline	Baseline
attack_logs	Network Attack
java_shell	Java Memory Horse
file_tamper	Core File Monitoring
tamper_protect_logs	Webpage Tamper-proofing Event
tamper_protect_exceptions	Webpage Tamper-proofing Exception
agent_uninstall	Client Uninstall
agent_offline	Client Offline

Asset Log

Cls_event_type	Log Type Value
machines	Host List
asset_system	Resource Monitoring
asset_account	Account
asset_netstat	Port
asset_process	Processes
asset_app	Software Applications
asset_database	Database
asset_web_app	Web Applications
asset_web_service	Web Services
asset_web_frame	Web Frameworks
asset_web_location	Websites
asset_jar	JAR Package
asset_init_service	Start Service
asset_scheduled_task	Scheduled Tasks

asset_env	Environment Variables
asset_core_module	Kernel Modules
asset_package	System Installation Package

Client Reporting Logs

Cls_event_type	Log Type Value
client_log	Host Raw Log
dns_log	DNS Log
process_snapshot	Process Snapshot Log
net_log	Network Quintuple Log
file_log	File Monitoring Log
login_log	Login Flow Log

<Event Log Field Descriptions>

Public Field Description

Field	Type	Description
id	string	Database Record ID
appid	string	User AppID
create_time	string	Event Creation Time
modify_time	string	Event Modification Time
cls_event_type	string	Event Type
event_status	string	Event Status (create, modify, delete)

File Detection and Elimination Field Description

Field	Type	Description
instance_id	string	Instance id
uuid	string	Machine UUID

hostip	string	Host IP
file_path	string	File path
md5	string	File MD5
filesize	string	File Size
file_create_time	string	File creation time
file_modify_time	string	File modification time
file_access_time	string	File access time
status	string	Status (Processing, Trusted, Isolated, Allowlisted File, File deleted, Isolation, Recovering, Event record deleted)
virus_name	string	Virus name
bwtype	string	Sample attributes (10: Allowlisted; 20~29: Blacklisted)
path_md5	string	File path MD5

Abnormal Process Field Description

Field	Type	Description
instance_id	string	Instance ID
uuid	string	Machine UUID
hostip	string	Host IP
pid	int	Process ID
exe_path	string	Process Path
exe_md5	string	Process MD5
exe_desc	string	Process details
exe_argv	string	Process Parameters
exe_create_time	string	Process creation time

exe_modify_time	string	Process modification time
exe_access_time	string	Process access time
status	string	Status (Processing, Trusted, Cleaned Up, exited)
start_time	string	Process start time
virus_name	string	Virus name
latest_scan_time	string	Latest scan time
pstree	string	Process tree details, JSON format
risk_level	string	Risk Level (Tip, Low, Medium, High, Critical)
pay_version	string	Machine version (Basic Version, Professional Version, Flagship Edition, Inclusive Edition)
rss	int	Process Memory
permission	string	Process permissions

Abnormal Login Field Description

Field	Type	Description
instance_id	string	Instance id
uuid	string	Machine UUID
hostip	string	Host IP
username	string	Login username
count	string	Number of logins (aggregated per minute)
src_ip	string	Login source IP address
dst_port	string	Login port
src_machine_name	string	Login source machine name
login_time	string	Login time

status	string	Status (Normal login, Abnormal login, Whitened, Deleted, Confirmed intrusion login, Processed, Ignored)
location	string	Position

Password Cracking Field Description

Field	Type	Description
instance_id	string	Instance ID
uuid	string	Machine UUID
hostip	string	Host IP
username	string	Username
count	string	Number of attempts
event_type	string	Event type (Brute Force Failure, Brute Force Success, Brute force non-existent account)
src_ip	string	Source IP
dst_port	string	Source port
src_machine_name	string	Source machine name
status	string	Status (Pending, Ignored, False alarm, Deleted, Allowlist hit, Processed, Allowlisted)
location	string	Position
banned	string	Block status (Not blocked, Blocked, Not blocked (blocking not enabled), Not blocked (non-professional version), Not blocked (allowlisted), Not blocked (no public IP bound), Block failed (API exception), Block failed (intranet not supported), Block failed (AZ not supported))

Malicious Request Field Description

Field	Type	Description
instance_id	string	Instance id
uuid	string	Machine UUID

hostip	string	Host IP
url	string	Domain name
pid	string	Process ID
process_name	string	Process name
cmd_line	string	Command Line
status	string	Status (Pending, Deleted, Allowlisted, User untrusted, Processed, Ignored)
access_count	string	Requests
query_time	string	First request time
merge_time	string	Recent request time

High-Risk Command Field Description

Field	Type	Description
instance_id	string	Instance ID
uuid	string	Machine UUID
hostip	string	Host IP
user	string	Executing user
platform	string	Platform
exec_time	string	Command execution time
bash_cmd	string	Executed command
status	string	Status (Processing, Dangerous command, Normal command, Ignored, Deleted)
rule_name	string	Matched rule name
rule_level	string	Command risk level (High, Medium, Low)

Local Privilege Escalation Field Description

Field	Type	Description

instance_id	string	Instance id
uuid	string	Machine UUID
hostip	string	Host IP
process_name	string	Process name
full_path	string	File path
pid	string	Process ID
cmd_line	string	Command Line
user_name	string	Executing user
user_group	string	Group of the executing user
proc_file_privilege	string	Process file permissions information
ppid	string	Parent process ID
parent_proc_name	string	Parent Process Name
parent_proc_user	string	User executing the parent process
parent_proc_group	string	Associated group of the user executing the parent process
parent_proc_path	string	Parent Process Path
find_time	string	Execution Time
proc_tree	string	Process Tree
sid	string	User session ID, currently defaults to 0
uid	string	User ID
gid	string	User group ID
euid	string	Valid user ID
egid	string	Valid user group ID

status	string	Status (Processing, Privilege Escalation Event, Allowlist, Processed, Ignored, Deleted)

Rebound Shell Field Description

Field	Type	Description
instance_id	string	Instance id
uuid	string	Machine UUID
hostip	string	Host IP
dst_ip	string	Target IP
dst_port	string	Destination Port
process_name	string	Executed Process
full_path	string	Process Path
pid	string	Process ID
cmd_line	string	Executed command
user_name	string	Executing user
user_group	string	Group of the executing user
ppid	string	Parent process ID
parent_proc_name	string	Parent Process Name
parent_proc_user	string	User executing the parent process
parent_proc_group	string	Associated group of the user executing the parent process
parent_proc_path	string	Parent Process Path
find_time	string	Execution Time
proc_tree	string	Process Tree

status	string	Status (Processing, Reverse Shell Event, Allowlist, Processed, Ignored, Deleted)

Vulnerability Field Description

Field	Type	Description
instance_id	string	Instance id
uuid	string	Machine UUID
hostip	string	Host IP
status	string	Vulnerability Status (Processing, Ignored, Fixed, Detecting, Fixing, Rolling Back, Fix Failed, Expired, Offline)
vul_category	string	Vulnerability Category (Web application vulnerabilities, system component vulnerabilities, Linux system vulnerabilities, Windows system vulnerabilities)
descript	string	Vulnerability Event Details
path	string	Vulnerability File Path
remark	string	Vulnerability Remark
name	string	Vulnerability Name
fix	string	Fix Description
cve_id	string	CVE number
reference	string	Reference Description
level	string	Vulnerability Level (Low, Medium, High, Note)
is_emergency	string	Urgent or not

Baseline Field Description

Field	Type	Description
instance_id	string	Instance ID
name	string	Baseline Name
uuid	string	Machine UUID

hostip	string	Host IP
status	string	Status (Failed, Ignored, Passed, Deleted, Detecting)
level	string	Level (Low, Medium, High, Serious)
descript	string	Description
remark	string	Remarks
rule_id	string	Baseline classification ID
category_name	string	Baseline classification name
item_id	string	Baseline rule ID
fix	string	Suggestions for Fix

Network Attack Field Description

Field	Type	Description
instance_id	string	Instance ID
uuid	string	Machine UUID
dst_port	int	Destination Port
src_ip	string	Source IP
type	string	Type, attempted attack/successful attack
status	string	Event status, Processing/Processed/Allowlisted/Ignored/Deleted/Defense enabled
count	int	<Event merge count times>
svc_ps	string	Service process details, JSON format
net_payload	string	Attack packet (plaintext)
merge_time	string	Event merge time (latest detection time)
host_op_type	string	Abnormal behavior type, no compromise behavior/RCE (command execution)/DNS log/write file
host_op_pstree	string	Abnormal behavior process tree, JSON format

host_op	string	Abnormal behavior content
hostip	string	Host IP

Java Memory Horse Field Description

Field	Type	Description
instance_id	string	Instance ID
uuid	string	Machine UUID
type	string	Trojan type (Filter type, Listener type, Servlet type, Interceptors type, Agent type, others)
exe	string	Java Process Path
argv	string	Java Process Command Line
pid	string	Java Process ID
class_name	string	Java Webshell class_name
loader_class_name	string	Memory Horse loader_class_name
super_class_name	string	Memory horse parent class super_class_name
interfaces	string	Memory horse interfaces
recent_found_time	string	Recent detection time
status	string	Status (Processing, Whitened, Deleted, Ignored, Manually processed)
file_exist	string	File existence (File does not exist, File exists)
class_file	string	File path of the class

Core File Monitor Field Description

Field	Type	Description
instance_id	string	Instance ID

uuid	string	Machine UUID
hostip	string	Host IP
hostname	string	Host Name
process_exe	string	Process Path
process_argv	string	Process command line arguments
target	string	Target file path
status	string	Status (Processing, Whitened, Deleted, Ignored, Manually processed)
event_count	string	Event occurrence count
rule_name	string	Rule Name
event_detail	string	Event details, JSON format
pstree	string	Process Tree
rule	string	Rule group details, JSON format
level	string	Level (None, High, Medium, Low)

Webpage Anti-Tampering Event Field Description

Field	Type	Description
instance_id	string	Instance id
uuid	string	Machine UUID
path	string	File path
recover_type	string	Recovery Type (Content modification recovery, Permission modification recovery, Ownership modification recovery, Deletion recovery, Add deletion)
has_recovered	string	Restore status (Unresolved, Resolved)
recover_time	string	Restoration time
is_manual_recover	string	Manual recovery (No, Yes)

is_deleted	string	Deletion status (Not deleted, Deleted)
status	string	Status (Processing, Confirm Malicious, Confirm False Positive)
file_type	string	File type (regular file, directory, symlink)

Webpage Anti-Tampering Abnormal Field Description

Field	Type	Description
instance_id	string	Instance id
quuid	string	Machine QUUID
exception	string	Exception type (no exception, exceeded limit, Agent offline, timeout, insufficient disk space, machine destroyed, file changed during backup, file not found during backup, exceeded limit, monitoring path is not a directory, exceeded limit, file type not supported, exceeded limit, number of files exceeds limit, exceeded limit, path too long, exceeded limit, file too large, exceeded limit, file read failed, exceeded limit, protection directory, too many subdirectories, other)
exception_message	string	Exception Note

Client Uninstall Field Description

Field	Type	Description
instance_id	string	Instance id
uuid	string	Machine UUID
pstree	string	Process Tree
uninstall_time	string	Uninstall Time

Client Offline Field Description

Field	Type	Description
instance_id	string	Instance id

uuid	string	Machine UUID
offline_time	string	Machine offline time

Asset Log Field Description

Public Field Description

Field	Type	Description
id	string	Database Record ID
appid	string	User AppID
host_name	string	Host Name
host_ip	string	Host private network IP
wan_ip	string	Host public network IP
instance_id	string	Instance id
os_name	string	Operating system name
os_type	string	Operating system type (Unknown, CentOS, Debian, Gentoo, RedHat, Ubuntu, WindowsServer, TencentOS, CoreOS, FreeBSD, SUSE)
create_time	int	Creation time in timestamp format
update_time	int	Asset update time, timestamp format
cls_event_type	string	Event Type
event_status	string	Event Status (create, modify, delete)

Host List Field Description

Field	Type	Description
quuid	string	Machine QUUID
machine_type	string	Machine Type (CVM, LH, Other, ECM)
region	string	Region
project_id	int	Project ID of the instance

instance_state	string	Instance Status (PENDING, LAUNCH_FAILED, RUNNING, STOPPED, STARTING, STOPPING, REBOOTING, SHUTDOWN, TERMINATING, TERMINATED)
restrict_state	string	Business status (NORMAL, EXPIRED, PROTECTIVELY_ISOLATED, TERMINATED_PRO_VERSION)
instance_name	string	Instance Name
private_ip_addresses	string	Private network address of the instance
public_ip_addresses	string	Public network address of the instance
ipv6_addresses	string	IPv6 address of the instance
vpc_id	string	vpc id
os_name	string	Operating system name
os_type	string	Operating system type (Unknown, CentOS, Debian, Gentoo, RedHat, Ubuntu, WindowsServer, TencentOS, CoreOS, FreeBSD, SUSE)
installed_cwp	int	Whether the Cloud Workload Protection Platform client is installed (0: Not installed, 1: Installed)
latest_sync_time	string	Last Synchronization Time

Resource Monitoring Field Description

Field	Type	Description
core_version	string	Kernel Version
boot_time	int	System boot time, Unix timestamp
cpu_info	string	CPU information
cpu_size	int	CPU quantity
cpu_load	float	CPU Uitilization
memory_size	int	Memory capacity: MB

memory_load	float	Memory Usage
disk_size	int	Hard disk quantity: MB
disk_load	float	Hard Disk Usage

Account Field Description

Field	Type	Description
group_name	string	Account GroupName
status	string	Account Status (block, enable)
is_root	string	Whether it has root permission
name	string	Account Name
type	string	Account Type (guest user, standard user, administrator user)
home_path	string	Home directory
shell	string	Shell path
password_change_time	string	Password modification time
password_due_days	int	Password expiration in days, -1 means never expire
password_lock_days	int	Password lock time in days, -1 means infinite
password_warn_days	int	Password expiration reminder in days
password_change_type	string	Password modification settings (non-modifiable, modifiable)
password_status	string	Password status (normal, about to expire, expired, locked)
login_type	string	Login method (non-login, key only, password only, key and password)
last_login_time	int	Last login time

last_login_terminal	string	Recent login terminal
last_login_ip	string	Recent login IP
disable_time	string	Account expiration time

Port Field Description

Field	Type	Description
name	string	Process name
version	string	Process version
path	string	Process Path
parent_process_name	string	Parent Process Name
pid	string	Process ID
user	string	Run user
group_name	string	User group
start_time	int	Startup time, Unix timestamp
param	string	Startup parameter
tty	string	Process TTY
port	string	Port
ppid	string	Parent process ID
proto	string	Port Protocol

Software Application Field Description

Field	Type	Description
name	string	Application Name
type	string	Application type (operation and maintenance tool, database, security application, suspicious application,

		system architecture, system application, WEB operation and maintenance, others)
bin_path	string	Binary Path
config_path	string	Configuration file path
process_count	int	Number of associated processes
version	string	Version No.

Process Field Description

Field	Type	Description
name	string	Process name
group_name	string	Process User Group
desc	string	Process description
path	string	Process Path
pid	string	Process ID
ppid	string	Parent process ID
parent_process_name	string	Parent Process Name
user	string	Run user
start_time	int	Start time
param	string	Startup parameter
tty	string	Process TTY
version	string	Process version
status	string	Process status (no, executable, interruptible, uninterruptible, paused status or tracking status, zombie state, to be destroyed, idle, wait for memory allocation)
package_name	string	Package name

Database Field Description

Field	Type	Description
name	string	Database Name
version	string	Version
port	string	Port
proto	string	Protocol
user	string	Run user
ip	string	Binding IP
config_path	string	Configuration file path
log_path	string	Log File Path
data_path	string	Data path
permission	string	Run Permission
error_log_path	string	Error Log Path
plugin_path	string	Plug-in Path
bin_path	string	Binary Path
param	string	Startup parameter

Web Application Field Description

Field	Type	Description
name	string	Application Name
desc	string	Application Description
version	string	Version
root_path	string	Root Path
service_type	string	Service type
domain	string	Site domain name
virtual_path	string	Virtual path

plugin_count	int	Number of plugins

Web Service Field Description

Field	Type	Description
name	string	Framework name
version	string	Version
bin_path	string	Binary Path
service_type	string	Service type
user	string	Startup user
install_path	string	Installation Path
config_path	string	Configuration Path
process_count	int	Number of associated processes

Web Framework Field Description

Field	Type	Description
name	string	Framework name
version	string	Version
lang	string	Language
service_type	string	Service type
path	string	Application Path

Web Site Field Description

Field	Type	Description
name	string	Domain name
port	string	Site Port
proto	string	Site Protocol
service_type	string	Service type

path_count	int	Number of Site Paths
user	string	Run user
ip	string	Binding IP
command	string	startup command

JAR Package Field Description

Field	Type	Description
name	string	Name
type	string	Type (application, system class library, Web Service Built-in Library, others)
status	string	Executable or not
version	string	Version
path	string	Path

Startup Service Field Description

Field	Type	Description
name	string	Name
type	string	Type
status	string	Default enabling status (enabled, not enabled)
user	string	Startup user
path	string	Path

Scheduled Task Field Description

Field	Type	Description
status	string	Default enabling status (enabled, not enabled)
cycle	string	Execution cycle
command	string	Execute a command or script

user	string	Startup user
config_path	string	Configuration file path
os_info	string	Operating System

Environment Variable Field Description

Field	Type	Description
name	string	Name
type	string	Type (user, system)
user	string	Startup user
value	string	Environment variable value

Kernel Module Field Description

Field	Type	Description
name	string	Name
desc	string	Description
path	string	Path
version	string	Version
size	int	Size

System Installation Package Field Description

Field	Type	Description
name	string	Installation Package Name
desc	string	Description
version	string	Version
install_time	int	Installation time, Unix timestamp
type	string	Type

<Client Log Field Description

Raw Log Field Description

Field	Type	Description
appid	int	User AppID
uuid	string	Machine UUID
instance_id	string	Instance id
path	string	Log File Path
tag	string	Tag (user-defined in the future)
time	string	Log Time
log	string	Log content

DNS Log Field Description

Field	Type	Description
appid	int	User AppID
quuid	string	Machine QUUID
uuid	string	Machine UUID
instance_id	string	Instance id
recv_time	int	Timestamp
domain	string	Domain name
hostip	string	Host IP
platform	string	Platform: Linux, Windows
pid	int	Process ID
process_path	string	Process Path
cmdline	string	Process command line arguments
count	int	Access count within the reporting cycle

Process Snapshot Log Field Description

Field	Type	Field Description
appid	string	Account AppID
quuid	string	Host QUUID (corresponding to CVM UUID)
uuid	string	Host UUID
hostip	string	Host IP (with backend connection IP)
instance_id	string	Instance ID
event_name	string	Event type: process – process event
pid	int	Process ID
ppid	int	Parent process ID
sid	int	Process session ID (Linux only)
uid	int	Process UID (Linux only)
gid	int	Process GID (Linux only)
euid	int	Process EUID (Linux only)
egid	int	Process EGID (Linux only)
report_type	int	Reporting type: 0 – real-time process, 1 – process snapshot
parent_proc_name	string	Parent process name
process_name	string	Process name
process_path	string	Process Path
cmdline	string	Process command line
user_name	string	Process startup user
process_md5	string	Process MD5
platform	string	Platform: Linux, Windows
time	int	Event collection timestamp
timestamp	string	<Event store date and time>

insert_time	int	Event store timestamp

Network Quintuple Log Field Description

Field	Type	Field Description
appid	string	Account AppID
quuid	string	Host QUUID (corresponding to CVM UUID)
uuid	string	Host UUID
hostip	string	Host IP (with backend connection IP)
instance_id	string	Instance id
event_name	string	Event type: net – Network Quintuple
pid	int	Process PID
proc_path	string	Process Path
argv	string	Process execution parameters
username	string	Process owner: User group
src_ip	string	Source IP
src_port	int	Source Port
dst_ip	string	Target IP
dst_port	int	Destination Port
first_time	int	First trigger time within the reporting cycle
last_time	int	Last trigger time within the reporting cycle
count	int	Trigger count within the reporting cycle
time	int	Event collection timestamp
timestamp	string	<Event storage date>
insert_time	int	Event store timestamp

File Monitoring Log Field Description

Field	Type	Field Description
appid	string	Account AppID
quuid	string	Host QUUID (corresponding to CVM UUID)
uuid	string	Host UUID
hostip	string	Host IP (with backend connection IP)
instance_id	string	Instance ID
event_name	string	Event type: file – file operation event
pid	int	Process ID
ppid	int	Parent process ID
session_id	int	Process session ID (Linux only)
uid	int	Process UID (Linux only)
gid	int	Process GID (Linux only)
file_path	string	Operation file path
cwd	string	Current execution path of the process
proc_path	string	Process Path
argv	string	Process command line
username	string	User of file operations
parent_proc_name	string	Parent process name
proc_name	string	Process name
proc_md5	string	Process MD5
proc_perm	string	Execution permission of the process file
proc_mtime	int	Process file modify time
proc_ctime	int	Process file change time
proc_atime	int	Process file access time
operation	string	File operation types: write–Write rename–

		Rename
file_size	int	File Size
file_mtime	int	Operation file modify time
file_ctime	int	Operation file change time
file_atime	int	Operation file access time
file_perm	string	Permission to operation file
file_owner	string	Ownership of operation file user
time	int	Event collection timestamp
timestamp	string	<Event store date and time>
insert_time	int	Event store timestamp

Login Flow Log Field Description

Field	Type	Field Description
appid	string	Account AppID
quuid	string	Host QUUID (corresponding to CVM UUID)
uuid	string	Host UUID
hostip	string	Host IP (with backend connection IP)
instance_id	string	Instance id
event_name	string	Event type: login – login event
src_ip	string	Source IP of login
dst_port	int	Target port of login
protocol	string	Log-in Protocol
count	int	Number of logins
event_type	string	Event status: success: Login successful fail: Login failed
time	int	Event collection timestamp

insert_time	int	Event store timestamp