Cloud Workload Protection Platform

Operation Guide

Product Documentation

Contents

Operation Guide
Security Dashboard

Last updated：2024-08-13 16:29:49

This document describes how to use Security Dashboard.

Overview

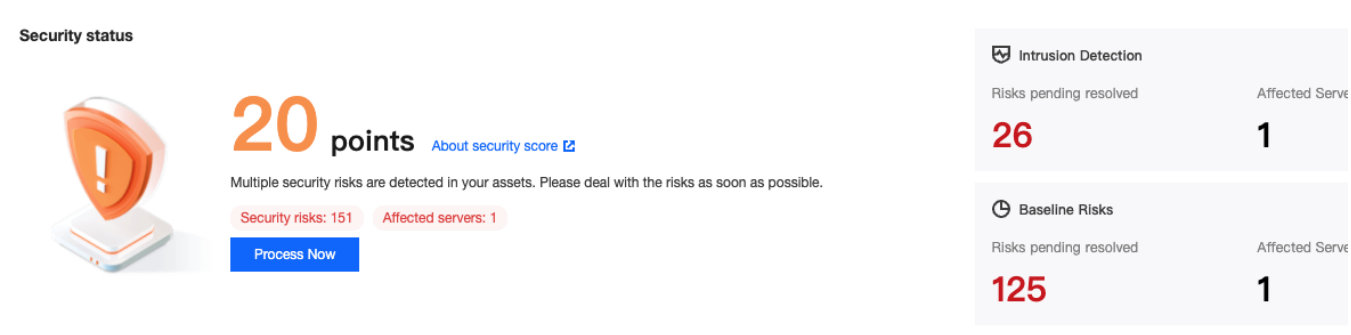
As the homepage of Cloud Workload Protection Platform (CWPP), Security Dashboard displays security score, pending risks, security protection status, risk trend, and new security events; pushes security notices to keep you updated with the latest threat intelligence of CWPP; provides documentation and suggestions to help you defend against intrusion and attacks and ensure your server security.

Operation Guide

1. Log in to the CWPP console.
2. Click **Security Dashboard** on the left sidebar. The fields and operations related to the feature are described as follows.

Security Status

1. The **Security Status** section presents the security score and risk information, and provides quick access to risk handling pages.



Security score: The score is calculated based on the number of security events and their threat level. For more information about the scoring rules, see Security Score Overview.
Risk information: It contains three categories of information: detected intrusions, vulnerability risks, and baseline risks, and shows the number of pending risks and the number of affected servers.

Intrusion Detection: Malicious File Scan, Unusual Login, Password Cracking, Malicious Requests, Reverse Shell, Local Privilege Escalation, and High-Risk Commands.
Vulnerability Risks: Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities in Vulnerability Management.
Baseline Risks: Only risks in Baseline Management.
Cyber Risks: Statistics on the number of pending attack risks and the number of affected hosts.
2. Click **Resolve Now** to open the pop-up of the risk processing details, where you can view detailed information on intrusion detection, vulnerabilities, baseline risks, and cyber risks. Click the corresponding **Risk Card** to navigate to the corresponding risk processing interface.

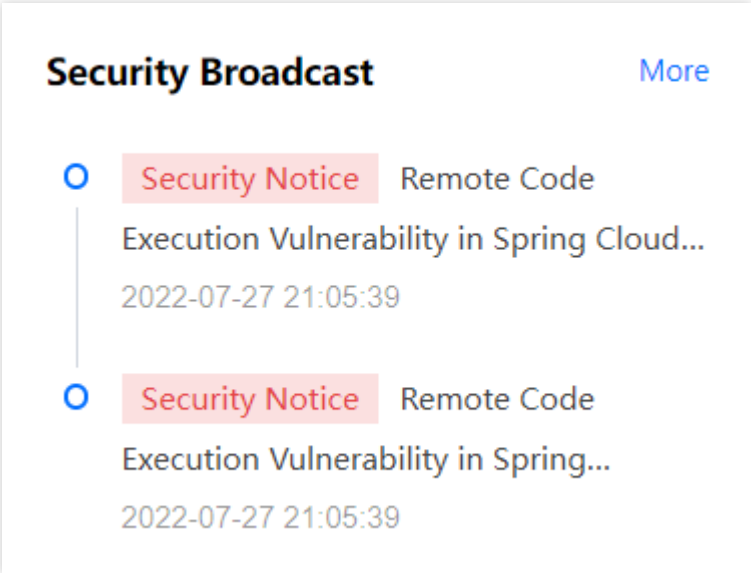
Level	Health Check Score	Font Color	Status Description
Good	90 - 100	Green	The asset security status is good. Continue to maintain and conduct regular inspections.
Medium	60 - 89	Orange	There are many security risks in the assets. It is recommended to process security events promptly.
Bad	20 - 59	Red	There are critical security risks in the assets. Process security events as soon as possible.

Note:
The lowest score for the CWPP status health check is 20.
Penalty items are calculated according to the classification of security events. Severity level classification of security events and rules of penalty:

Level	Security Events (calculated by the number of events)	Penalty Per Event	Maximum Total Penalty
Critical	Trojan files, brute-force attacks, and malicious requests	-40	-50
High	Severe vulnerabilities, high-risk vulnerabilities, critical baselines, high-risk baselines, abnormal log-in (high-risk), local privilege escalation, and reverse shell	-10	-20
Medium	Medium-risk vulnerabilities, and medium-risk baselines	-3	-10
Low	Low-risk vulnerabilities, and low-risk baselines	-2	-5
Other	Basic edition protection, or CWPP agent not installed	-1	-5

Security Intelligence

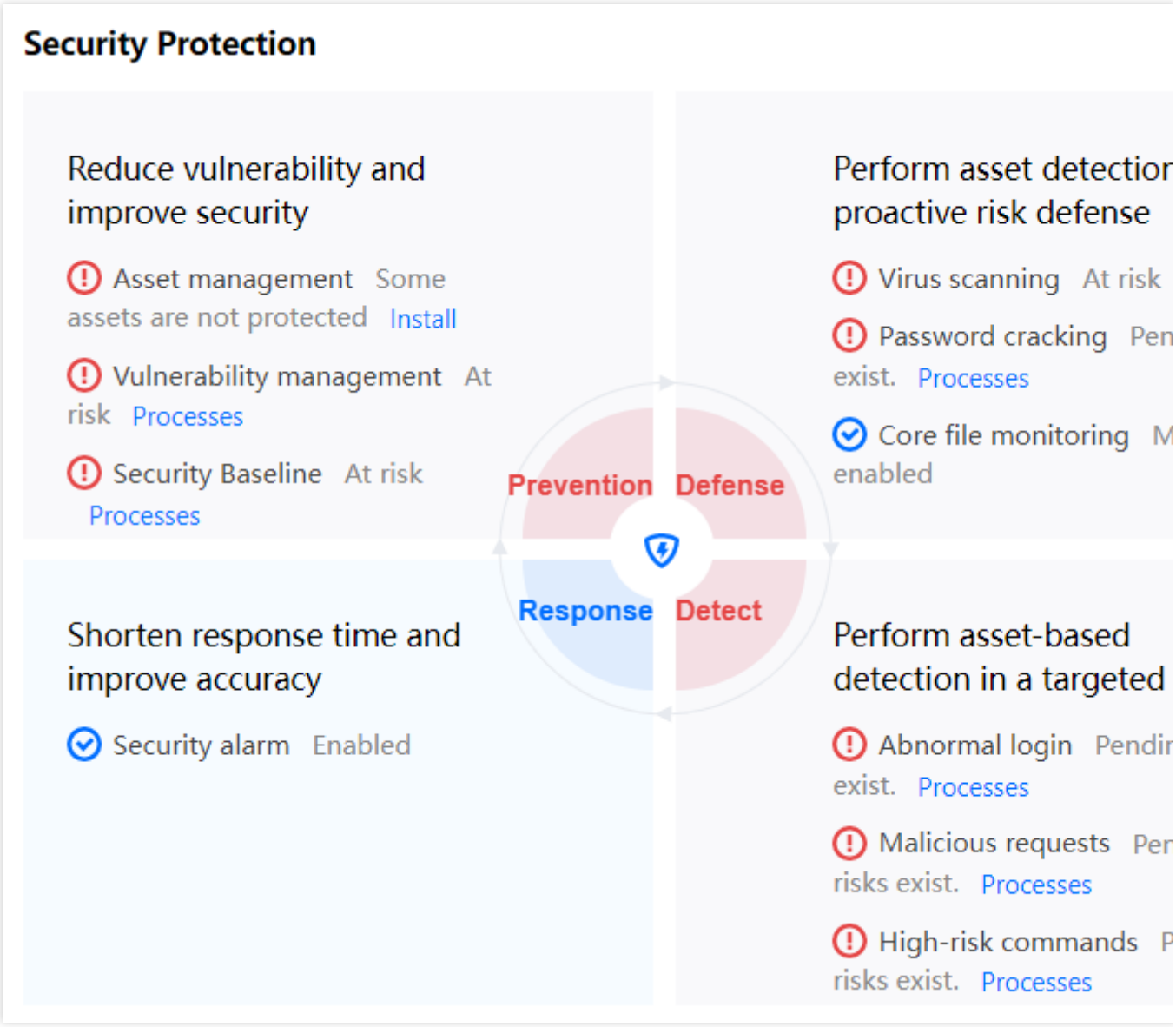
The **Security intelligence** section shows the feature updates, news about honors and awards, urgent notifications, and version release information.



Click the intelligence title to check details. Click **More** to view all the security intelligence.

Security Protection

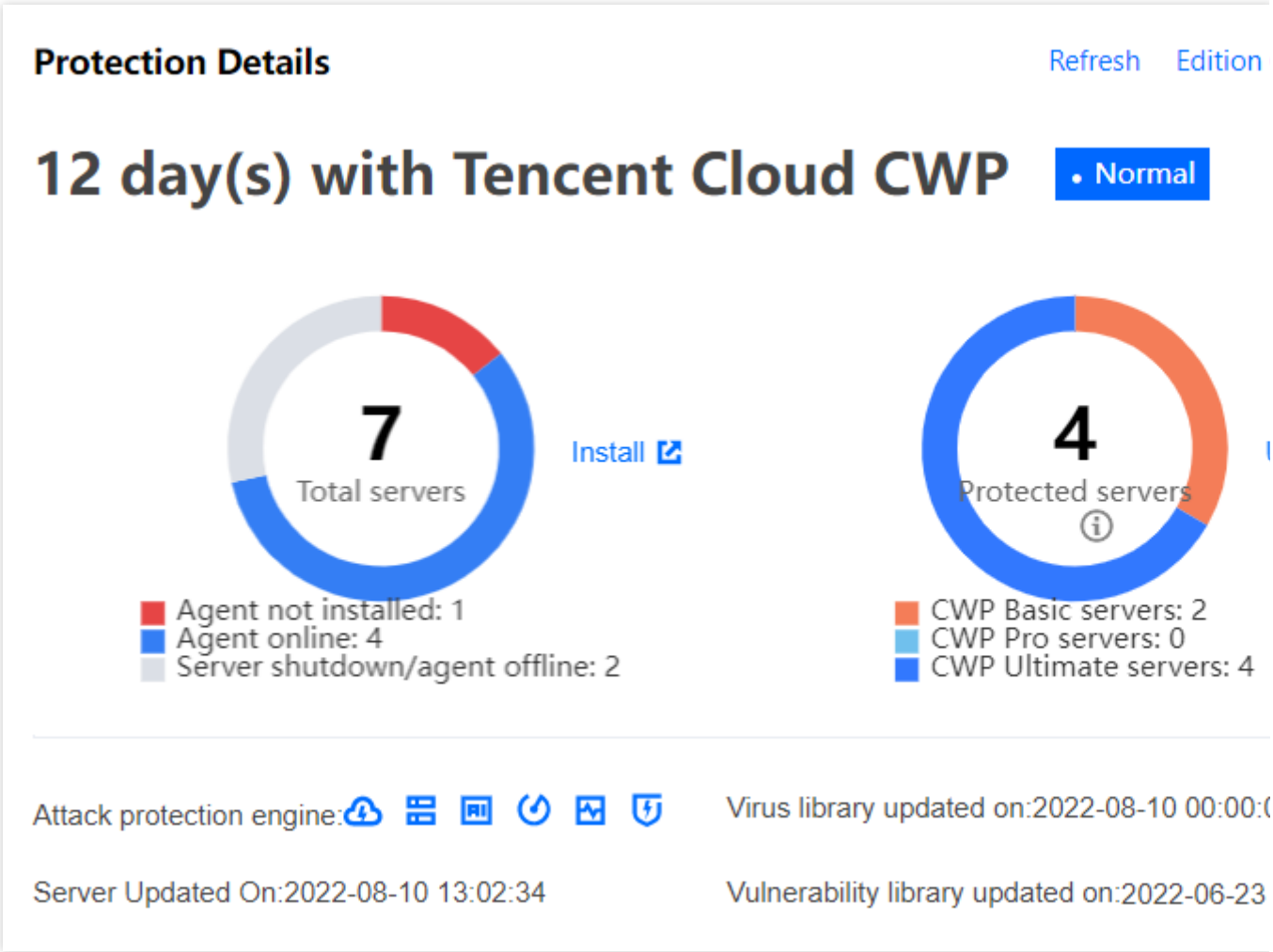
The **Security Protection** section displays the complete anti-intrusion solution (prevention-defense-detection-response) of CWPP, and the security protection items required for each process.



If all the protection items are enabled, you can get a clear picture of the security of your servers and get quick access to the risk handling pages.

Protection Details

The **Protection Details** section shows the usage data of various CWPP services.



Days of Protection: The total time the CWPP Agent has been installed on the server.

Total servers: The total number of Tencent Cloud servers (CVMs, Lighthouse servers, CPM 1.0, ECMs) and non-Tencent Cloud servers.

Protected servers: The total number of the servers protected by CWPP Pro/Ultimate.

Engines: If you have purchased the CWPP Pro/Ultimate licenses, six protection engines are automatically activated: Cloud Security Engine, BinaryAI Engine, TAV Engine, Unusual Behavior Engine, Threat Intelligence Engine, and Anti-Attack Engine.

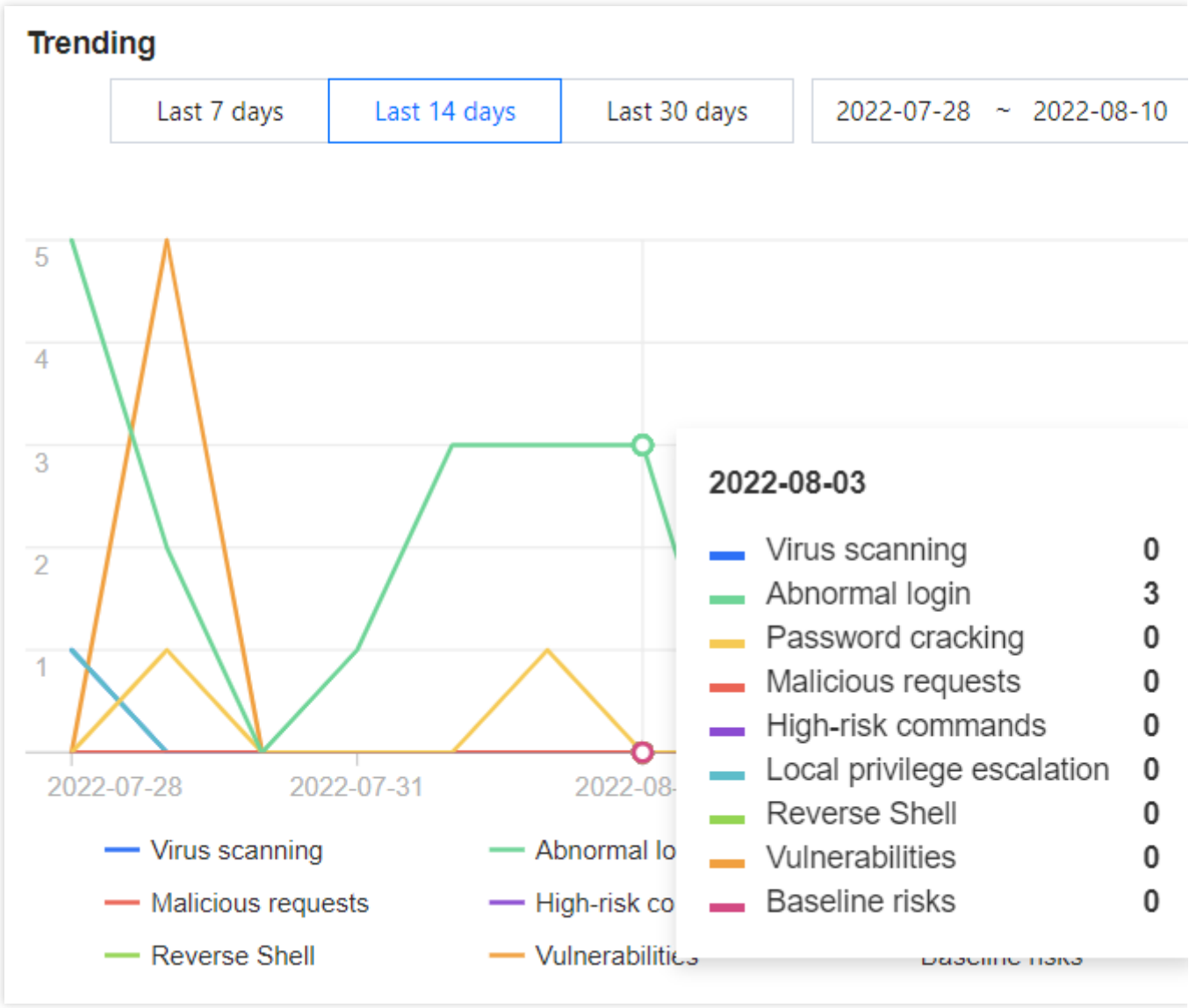
Virus database update time: The virus library is automatically updated at 0:00 every day.

Server update time: Click **Update now** in the upper right corner to manually update the server list.

Vulnerability Library Update Time: From time to time.

Risk Trend

On the **Risk Trend** section, the statistics of various risks are displayed in a line graph, which visually presents the risk trend of servers.



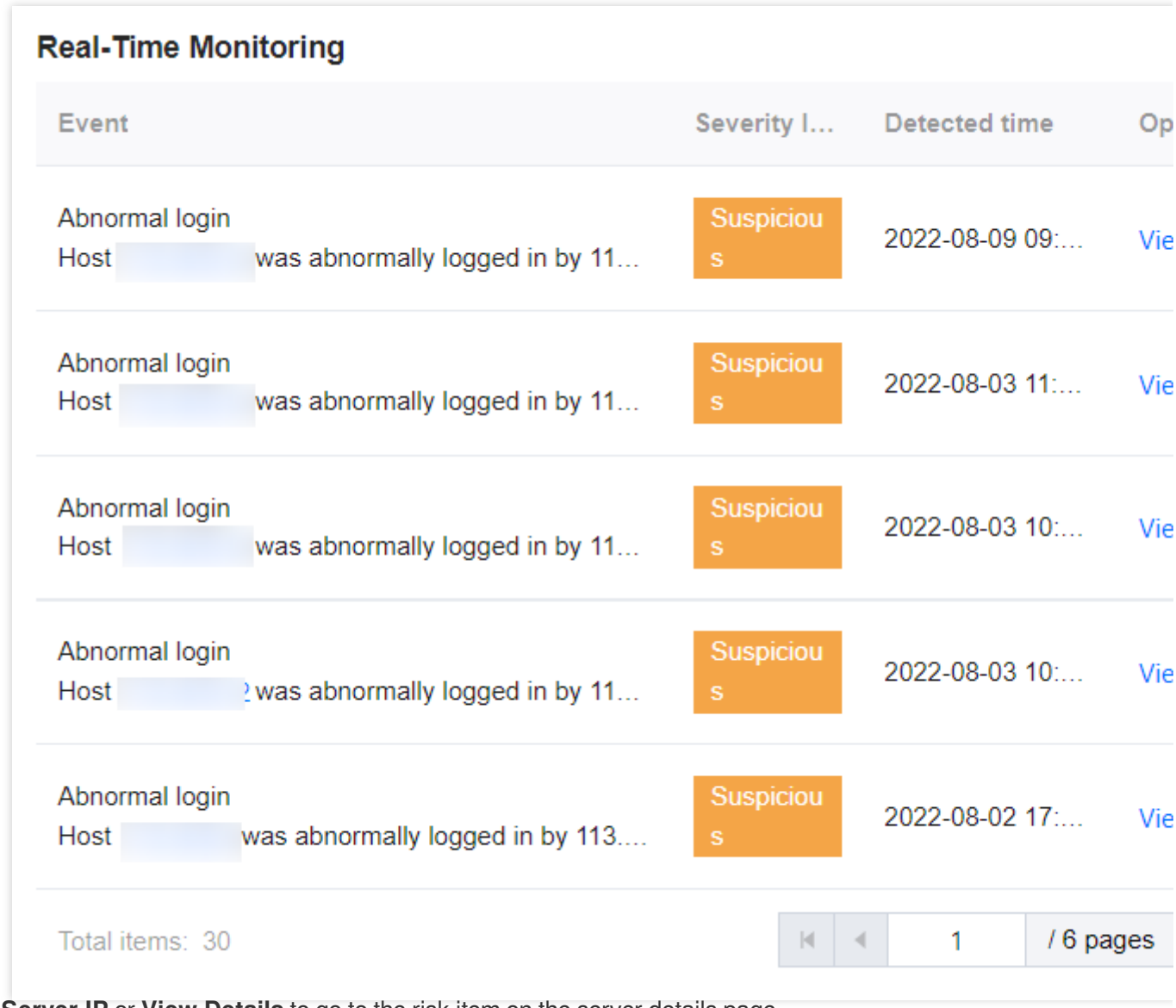
You can view the risk statistics for the last 7 days, the last 14 days, the last 30 days, or a custom date range. Click **Download** to export the risk statistics for the selected date range.

Note:

The number of risks is the number of new pending events on the current day and is updated every hour.

Real-time monitoring

The **Real-time monitoring** section displays the newly discovered security events in real time.



Click **Server IP** or **View Details** to go to the risk item on the server details page.

Asset Overview

Last updated：2024-08-13 16:29:49

This document describes how to use Assets Dashboard.

Overview

Assets Dashboard 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.

Important Notes

Asset Dashboard is available to all Tencent Cloud users. The collected asset fingerprint items vary with different CWPP editions, so the data displayed in Assets Dashboard varies with the editions. Only hosts with the paid protection edition can collect asset fingerprint data. Basic edition hosts must first upgrade the version.
The asset fingerprints collected by each edition are as follows:

CWPP Edition	Supported Asset Types
CWPP Basic (free)	N/A
CWPP Pro	10 items: Resource Monitoring, Accounts, Ports, Processes, Software Applications, Databases, Web Applications, Web Services, Web Frameworks, and Websites
CWPP Ultimate	16 items: 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

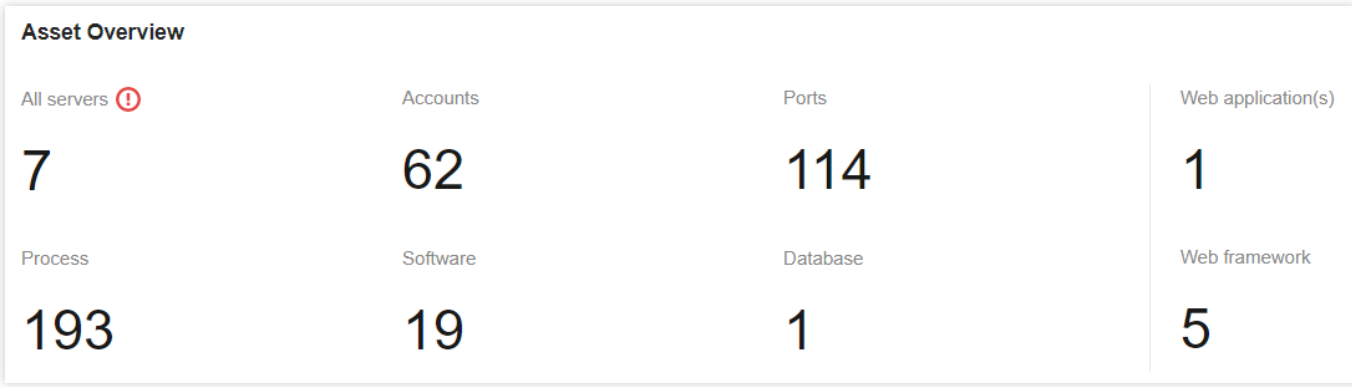
Note:
Asset fingerprint data is collected automatically every 8 hours (manual collection is supported).

Operation Guide

1. Log in to the CWPP console.
2. Click **Assets Dashboard** on the left sidebar. The fields and operations related to the feature are described as follows.

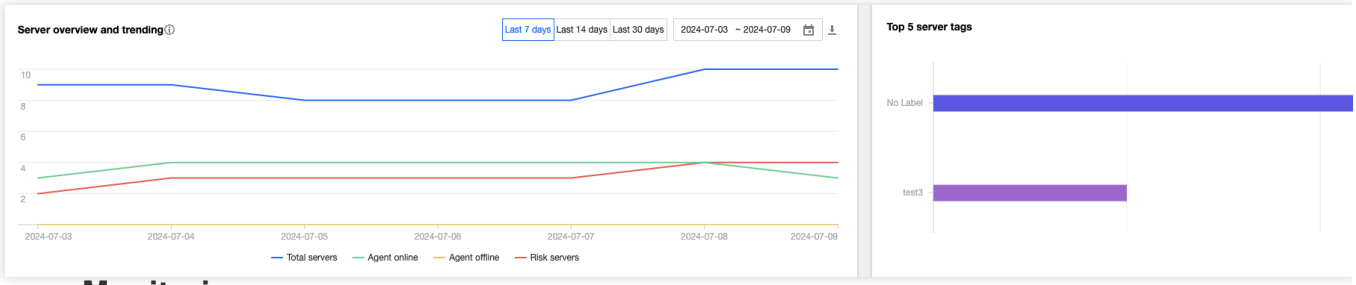
Assets Dashboard

The **Assets Dashboard** section displays the statistics of all assets and asset fingerprints.



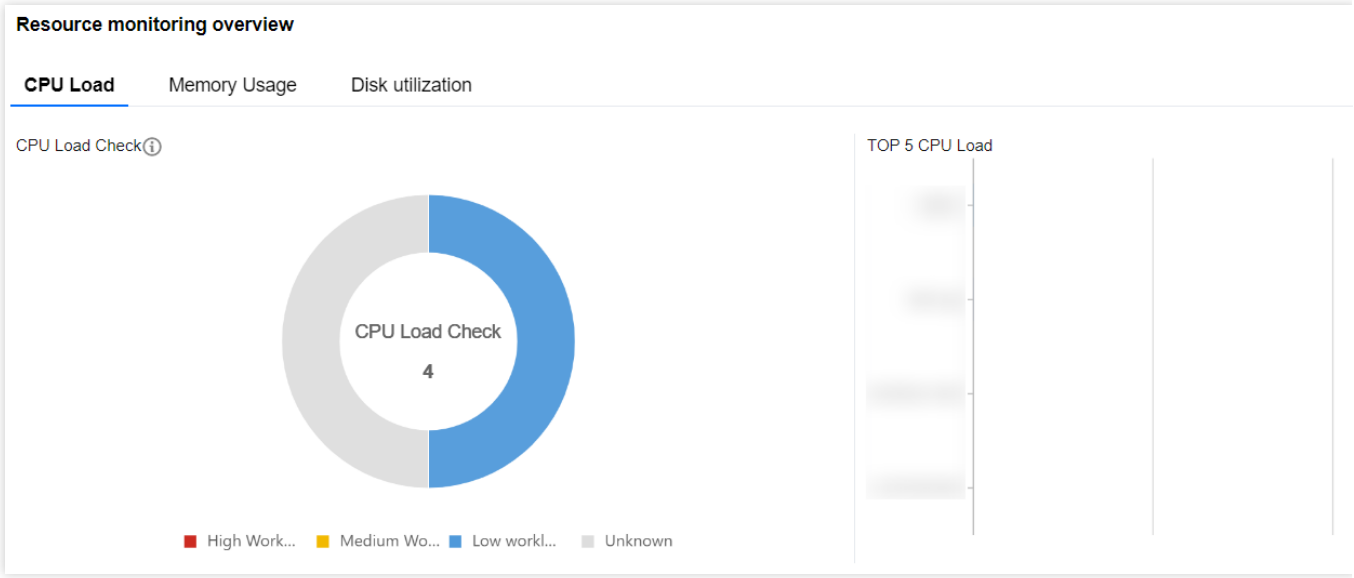
Server Overview and Trending

The server overview and trending chart (total servers, online servers, offline servers, and risky servers) supports querying any time period within one year and supports downloading and exporting. Top 5 server tags allow you to view the five most frequently used tags across all hosts.You can view the statistics for the past 7/14/30 days, or a custom period . The data generated 3 months ago is not displayed.Click **Download** to export the daily data of the server for the selected date range.



Resource Monitoring

The **Resource monitoring** section displays the distribution of system load, memory usage, disk usage, and the top 5 servers ranked by these dimensions.

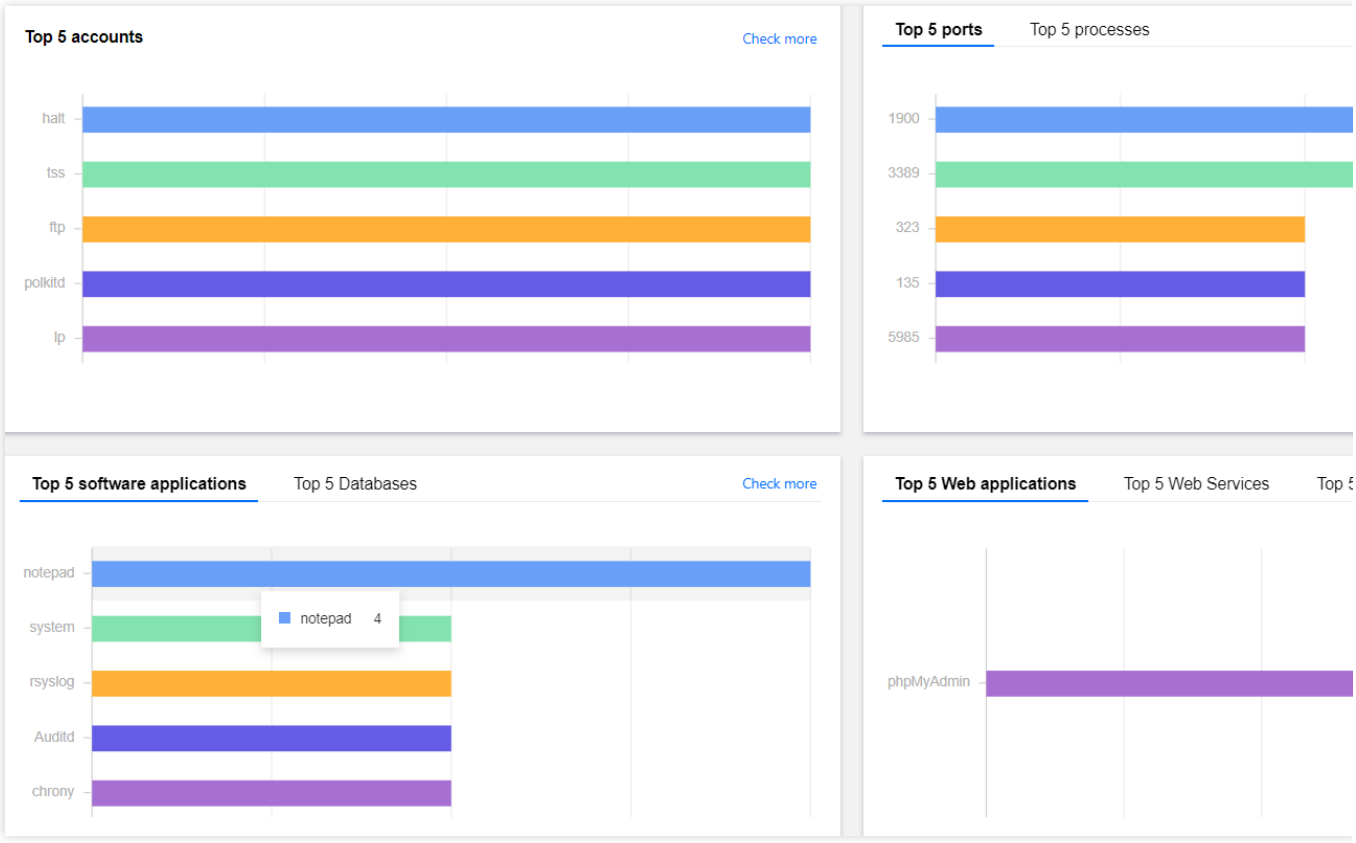


Note:

The statistics of system load are only available for Linux servers (Windows servers are not supported).

TOP 5 Asset Fingerprints

TOP 5 Asset Fingerprints displays the top 5 accounts, ports, processes, software applications, databases, Web applications, Web services, Web frameworks, and Web sites.



Server List

Last updated：2024-08-13 16:29:50

The host list is a core component of the CWPP service, providing a comprehensive, visualized and unified host management interface. It helps security administrators respond to CWPP risks more efficiently. This document will introduce how to access and manage hosts.

Restrictions

Range of Hosts with CWPP Access:

Host Type	Specific Host Types	Linux System	Windows System
Tencent Cloud Host	CVM, Lighthouse, ECM, and CPM 1.0	Supported Architectures: x86, and ARM Access Methods: VPC, and basic network	Supported Architectures: x86 Access Methods: VPC, and basic network
Non-Tencent Cloud Hosts	Ali ECS, Huawei ECS, Microsoft Azure, DigitalOcean Droplets, Amazon EC2, OracleCloud Compute ... other cloud servers, and local IDC servers	Supported Architectures: x86, ARM Accessible Methods: Public Network Direct Connection, Public Network Proxy, DC	Supported Architectures: x86 Accessible Methods: Public Network Direct Connection, DC

Multi-cloud Account Host Asset Synchronization Range: Currently, only the ECS machine data under Alibaba Cloud accounts can be synchronized via AccessKey, regardless of the operating system. (Only machine data is synchronized; the CWPP client still needs to be installed manually)
If a host connected via the non-Tencent Cloud host installation method changes its IP, CWPP will check the device code and IP list. If both remain unchanged, it is not considered a new machine; otherwise, a new host data entry will be created.
If a Tencent Cloud host is terminated or a non-Tencent Cloud host is cleared, the original risk data will be deleted.

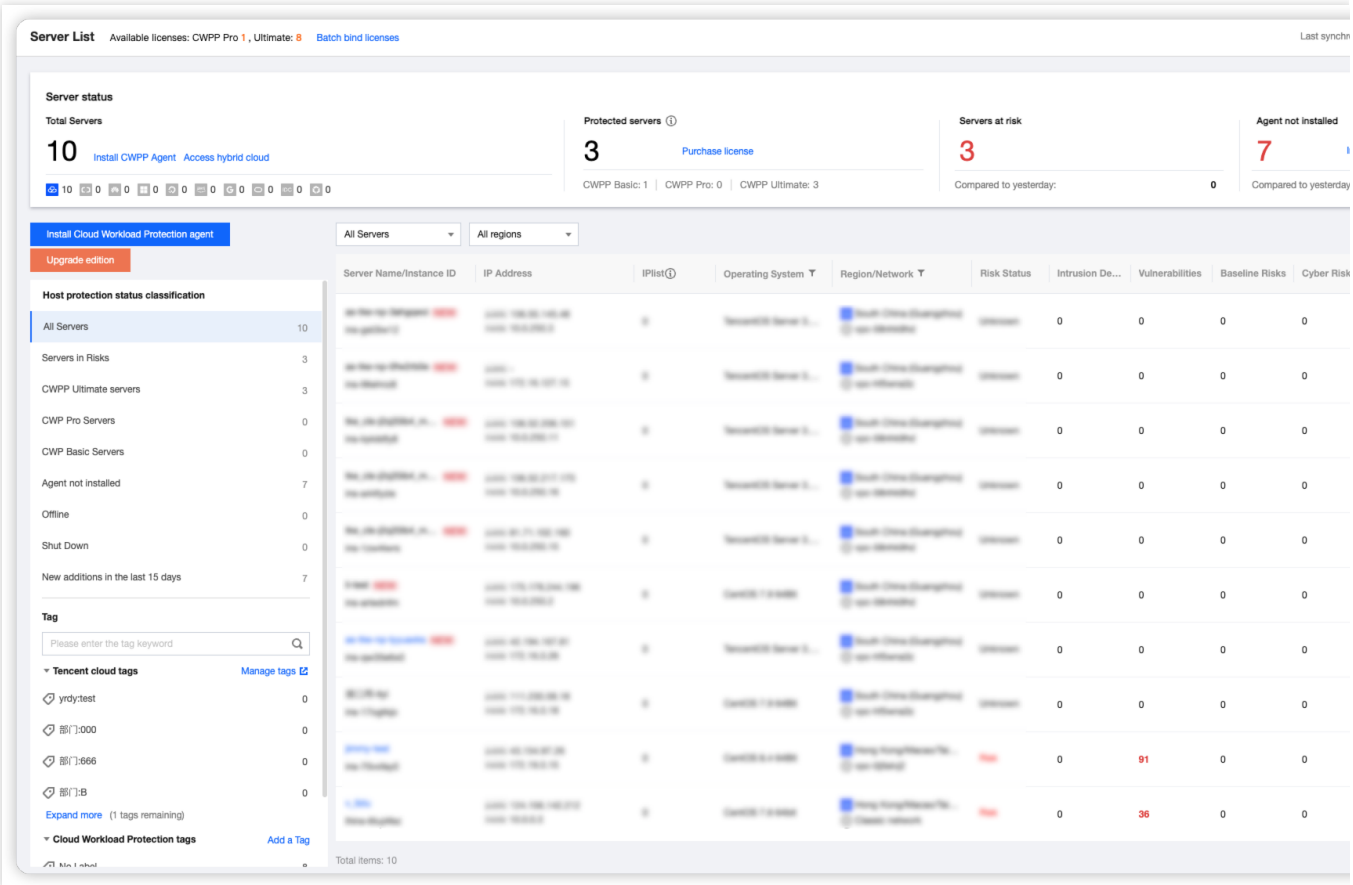
Protection Status Description

Risky host: The host has security risks.

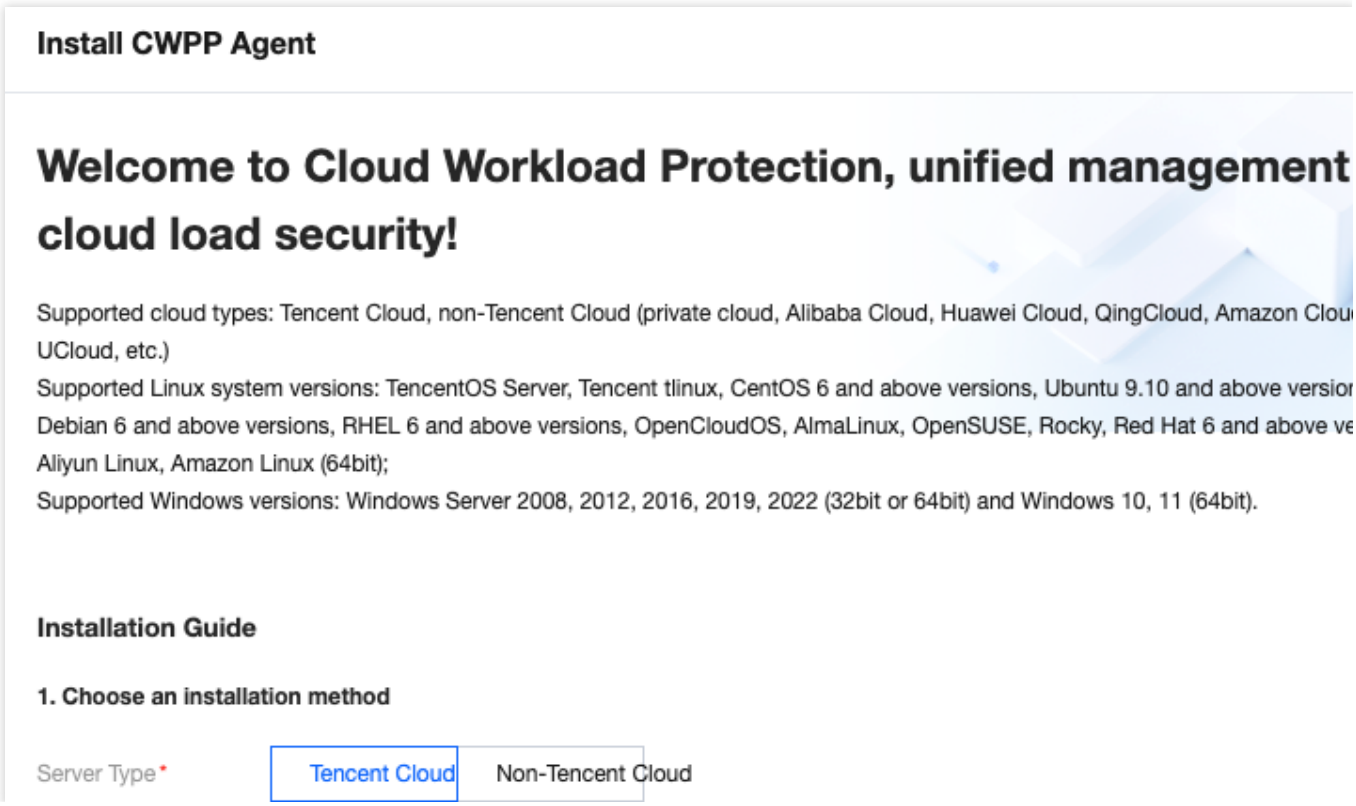
Ultimate Edition host: The host has installed the CWPP client and is bound with the Ultimate Edition authorization, providing Ultimate Edition protection.
Pro Edition host: The host has installed the CWPP client and is bound with the Pro Edition authorization, providing Pro Edition protection.
Basic Edition host: The host has only installed the CWPP client.
Client not installed (Unprotected): The host is a Tencent Cloud host but the CWPP client is not installed.
Offline:
Tencent Cloud host: The host's CWPP client is offline.
Non-Tencent Cloud host: The host's CWPP client is offline or the host has been shut down.
Note:
Because the status of non-Tencent Cloud hosts being shut down is unknown, they are viewed as being offline.
Shut down: The host is a Tencent Cloud host and is in a shutdown status.

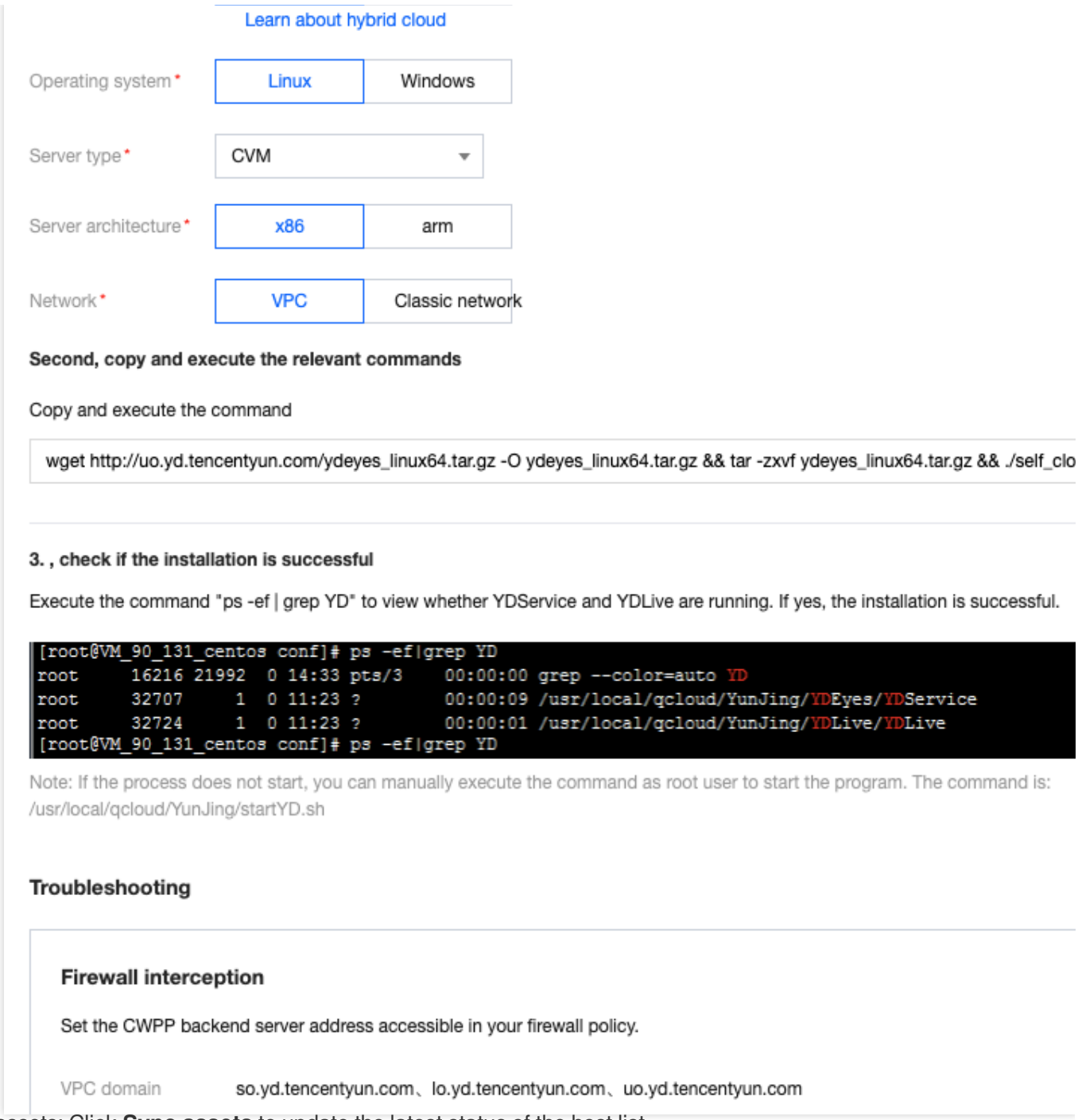
Host Configuration

1. Log in to CWPP Console, and in the left sidebar, choose **Asset** > **Server List.**
2. On the Server List page, you can Install Cloud Workload Protection agent, Sync assets, associate tags, Multi-cloud account management, Upgrade Edition, and Asset cleanup.



Install CWPP client: The CWPP client is an official Tencent Cloud security plugin and is a key prerequisite for CWPP protection. You can click **Install Cloud Workload Protection agent**, select the appropriate installation method, and verify whether the installation is successful.



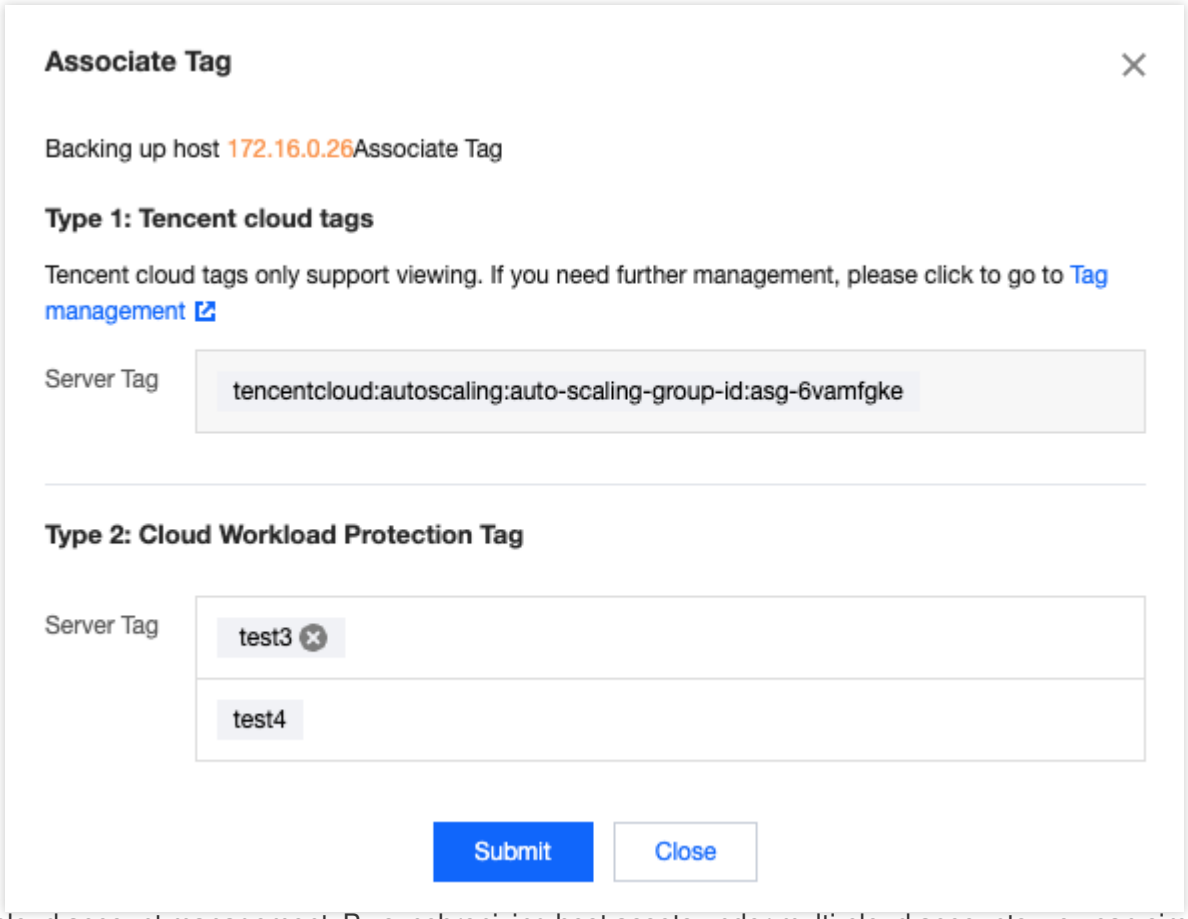


Sync assets: Click **Sync assets** to update the latest status of the host list.

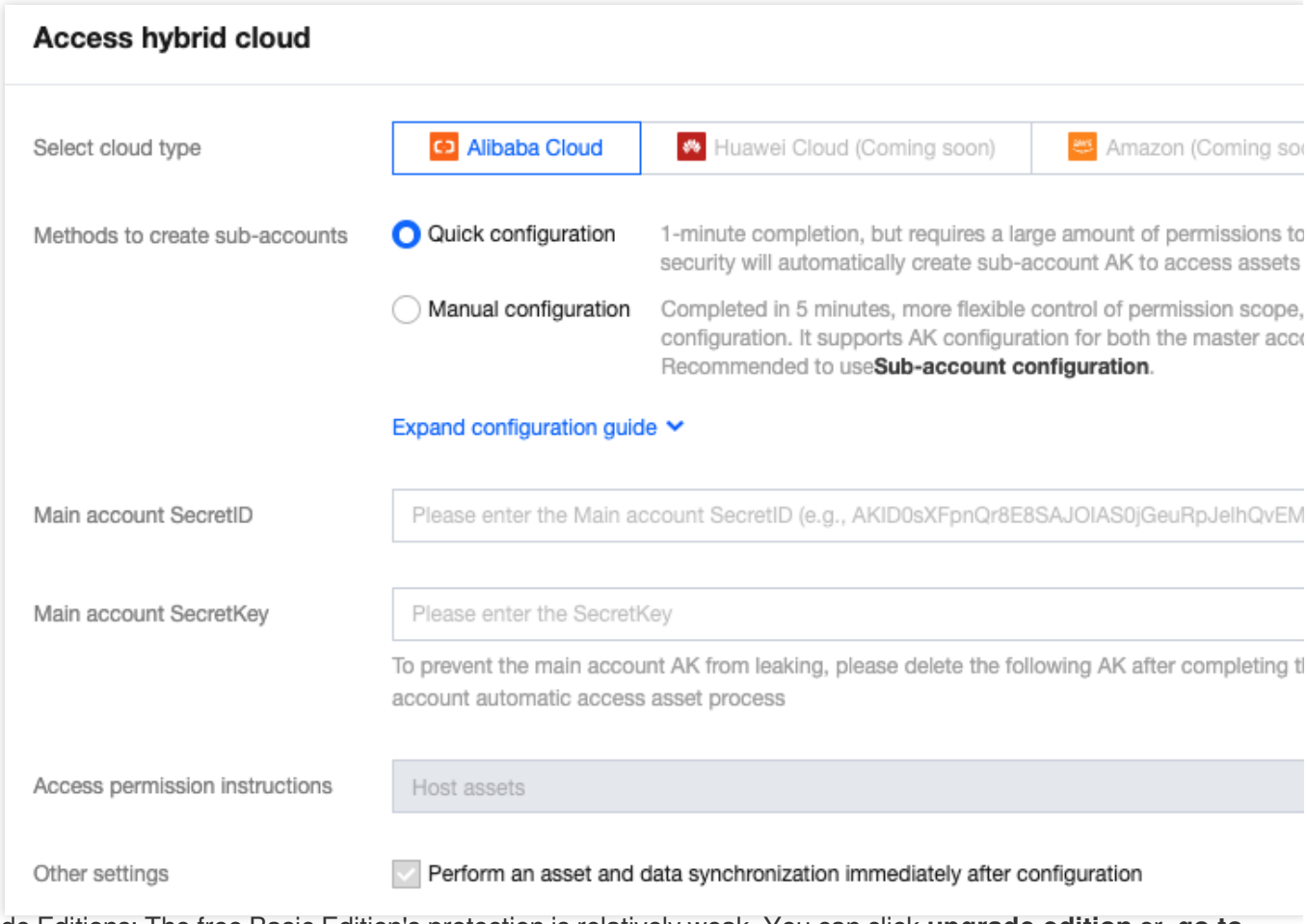
Associate tag: CWPP is compatible with Tencent Cloud tag and CWPP tags. Click the tag icon in the tag column to associate the tag with this host.

Tencent Cloud tag (key:value): Can only be associated with Tencent Cloud hosts.

Cloud Workload Protection Tag (value): Can be associated with both Tencent Cloud hosts and non-Tencent Cloud hosts.

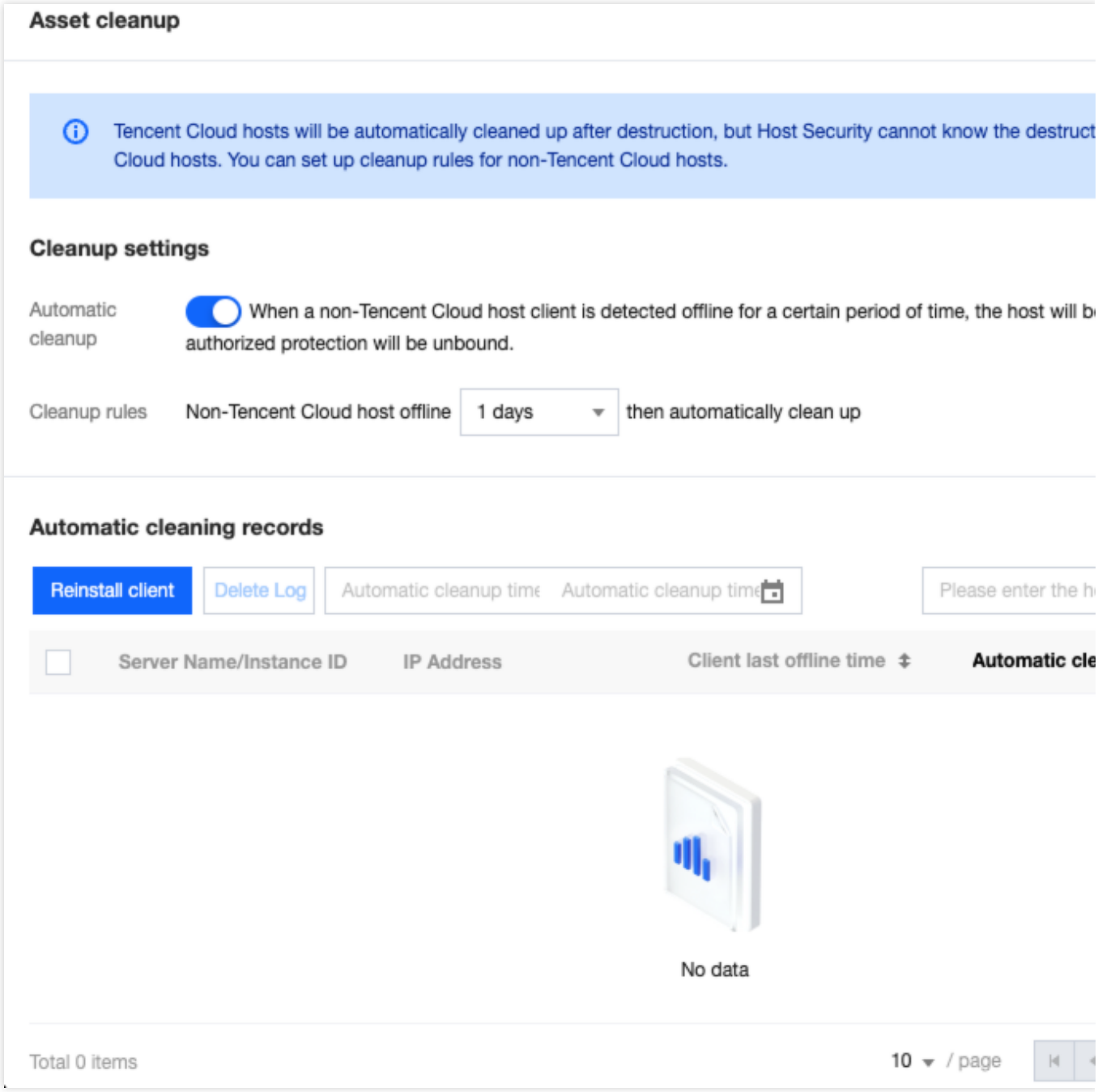


Multi-cloud account management: By synchronizing host assets under multi-cloud accounts, you can simplify management, integrate monitoring, and enhance risk visibility and response efficiency.



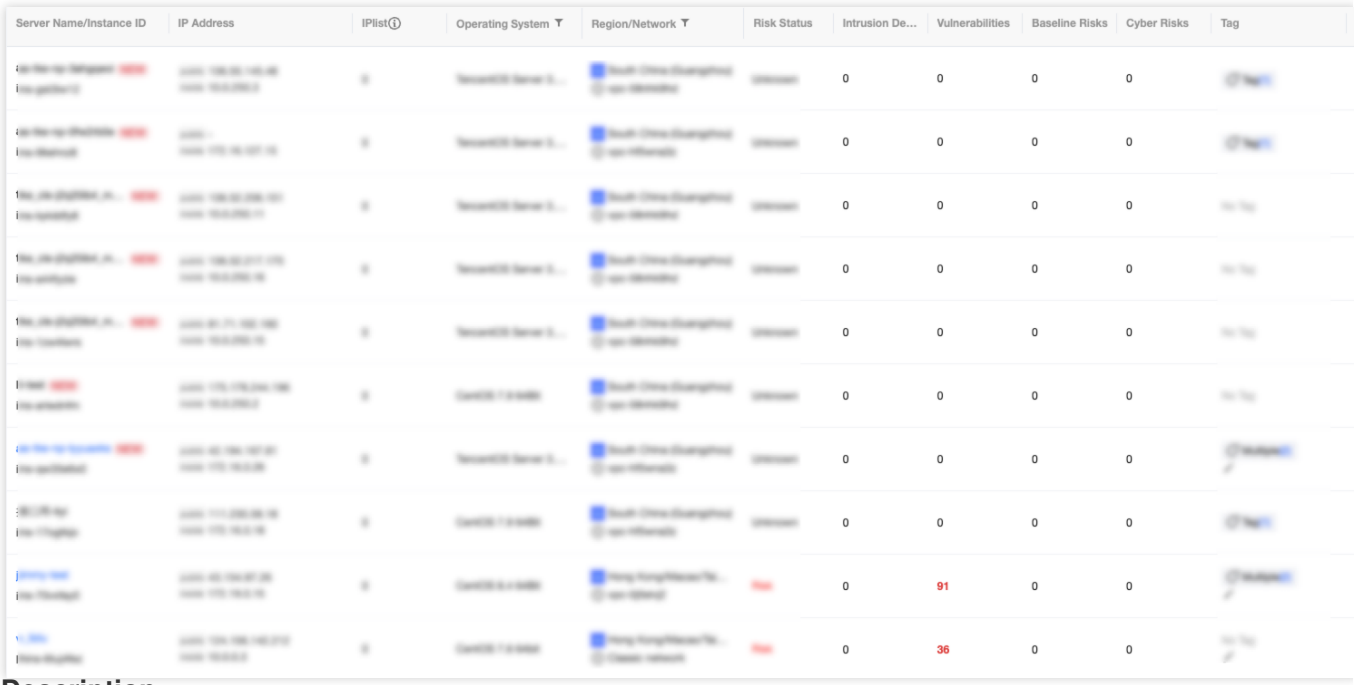
Upgrade Editions: The free Basic Edition's protection is relatively weak. You can click **upgrade edition** or **go to Bulk Authorization** to be redirected to the authorization management page. You can purchase higher-level protection licenses and bind them to basic Edition hosts to upgrade their protection.

Asset cleanup: After a Tencent Cloud host is terminated, it will be automatically cleaned. However, for non-Tencent Cloud hosts, their termination status is undetectable for CWPP. You can set cleaning rules for non-Tencent Cloud hosts. Then, if a non-Tencent Cloud host's client is offline for a certain duration, it will be automatically cleaned.



Server List

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



Field Description:

Server Name/Instance ID: Name and instance ID of the host.

IP Address: Public and private IP addresses of the host.

IP List: Network interface IP list.

Operating System: Operating system of the host.

Region/Network: Geographic location and network of the host.

Risk Status:

Unknown: The host does not have the client installed, or the host has the client installed but no risks have been detected (the protection of Basic Edition is weak, and potential risks may exist.).

Risk: The host has detected risks.

Intrusion Detection: Statistics of risks on the host including file scan, unusual log-in, password cracking, malicious requests, high risk commands, local privilege escalation, and reverse shell.

Vulnerabilities: Statistics of risks on the host including Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities.

Baseline Risks: Statistics of baseline inspection items not passed by the hosts.

Cyber Risks: Statistics of network attacks detected on the host.

Tag: Host-associated tag information.

Agent Status:

Unprotected: The host is a Tencent Cloud host, but the CWPP client is not installed.

Normal: The host has installed the CWPP client (Basic Edition or higher).

Offline: The client of the Tencent Cloud or non-Tencent Cloud host is offline, or the non-Tencent Cloud host is shut down.

Shut down: The Tencent Cloud host is shut down.

CWPP Edition: Basic, Pro, Ultimate, and - (indicates no protection)

Operation:

Install CWPP Agent: Provides installation guide for unprotected hosts.

Reinstall: Provides installation guide for hosts where the client is offline or shut down.

Uninstall: Provides a quick uninstall option for protected hosts.

License Management : Provides authorization management for hosts with paid protection Editions. Click to jump to authorization management page. You can rebind or unbind authorizations.

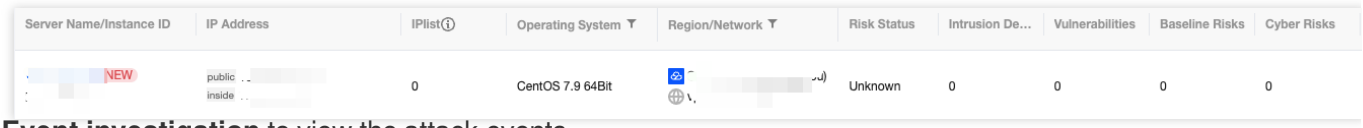
Notes: Provides a remark option for unprotected hosts. Remarks are allowed on reasons for not securing the host, facilitating subsequent management (remarks will be invisible if the client is installed later).

Note:

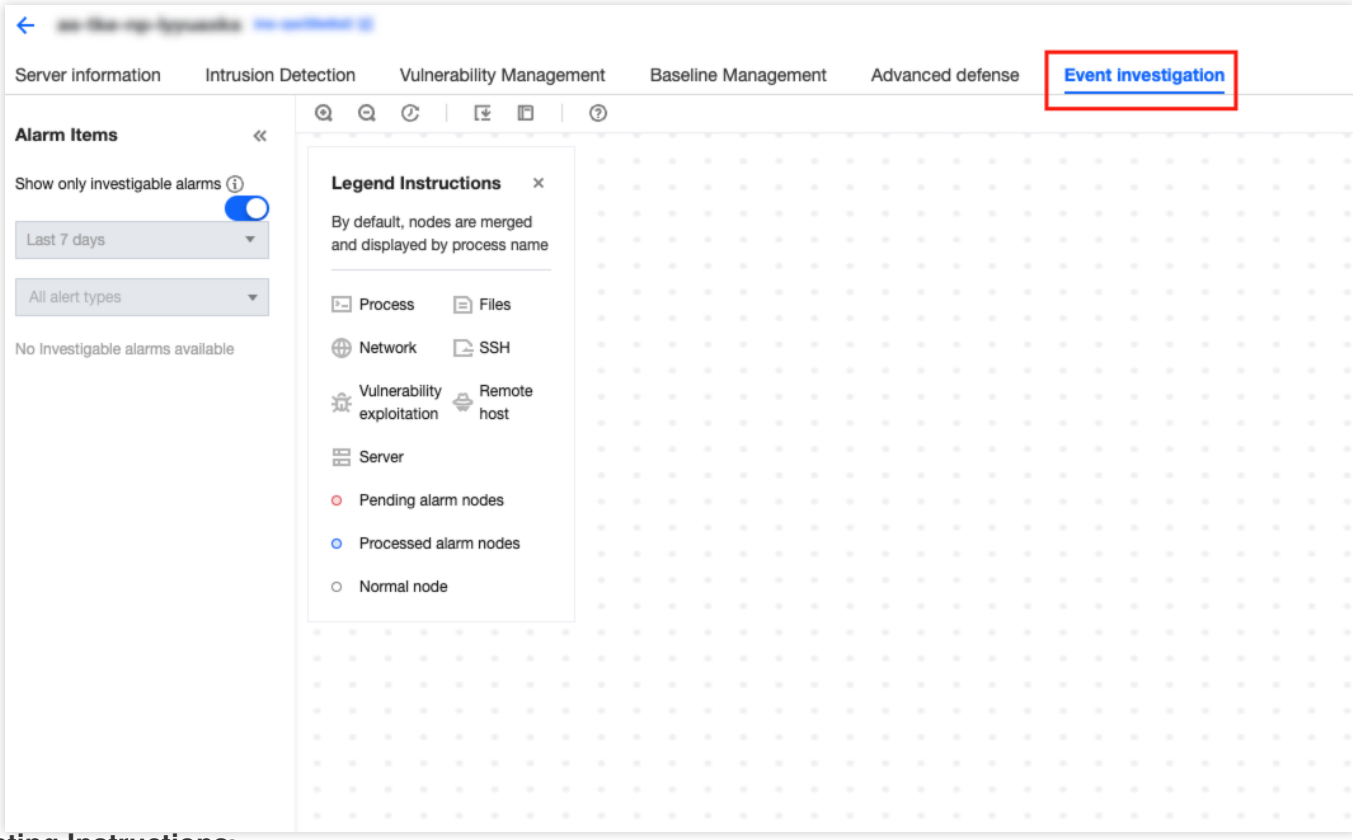
Unprotected hosts and offline hosts that meet the following four conditions can undergo a one-click and quick installation when you click either **Install CWPP Agent** or **Reinstall**.

1. The host is a Tencent CVM or Lighthouse.
2. The host is powered on.
3. The host is on a VPC network.
4. The host has TAT automated assistant installed.

Click intrusion detection, vulnerabilities, baseline risks, and cyber risks' **numerical value** to jump to the risk details.



Click **Event investigation** to view the attack events.



Operating Instructions:

For the current host, select an alarm data item to display the process execution in the middle of the screen, and to highlight the nodes that trigger the alarm.

Click **Alert Node** to view related alarms for that node. It supports viewing alarm details and processing of pending alarms.

If there are merged nodes, you can view them.

Asset Fingerprint

Last updated：2024-08-13 16:29:50

This document describes how to use the Asset Fingerprints feature.

Overview

Asset Fingerprints provides detailed asset data including server resource monitoring, accounts, ports, and processes, and gives you a quick overview of assets affected by security events.

Quota and Limits

Only hosts with the paid protection edition can collect asset fingerprint data. Basic edition hosts must first upgrade the edition.
The following lists the asset fingerprint items collected in different CWPP editions.

CWPP Edition	Supported Asset Types
CWPP Basic (free)	N/A
CWPP Pro	10 types of assets: Resource Monitoring, Accounts, Ports, Processes, Software Applications, Databases, Web Applications, Web Services, Web Frameworks, and Websites
CWPP Ultimate	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 package

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

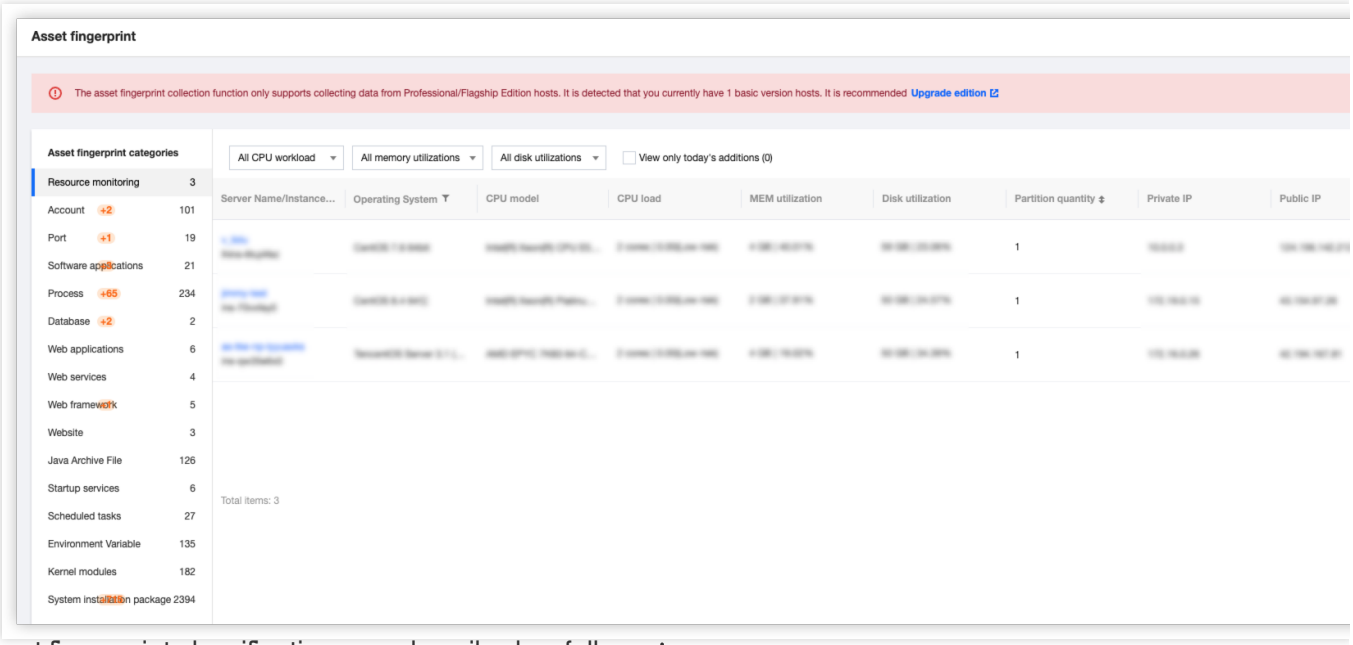
Operation Guide

1. Log in to the CWPP console, Click **Asset Fingerprints** on the left sidebar.
2. The asset fingerprints page displays a list of asset fingerprint classifications, including each asset fingerprint item and its corresponding number of servers. After an item from the asset fingerprint classification list on the left is

selected, the details of that fingerprint will be displayed on the right. It supports both query and export of fingerprint data.

Note

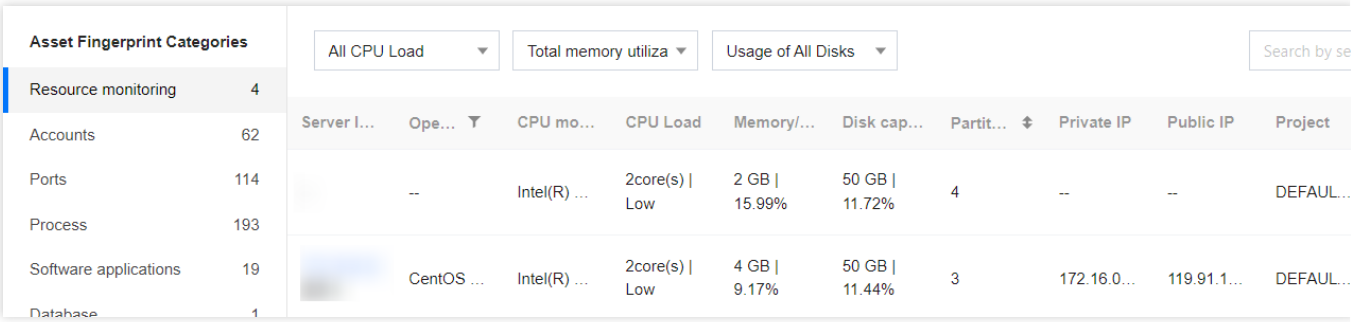
All asset fingerprint search features support fuzzy search.



The asset fingerprint classifications are described as follows：

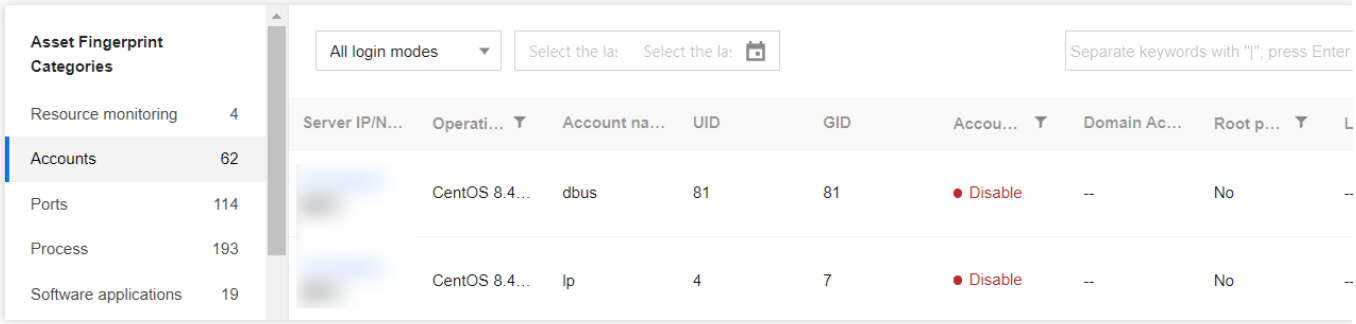
Resource Monitoring

Collects the data on server system load, memory usage, and disk usage.



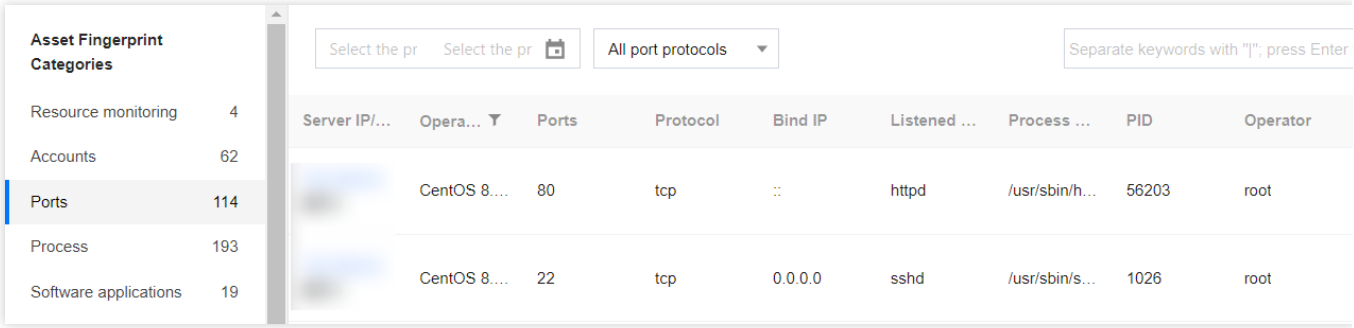
Accounts

Collects the data of all accounts on the server.



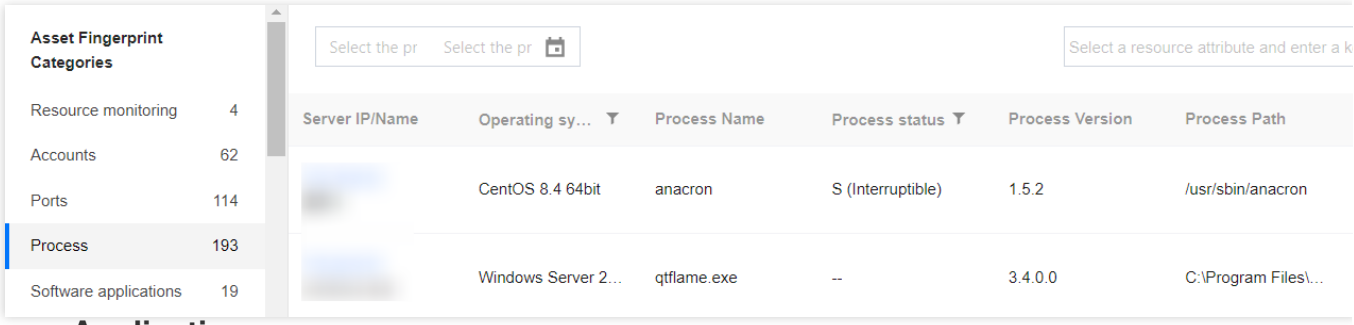
Ports

Collects the data of all used ports of the server.



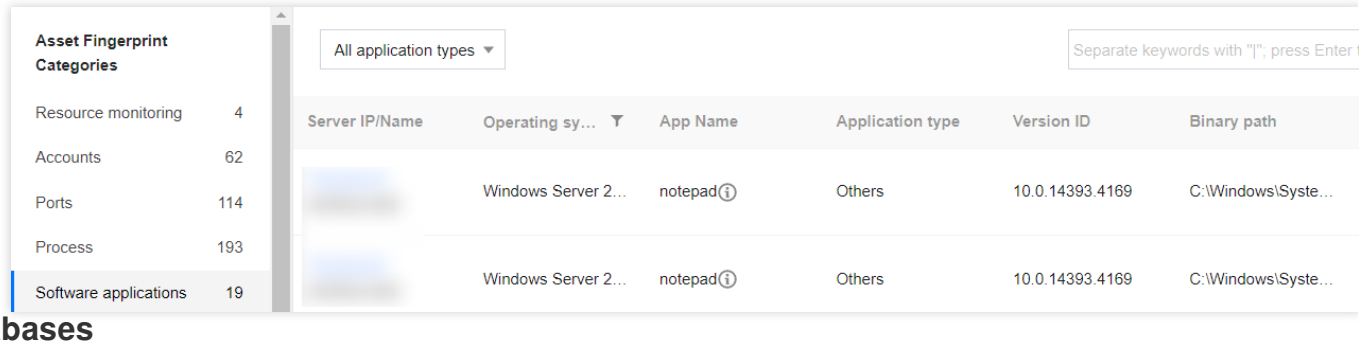
Processes

Collects the data of all processes running on the server.



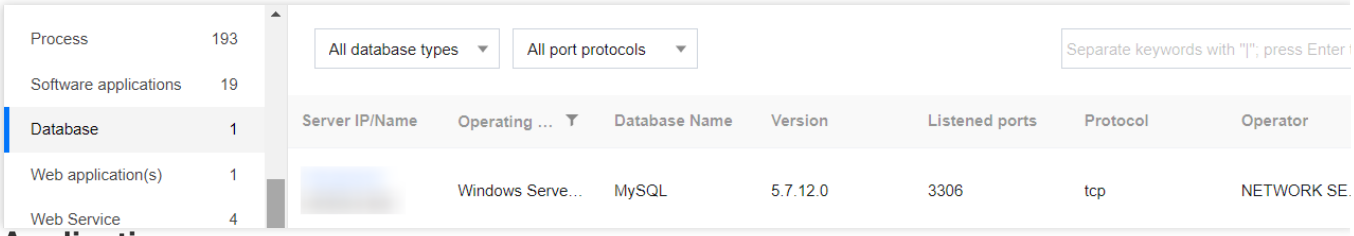
Software Applications

Collects the data of all software applications running on the server.



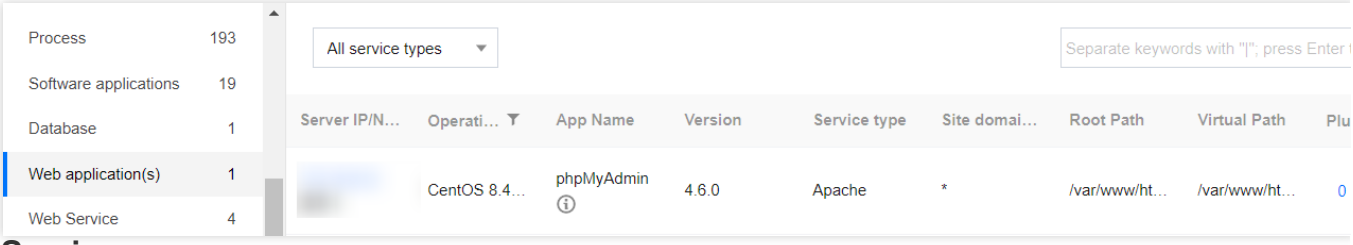
Databases

Collects the data of all databases running on the server.



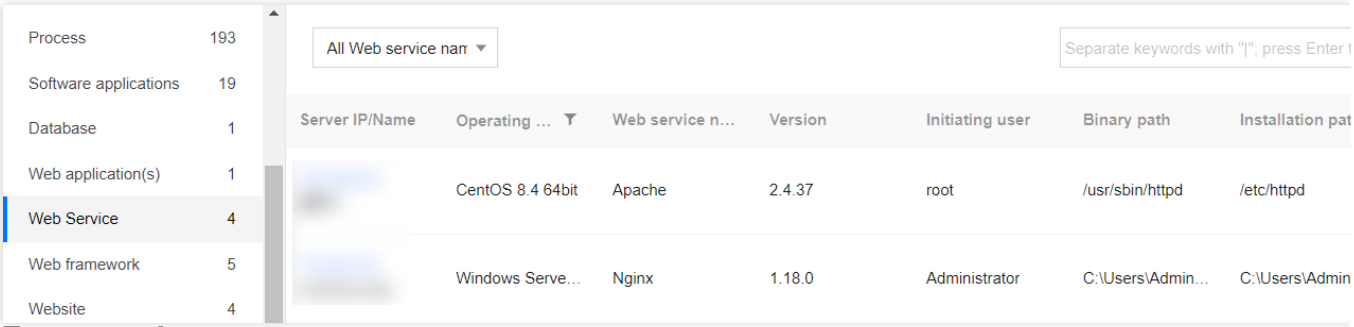
Web Applications

Collects the data of all Web applications running on the server.



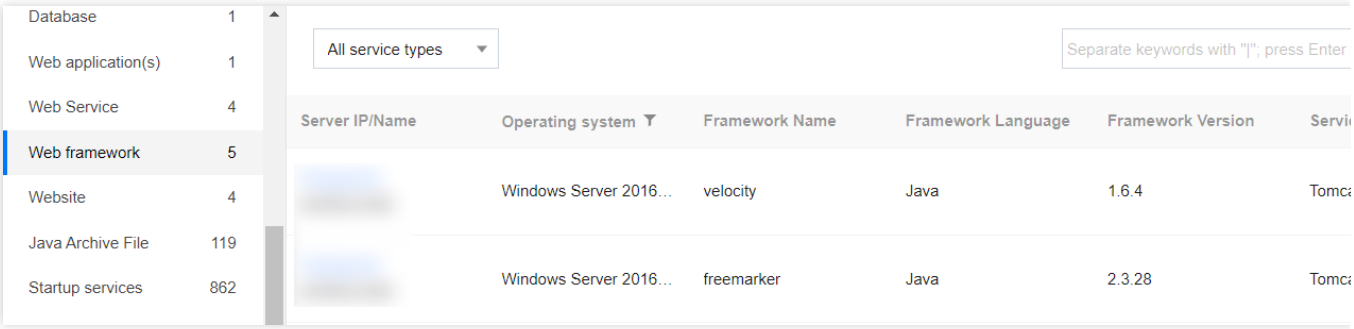
Web Services

Collects the data of all Web services running on the server.



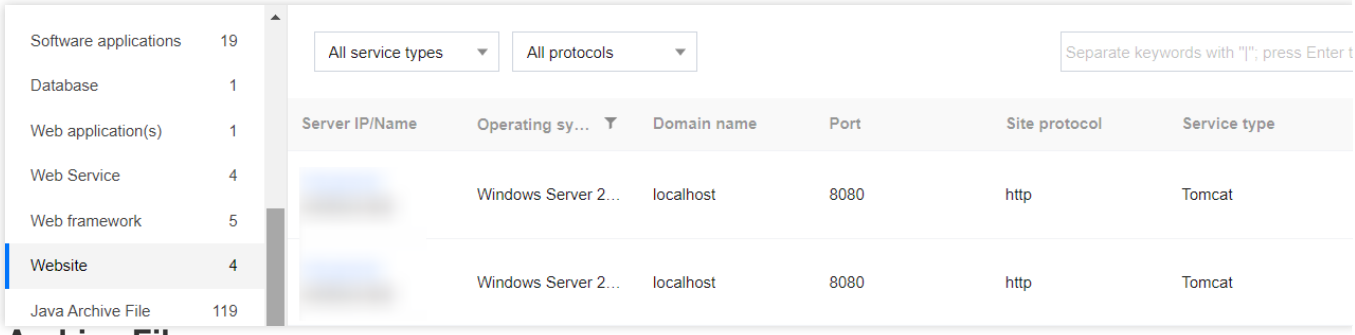
Web Frameworks

Collects all Web frameworks applied on the server.



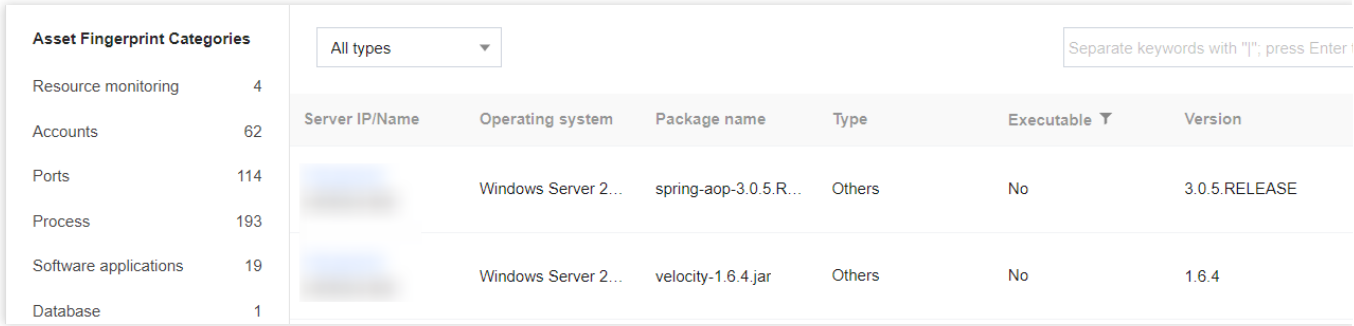
Websites

Collect the data of all websites deployed on the server.



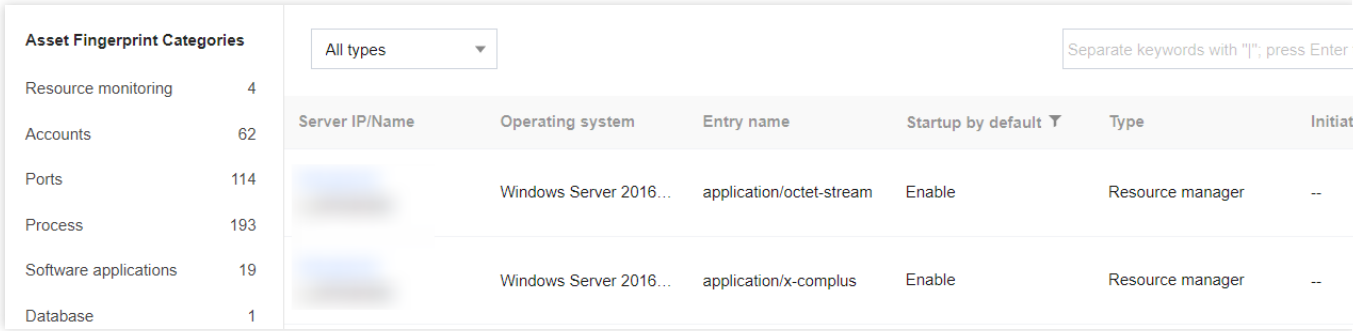
Java Archive Files

Collect the data of all Java archive files on the server.



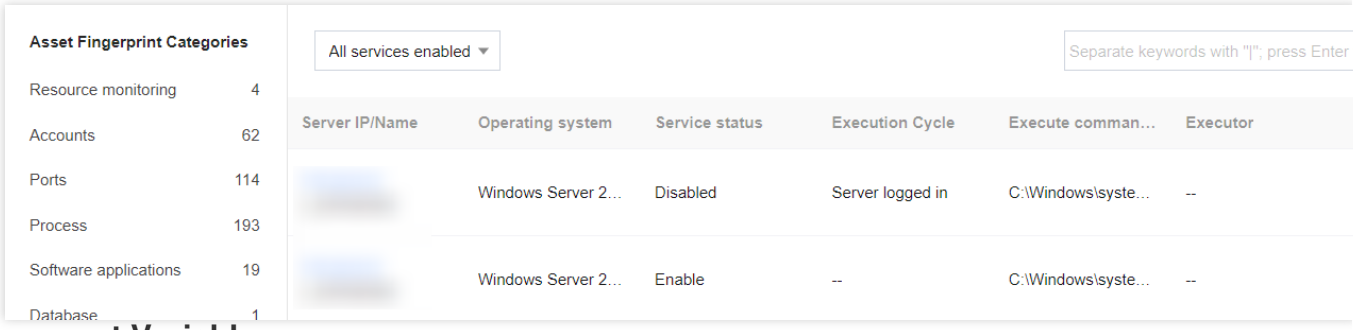
Startup Services

Collect the data of all startup services on the server.



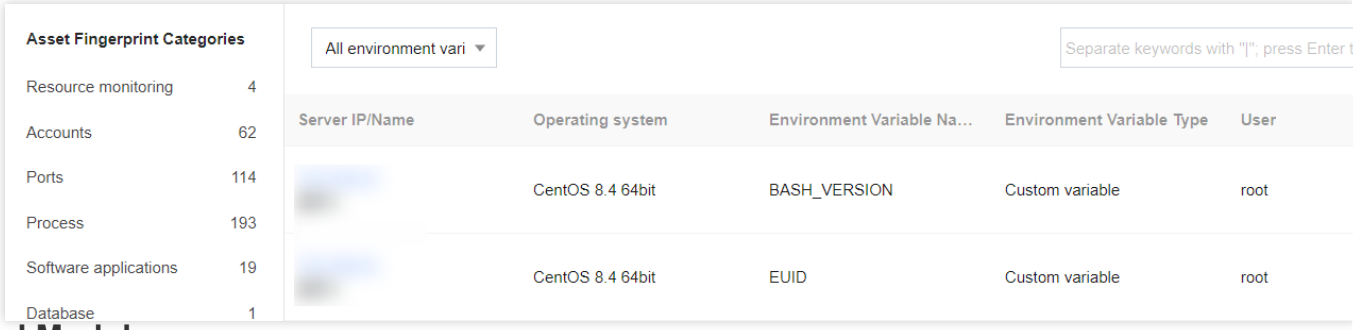
Scheduled Tasks

Collect the data of all scheduled tasks on the server.



Environment Variables

Collect the data of all environment variables of the server.

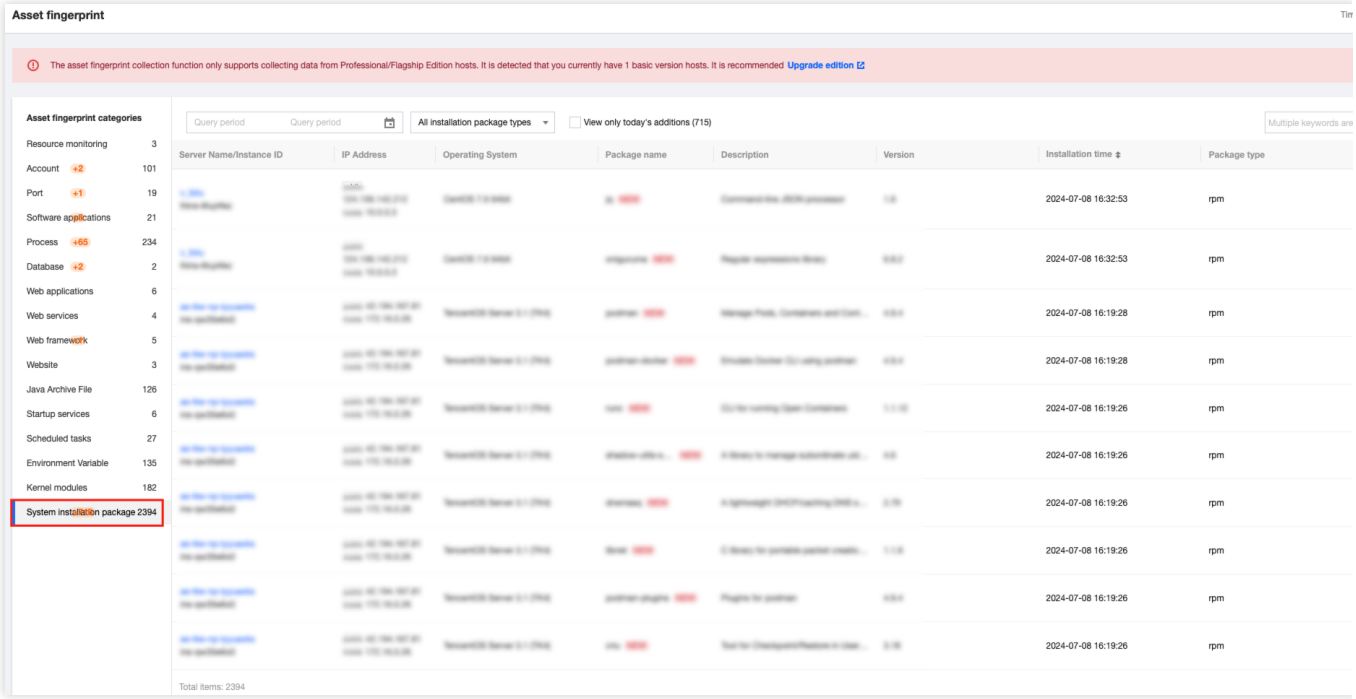


Kernel Modules

Collect the data of all kernel modules of the server.

System Installation Package

Collect the system installation package of the servers.



Vulnerability Management

Last updated：2024-08-13 16:29:49

This document describes how to use the Vulnerability Management feature to manage the vulnerabilities on your servers.

Overview

Tencent Cloud CWPP allows you to perform periodic and on-demand checks on mainstream servers (Windows, Linux, etc.) for vulnerabilities. CWPP allows you to check specified servers for specified categories of vulnerabilities and ignore certain vulnerabilities. It presents information such as vulnerability risks, vulnerability characteristics, risk level, and solutions in a visualized form to help you better manage vulnerability risks on your servers.

Important Notes

The Vulnerability Management feature is available only if you have at least one server bound to a (**CWPP Pro**/**Ultimate**) license.
The range of vulnerability management is described as follows:

Vulnerability Management feature	**Vulnerability Type**	**Linux System**	**Windows System**
Vulnerability scanning Applicable to Pro edition and Ultimate edition hosts.	Linux software vulnerabilities	✓	×
	Windows system vulnerabilities	×	✓
	Web-CMS vulnerabilities	✓	✓
	Application vulnerabilities	✓	✓
Exploit prevention Applicable to Ultimate edition hosts.	Linux software vulnerabilities	×	×
	Windows system vulnerabilities	×	×
	Web-CMS vulnerabilities	✓ Only supports some vulnerabilities.	×

	Application vulnerabilities	✓ Only supports some vulnerabilities.	×
Auto fix of vulnerabilities Applicable to Ultimate edition hosts.	Linux software vulnerabilities	✓ Only supports some vulnerabilities.	×
	Windows system vulnerabilities	×	×
	Web-CMS vulnerabilities	✓ Only supports some vulnerabilities.	✓ Only supports some vulnerabilities.
	Application vulnerabilities	×	×

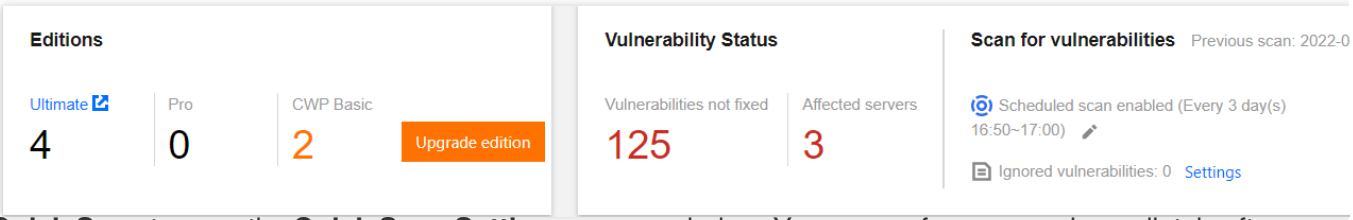
Due to the possibility of vulnerabilities fix affecting user business, automatic vulnerability fix is not immediately performed after detection. Users should review the vulnerabilities, click **Fix** , and perform data backup before proceeding with automatic fix.

Operation Guide

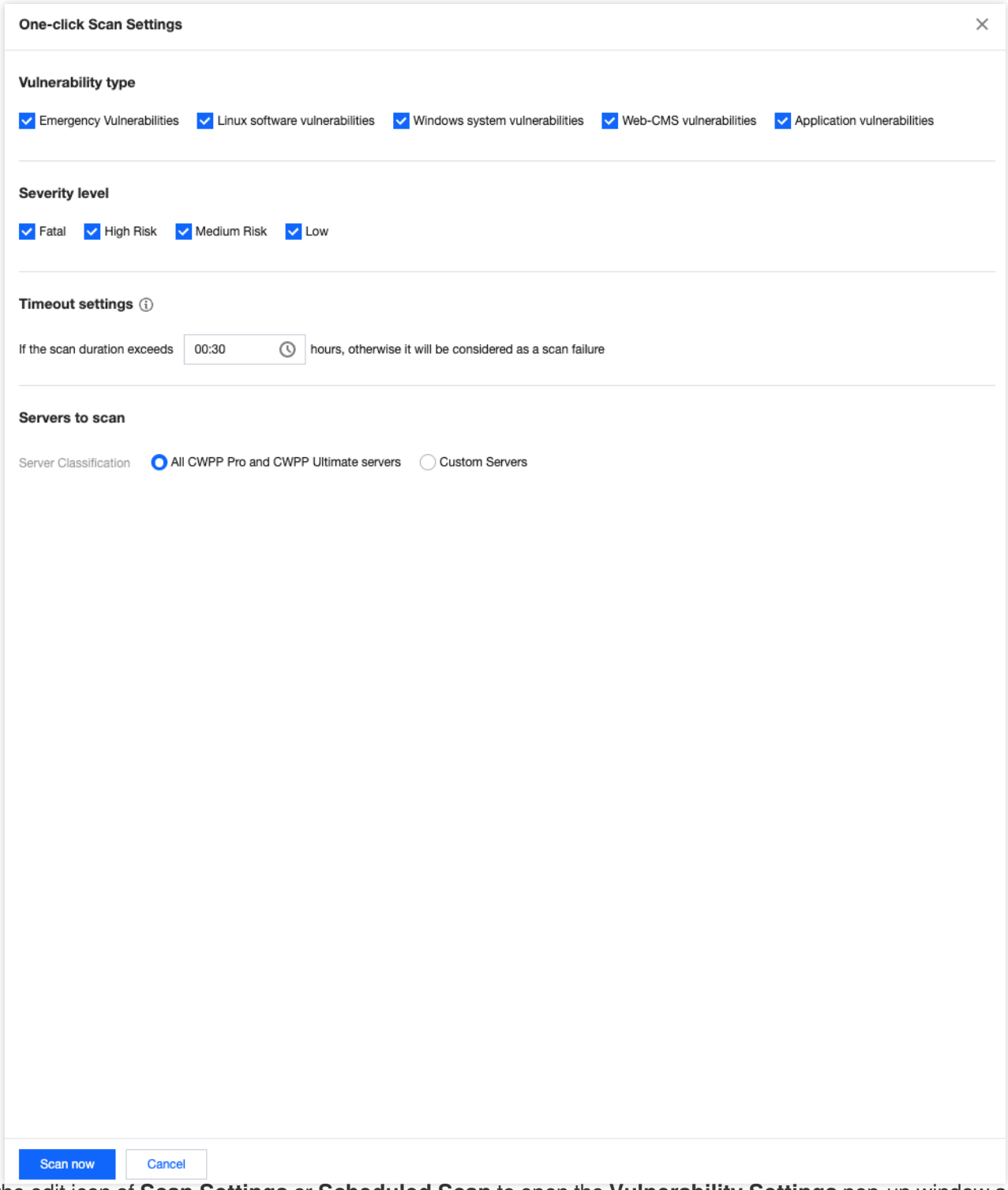
1. Log in to the CWPP console.
2. Click **Vulnerability Management** on the left sidebar. The fields and operations related to the feature are described as follows.

Vulnerability Scan

In the **Vulnerability Scan** section, you can perform a quick scan to obtain the results of the vulnerability scan, or set scheduled scans to identify and fix vulnerabilities in a timely manner.



Click **Quick Scan** to open the **Quick Scan Settings** pop-up window. You can perform a scan immediately after setting the vulnerability category, vulnerability level, scan timeout threshold, and servers covered by the scan.

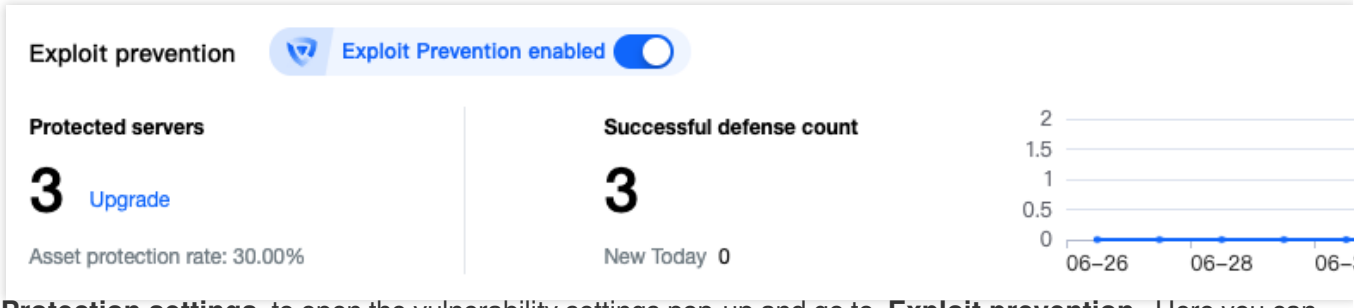


Click the edit icon of **Scan Settings** or **Scheduled Scan** to open the **Vulnerability Settings** pop-up window and select **Scheduled Scan**. You can enable scheduled scan, and set scan interval, vulnerability level, and vulnerability categories, which will take effect immediately.

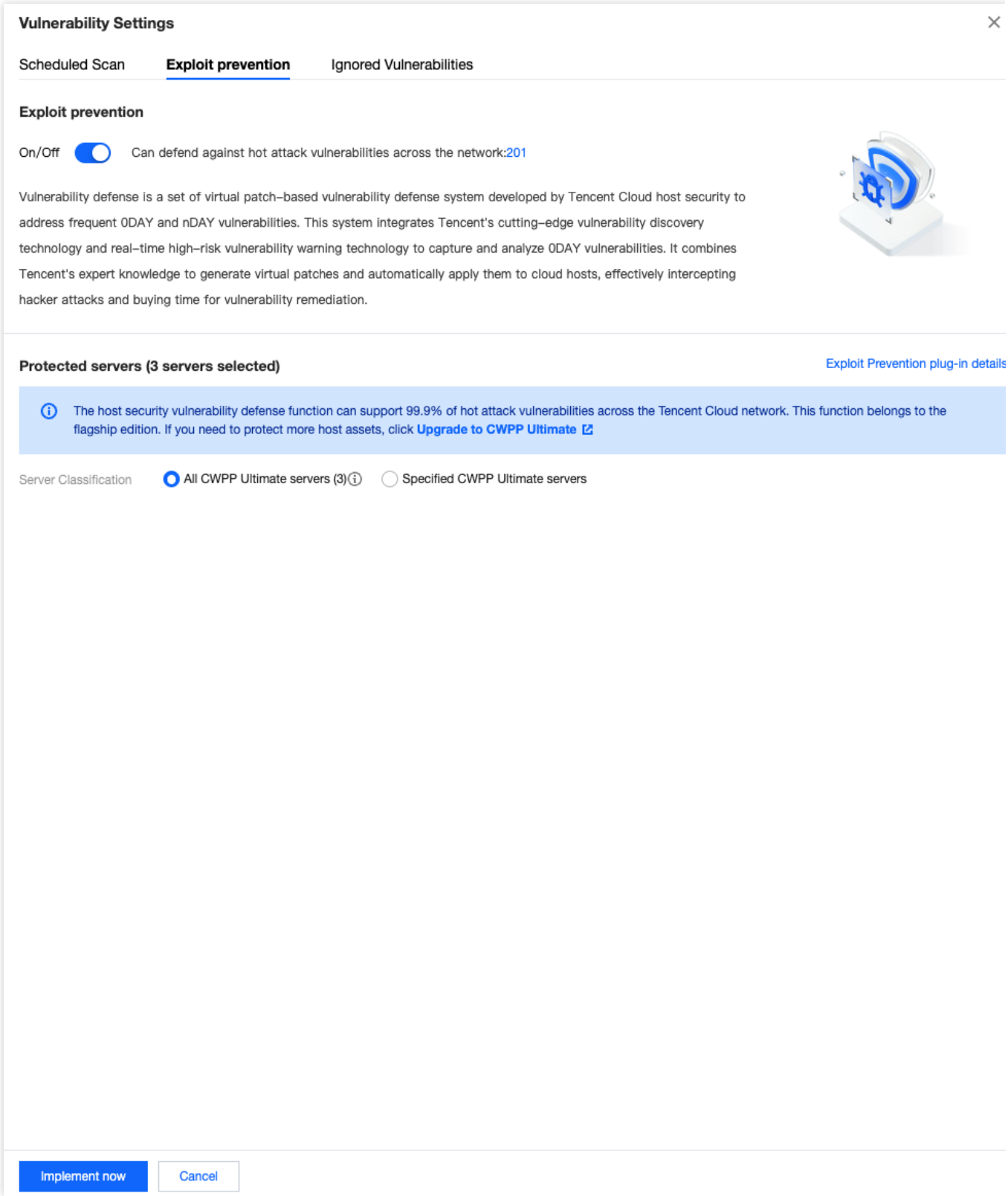
Click **Details** to view the details of the last scan. You can download the scan reports in a PDF or Excel format.

Exploit Prevention

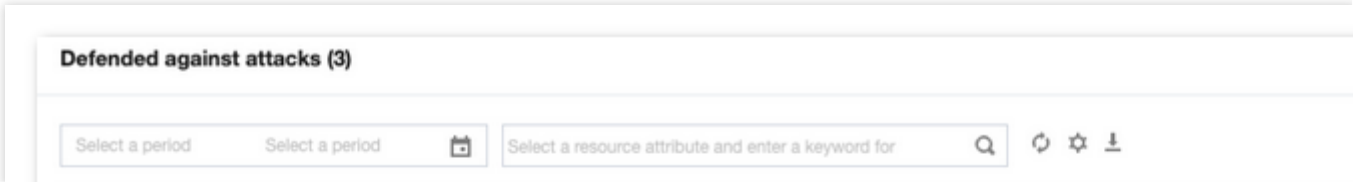
In the **Exploit prevention** module, you can enable/disable the exploit prevention switch, view situations including the number of protected servers, successful prevention count, and prevention trends.

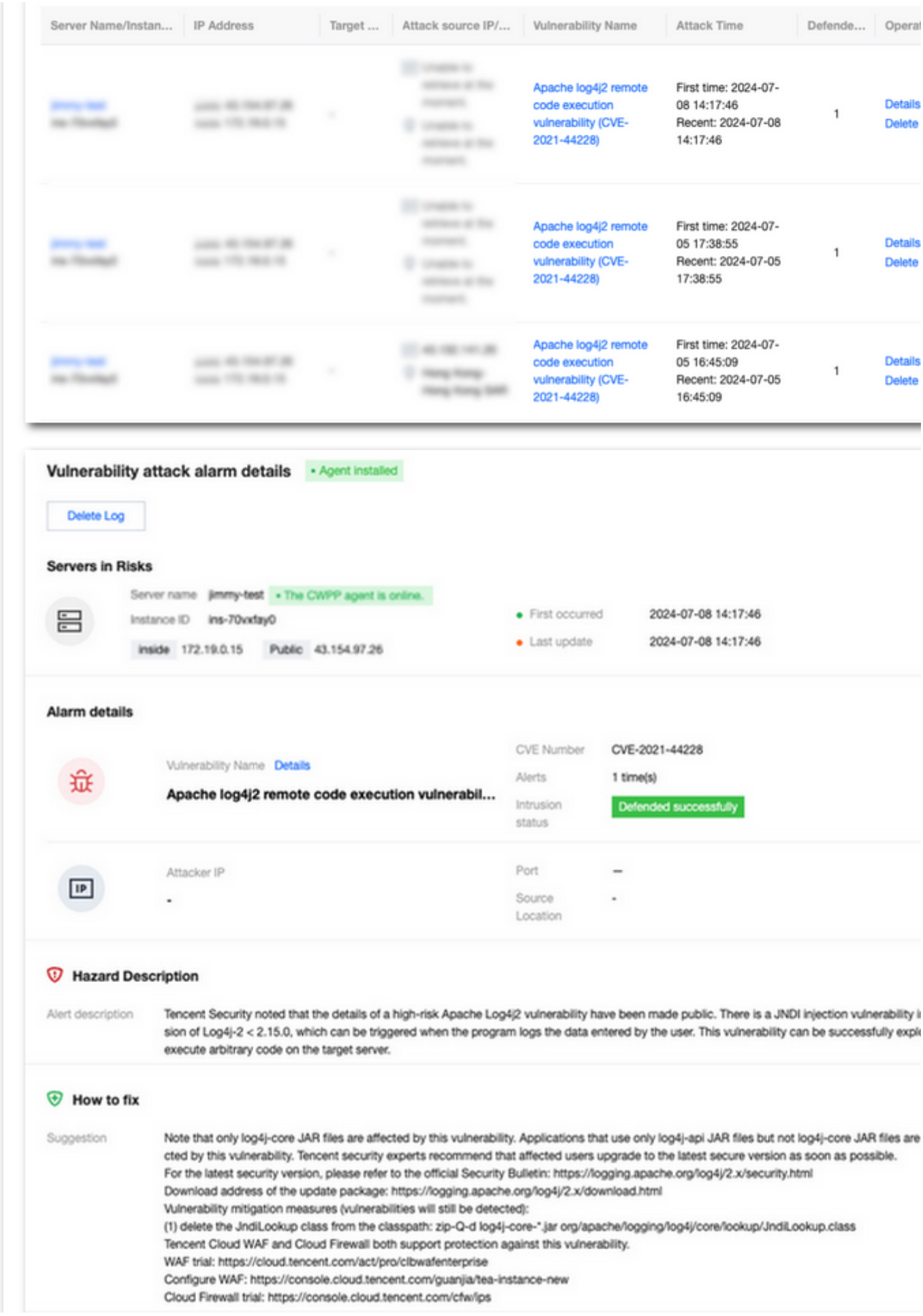


Click **Protection settings** to open the vulnerability settings pop-up and go to **Exploit prevention** . Here you can set the exploit prevention switch, view protectable vulnerabilities, select the prevention host range, and see prevention plugin details.



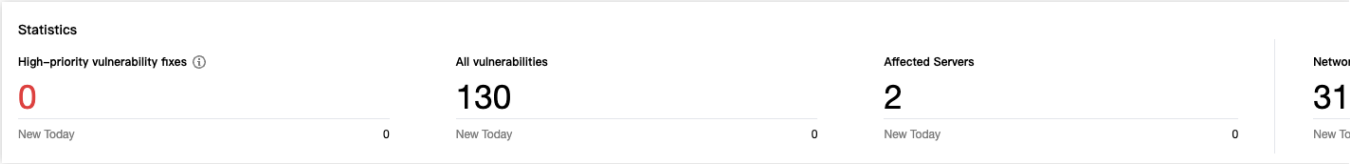
Click **Number of Successful Defenses** to view the current successfully prevented attacks and the attack details.



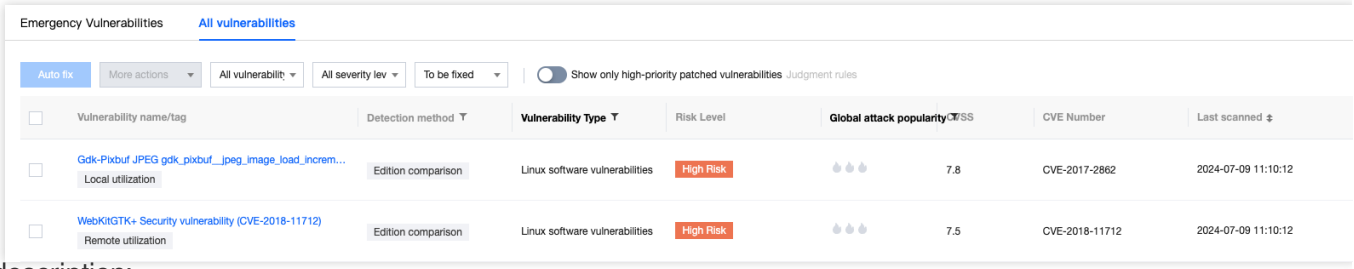


Vulnerability Handling

1. At the bottom of the vulnerability management page, you can view statistics of detected vulnerabilities and the detailed vulnerability list.
2. The **Statistics** module displays the status of vulnerability detections, the number of network attack events, today's new additions, and the total number of CWPP vulnerabilities in the database.



Field Description:
High-priority Vulnerability Fixes: This category displays hot attack vulnerabilities and severe/high-risk vulnerabilities, which need priority fixing. The default statistic shows the number of vulnerabilities to be fixed. Click **Custom Definition Rules** to define rules for determining high-priority vulnerabilities that need fixing.
All Vulnerabilities: The total number of detected Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities.
Affected Servers: The number of hosts with detected vulnerabilities.
Network Attack Events: The number of network attack events in the past month.
Supported Vulnerabilities: View the CWPP-supported vulnerability database. You can search up to 25 times daily, with each search displaying up to 100 results.
3. In the **Vulnerability List** module, the specific vulnerabilities detected are displayed, which are categorized into emergency vulnerabilities and all vulnerabilities. The two categories have no significant difference in features. The following introduces how to handle vulnerabilities to you, with **All vulnerabilities** as the example.



Field description:

Vulnerability Name/Tag: The detected vulnerability and the tag for the vulnerability (remote exploit, service restart, EXP exists, etc.).

Detection Method: Version comparison, and POC validation.

Vulnerability Category: Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities.

Threat Level: Critical, High, Medium, and Low.

CVSS: The score given by the Common Vulnerability Scoring System. The score ranges from 0 to 10, with 0 indicating the lowest risk and 10 the highest risk.

CVE No.: A unique number that identifies a vulnerability in the Common Vulnerabilities & Exposures library.

Last Detected: The time when the vulnerability was last detected.

Affected Servers: The number of servers where this vulnerability was detected.

Status: Pending, Fixing, Scanning, Fixed, Ignored, and Fix failed.

Auto Fix Status: Fix not supported, Auto fix (no restart required), and Auto fix (restart required).

Operation

Solution: For the vulnerabilities that cannot be automatically fixed, you can click **Solution** to open the vulnerability details pop-up window, and manually fix the vulnerability as described in the solution.

Auto Fix: Some Linux software vulnerabilities and Web-CMS vulnerabilities can be automatically fixed. You can click "Auto Fix" to open the vulnerability details pop-up window, and select the server to be fixed. For details, see Auto-Fixing of Vulnerabilities.

Rescan: Perform a scan again for this vulnerability.

Ignore: Ignore the vulnerability. This vulnerability will no longer be scanned on the server.

Baseline Management

Last updated：2024-08-13 16:29:50

This document describes how to use the Baseline Management to ensure baseline security for servers.

Overview

Tencent Cloud CWPP (Cloud Workload Protection Platform) allows you to perform periodic and quick baseline checks on servers based on default or custom baseline policies. You can also specify check items and servers to be included in baseline policies. By providing information such as baseline check pass rates, detected risks, threat levels, and suggestions on how to fix the vulnerabilities, the product helps you better manage the baseline security of your servers.

CWPP Editions

Basic Edition : If this is the first time you use it, it supports detection of all hosts in the default policy, but it can only display 5 results. It does not support baseline policy management, one-click detection, or periodic detection.
Pro Edition : Supports baseline policy management, allowing users to create or edit policies. It supports periodic and one-click detection for baseline policies.
Ultimate Edition : Supports baseline policy management, allowing users to create or edit policies. It supports periodic and one-click detection for baseline policies. Also supports custom weak password.

Operation Guide

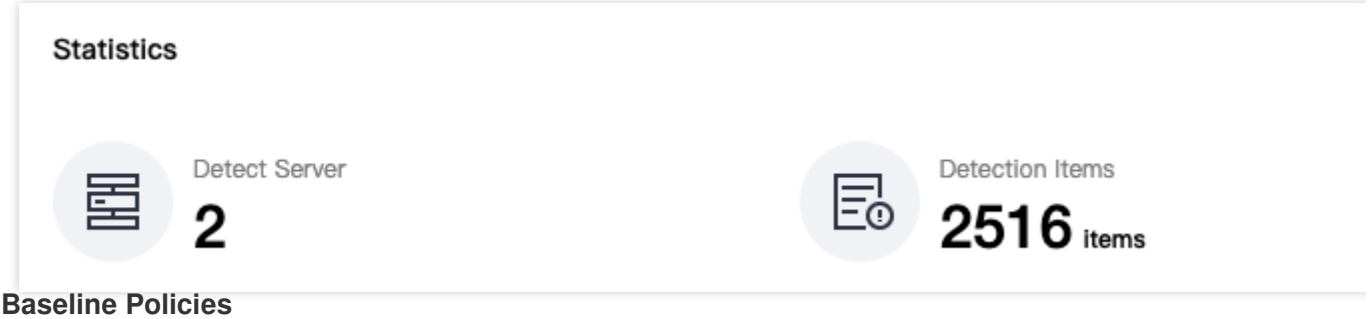
1. Log in to the CWPP console, and in the left sidebar, choose **Baseline Management** .
2. The baseline management page provides settings for baseline policies, periodic detection, and one-click detection for specified policies. It supports viewing the pass rate and risk status of baseline policies, as well as the list of baseline detection results. You can view details of the baselines and check items and their repair plans. You can also ignore specific check items for specified servers.

Baseline policies

A baseline policy is a collection of user-defined baseline check items, allowing you to track baseline pass rates and detected risks based on the dimensions included in the policy.
Tencent Cloud default baseline policies: Tencent Cloud CWPP provides default baseline policies based on mainstream network security baseline check items, including: weak password policy, CIS baseline policy, and Tencent Cloud best security practice policy. You can add check items and servers to be checked to a default baseline policy, under which the check is conducted once every 7 days by default (at 00:00 of the day).

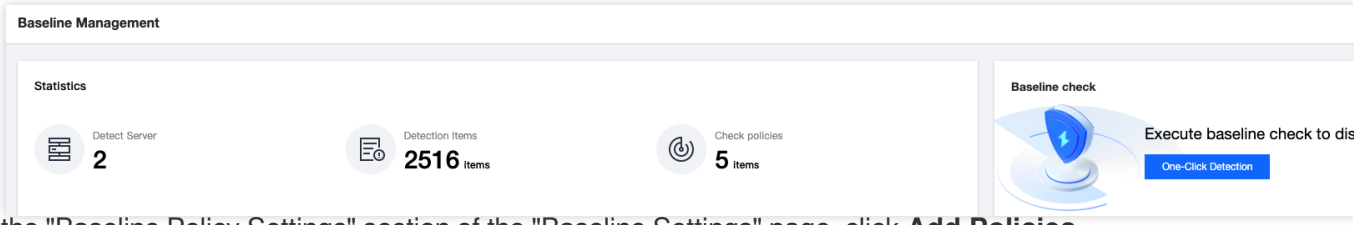
Note:

Pass rate of policy = the number of servers that pass all check items under this policy/the number of all servers checked under this policy

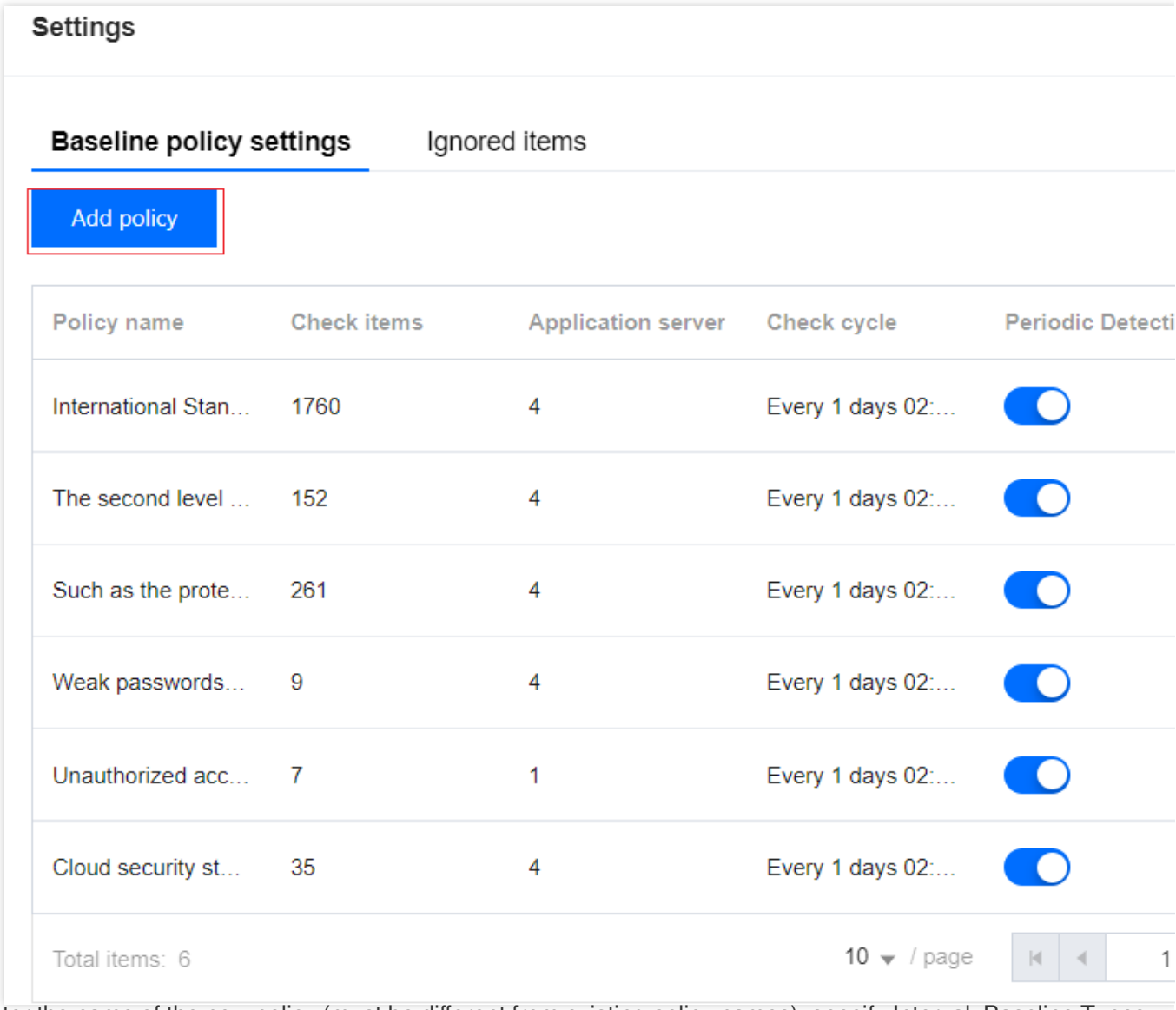


Add Baseline Policies

1.1 Click **Baseline Settings** in the upper right corner of the baseline check result section.



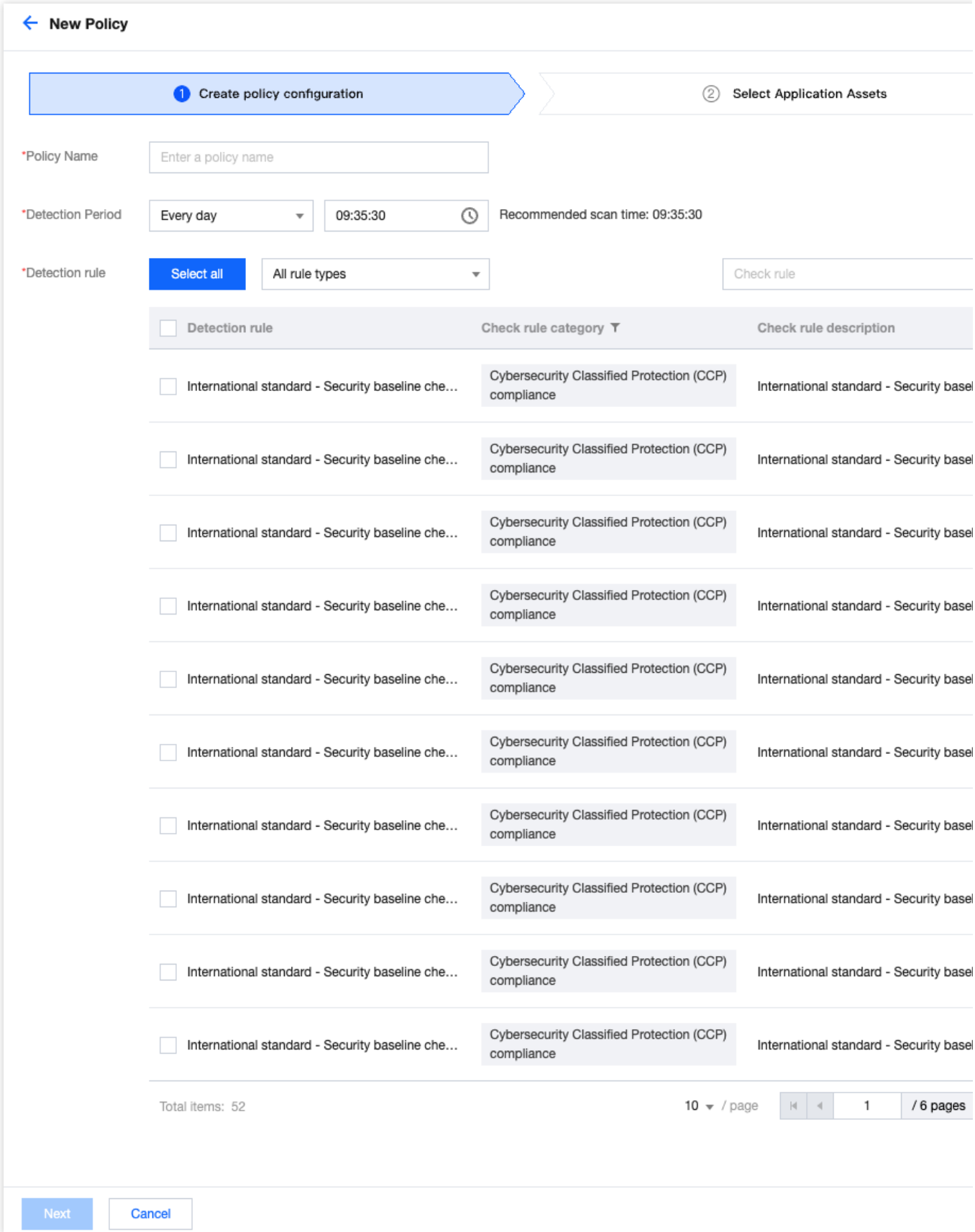
1.2 In the "Baseline Policy Settings" section of the "Baseline Settings" page, click **Add Policies**.



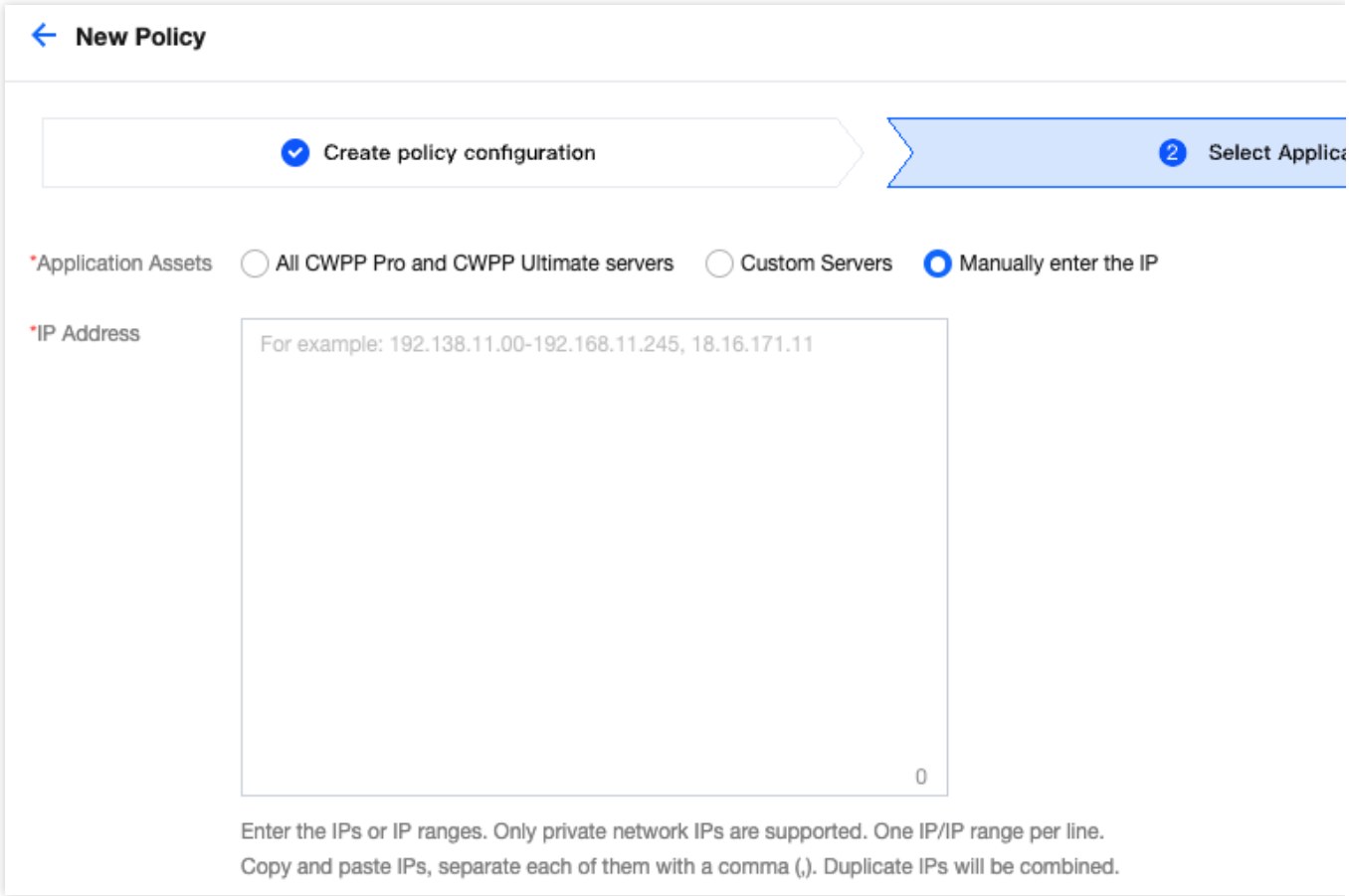
1.3 Enter the name of the new policy (must be different from existing policy names), specify Interval, Baseline Types, and Target Assets in the "Add Policies" page, and then click "Save and update".

Note:

A maximum of 20 baseline policies. If this limit is reached, you must delete an existing policy before you can create a new one.



1.4 Select the application assets based on actual needs, and click **Complete.**



Baseline Detection

Tencent Cloud CWPP supports **regular inspections** and **One-Click Detection** for baseline check items and allows checking specified baseline items on designated CVMs.

Note

If this is not the first time you use the baseline detection, you need to activate CWPP Pro edition or Ultimate edition to proceed with baseline detection.

One-click Detection

First Detection : When you use the baseline detection feature for the first time, We provide you with a free detection service for full-scale baseline policy check and comprehensive scan across all your servers, assisting you in identifying potential baseline security risks. We will display 5 baseline risks. If you need more baseline security features, we recommend upgrading to the Pro edition or Ultimate edition.

1.1 For baseline detection results display module, click **Trial Detection** .

1.2 In the Detection Prompt pop-up window:

Operation 1: Select the baseline policy to be checked, click **Start Inspection** (the inspection usually takes 2-5 minutes). After the inspection is complete, the results will be displayed as visualized charts on the vulnerability management page.

Operation 2: Click upgrade now to jump to the CWPP upgrade interface and upgrade CVM to the Pro edition.

Non-first Time Detection : When this is not the first time for you to use the baseline detection, you can choose the baseline policy to be checked, and click **One-Click Detection** (the inspection usually takes 2-10 minutes). If you do not have a Pro edition server yet, we recommend upgrading to the Pro edition immediately.

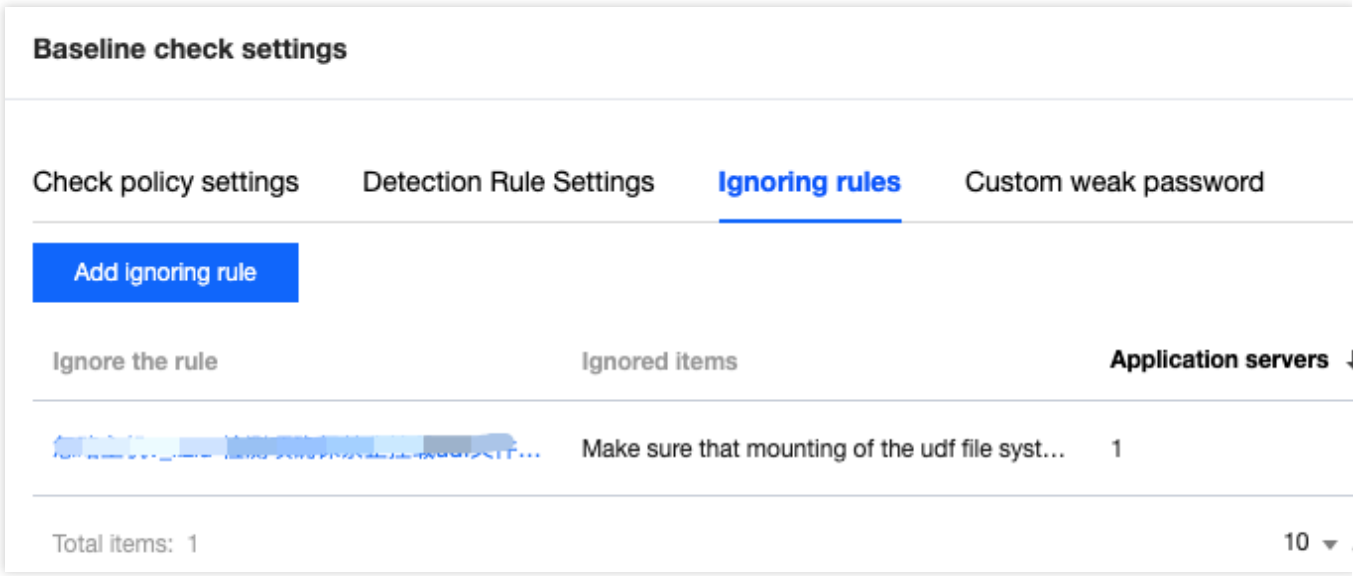
Periodic Detection

1. In the top right corner of the baseline management page, click **Baseline check settings** .
2. On the baseline check settings tab, you can configure periodic detection and manage ignored items.

Periodic Detection Settings : On the baseline policy settings tab, you can add or modify policies, set check cycle, and also enable or disable periodic detection. Additionally, it supports the deletion of user-defined policies.

Policy Name	Baseline rules	Baseline chec...	Application se...	Detection Period
[illegible]	50	2516	2	Every 1 days 17:05
[illegible]	12	1427	2	Every 1 days 01:00
[illegible]	9	9	2	Every 1 days 01:00
[illegible]	7	7	2	Every 1 days 01:00
[illegible]	6	35	2	Every 1 days 01:00

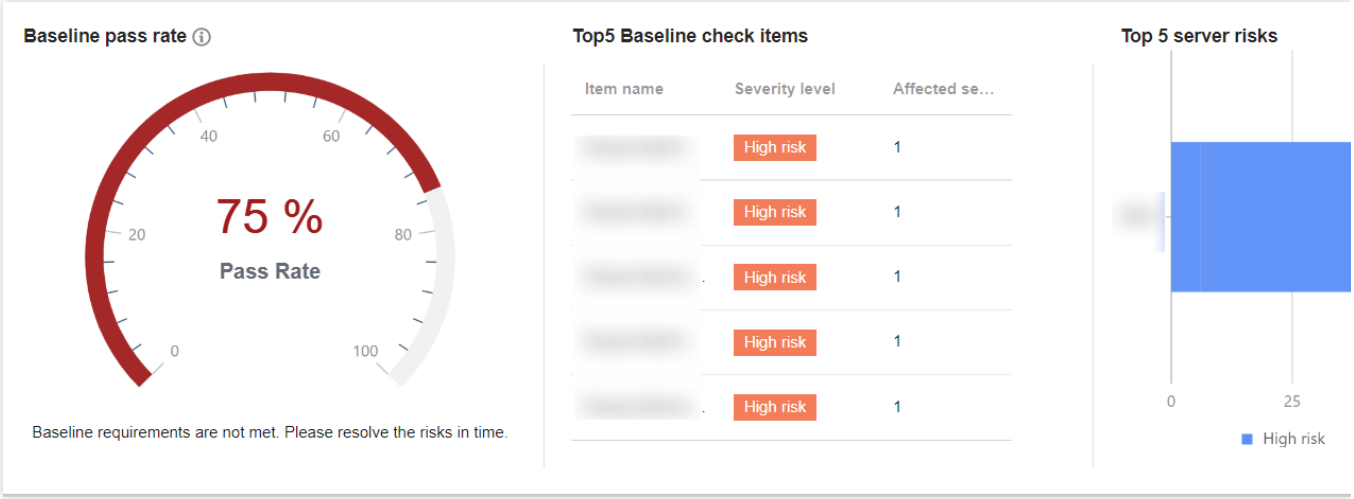
Ignoring rules Management : Under the ignored items management tab, you can view the ignored check items and their details, and perform unignore operations.



Periodic Check

1. Click **Baseline Settings** in the upper right corner of the baseline check result section.

2. You can set the interval of periodic checks and manage ignored check items

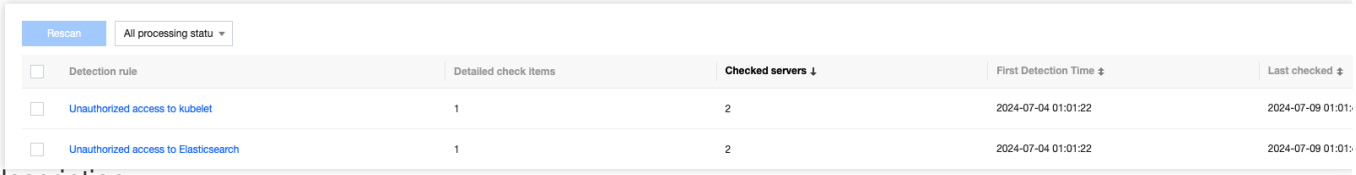


Visualized baseline data

After selecting baseline policies and running a check, the Baseline Management page shows the number of checked servers, number of check items, the pass rate of the baseline policies, top 5 baseline check items, and top 5 risk items, which are categorized by threat level.

Baseline check result list

At the bottom of the Baseline Management page, the list of baseline check results is shown, where you can view baseline details, perform fuzzy search and status filtering for a single baseline, and download all tables.



Field description:

Baseline Name: The name of the current baseline set, which contains multiple check items of the same category.

Threat Level: Divided into Severe, High, Medium, and Low

Baseline Check Items: The total number of check items included in the current baseline set.

Affected servers: The number of servers that do not pass every check item in the current baseline set under the baseline policy, i.e. the number of servers affected by this baseline set.

Last Checked: The time when the check items in the baseline set were last executed on a server.

Status: Pass, Fail and In Progress.

Operation: Allows you to view baseline details and run a recheck for failed baselines.

Rescan:

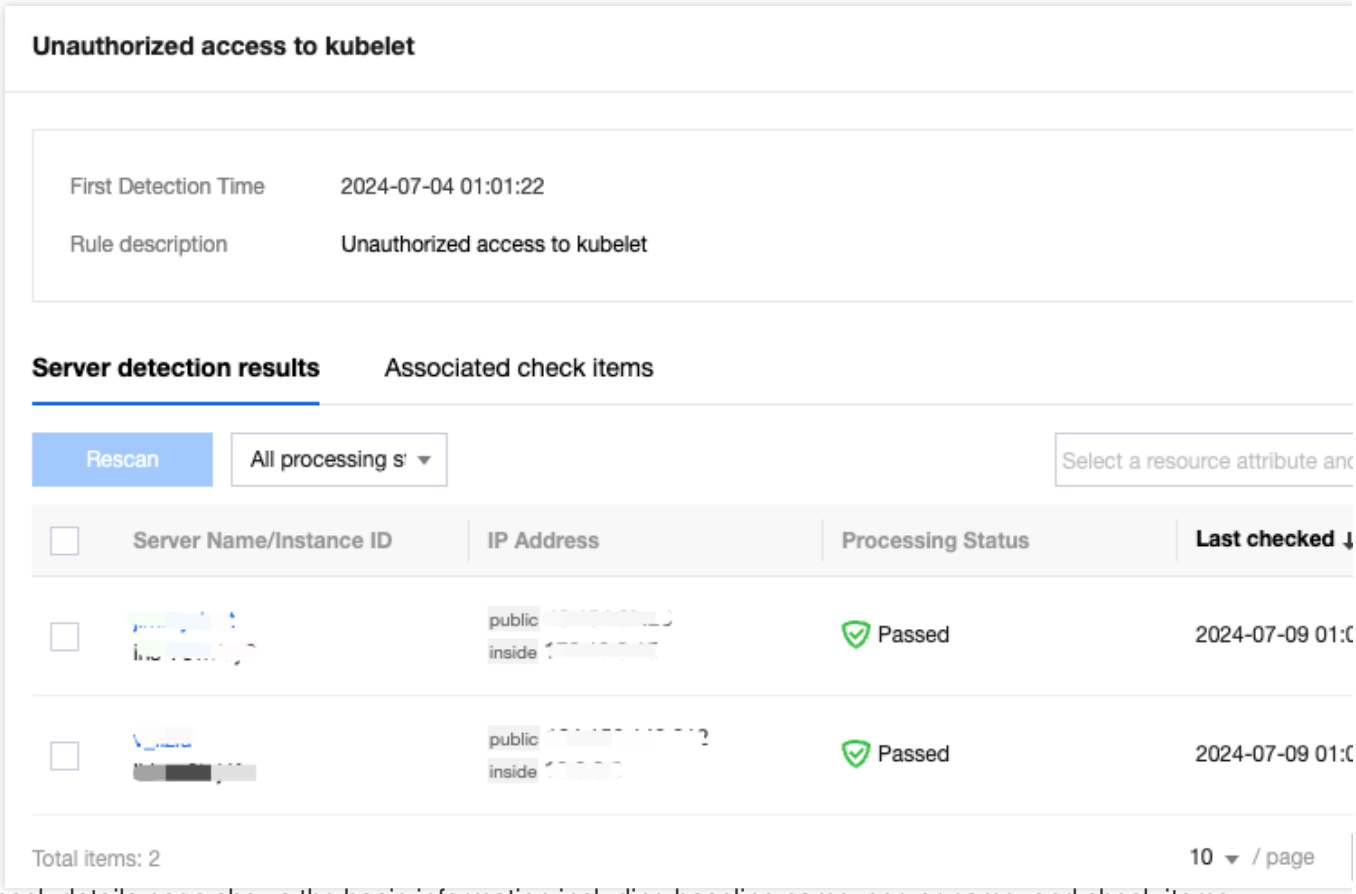
Option 1: Select the baselines for a recheck, and click **Recheck** in the upper left corner of the list to run a recheck for the selected baselines at one time.

Option 2: Click **Recheck** on the right of the desired baseline to run a recheck for the baseline.

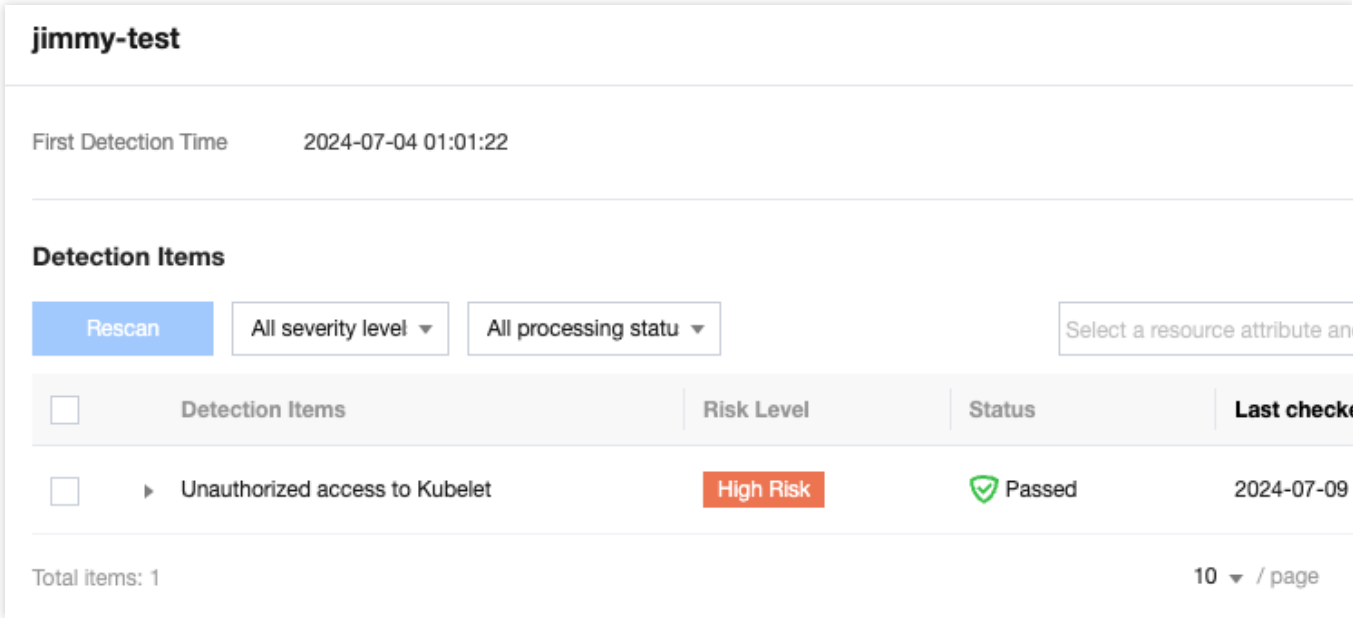
View details:

In the baseline check result list, locate the desired baseline, and then click **Details** in the Action column on the right to open the baseline details page.

The baseline details page shows 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 re-detection of servers, and viewing details of individual servers. In the action bar on the right of the target server, click **Details** to enter the detection details page.



The check details page shows the basic information including baseline name, server name, and check items.



You can run a Recheck or select Ignore for multiple check items. The ignored items can be viewed on the ignored risk item management page.

You can filter check items by threat level or status.

When you hover the mouse cursor over a check item, the details of the item, and solutions to the detected issue will appear.

Malicious File Scan

Last updated：2024-08-13 16:29:49

This document will introduce how to handle Trojan files in the CWPP console.

Malicious File Detection Settings

1. Log in to the CWPP console. In the left sidebar, choose **Intrusion Detection** > **File Scanning**.
2. On the malicious file scan page, click **Detection settings** at the top right. A settings page will pop up on the right side where you can configure the detection mode.

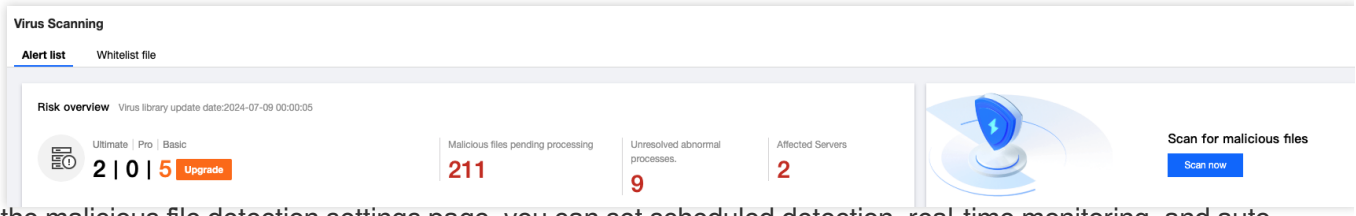
Note:

This feature is part of the Pro/Ultimate Edition. You can purchase protection authorization and bind your host to upgrade to the Pro/Ultimate Edition.

Malicious file detection supports Trojan file detection. All machines can cumulatively detect up to 5 malicious file security events for free. Beyond this limit, detection will stop. You can upgrade to the Pro or Ultimate Edition of CWPP to remove the limit. There are two common types of Trojan file detection:

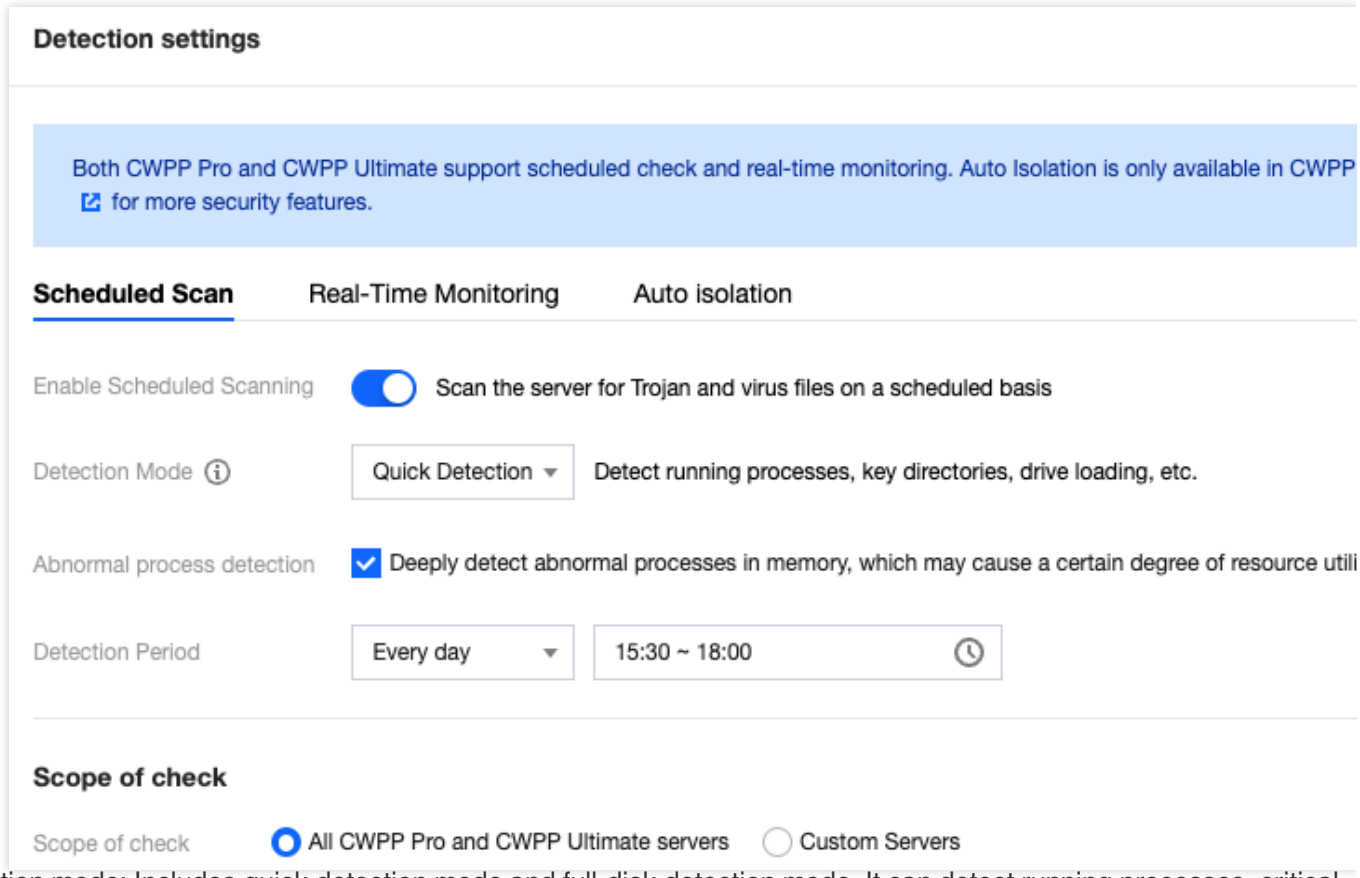
Webshell detection: Provides common detection for web site script-based backdoor Trojans, including those written in scripting languages such as ASP, PHP, JSP, and Python.

Binary detection: Provides detection for binary executable viruses and Trojans, such as DDoS Trojans, remote control software, and mining software on .exe, .dll, and .bin files, and sends alarms to users.



3. On the malicious file detection settings page, you can set scheduled detection, real-time monitoring, and auto isolation.

Scheduled detection: Click **Enable Scheduled Scanning**, 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, critical directories, and driver loading. 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 detections or timeouts.

Quick detection: For Linux systems, it will detect running processes, critical directories, and driver loading. For Windows, it will scan the C drive.

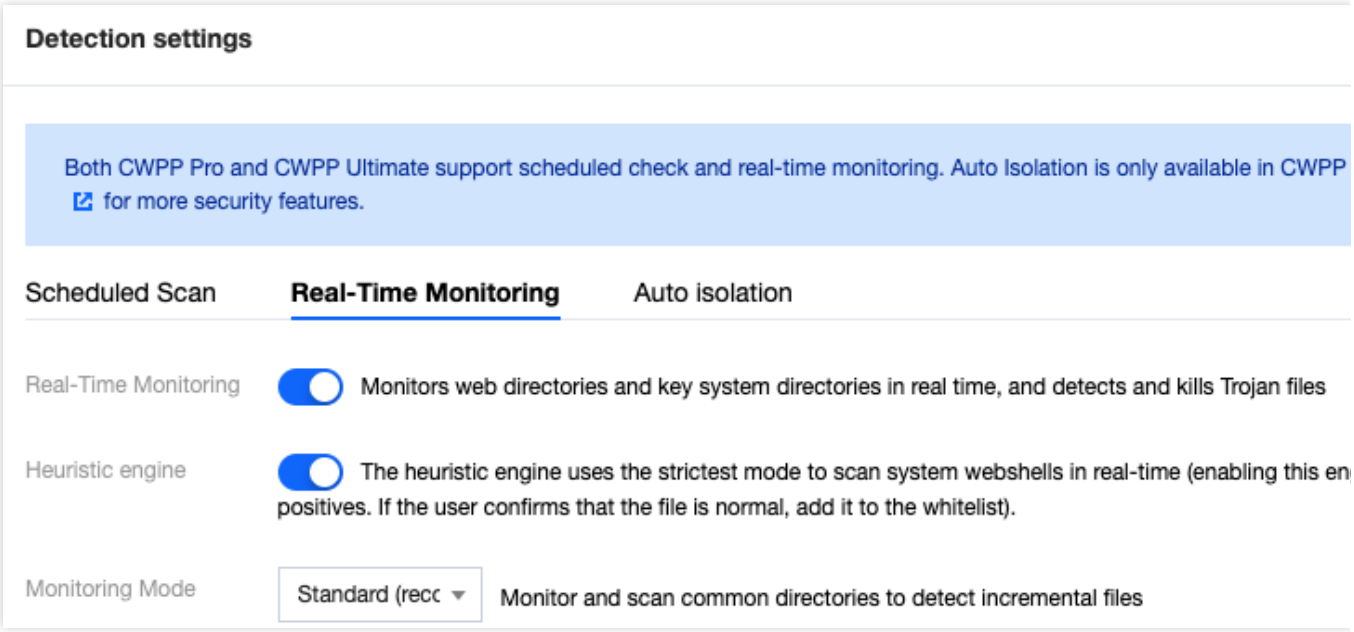
Full-disk detection: For Linux systems, it will also detect all system partitions in addition to the quick detection range. For Windows, it will scan the C, D, E, and F drives.

Abnormal process detection: Deeply detects abnormal processes in memory, which may cause a certain degree of increased resource occupancy rate. Choose with caution.

Detection period: You can choose a detection cycle of daily, every 3 days, or every 7 days.

Scope of check: Includes all Pro Edition servers and self-selected servers.

Real-Time monitoring: Click **Enable Real-Time Monitoring**, choose the monitoring mode, and then click **Save**. You can monitor web directories, system critical directories, scan and remove Trojan virus files in real-time.



Note:

Monitoring mode is divided into standard and recommendation modes.

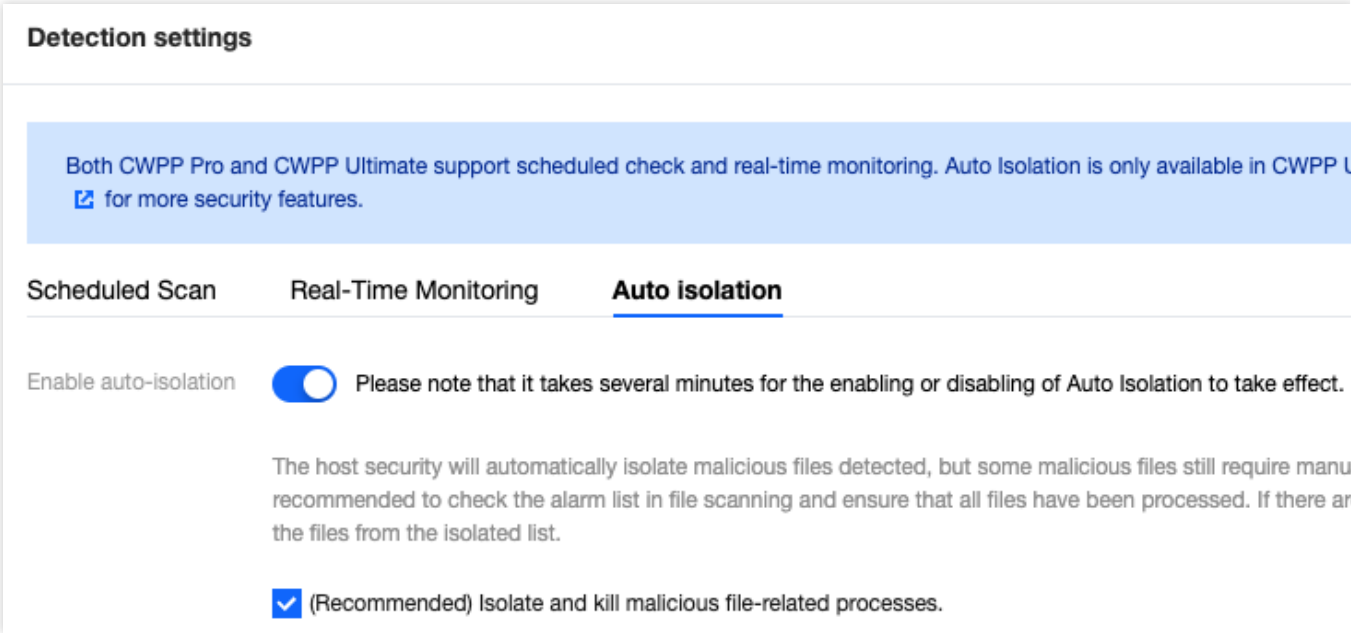
Standard: Monitors and scans for incremental files under common directories.

Deep: Monitors and scans for incremental files under all directories.

Auto isolation: Click **Enable auto-isolation** > **Save** to automatically isolate detected malicious files. Some malicious files still require manual confirmation to isolate. It is recommended to check all security events in the malicious file detection list to ensure they are all processed.

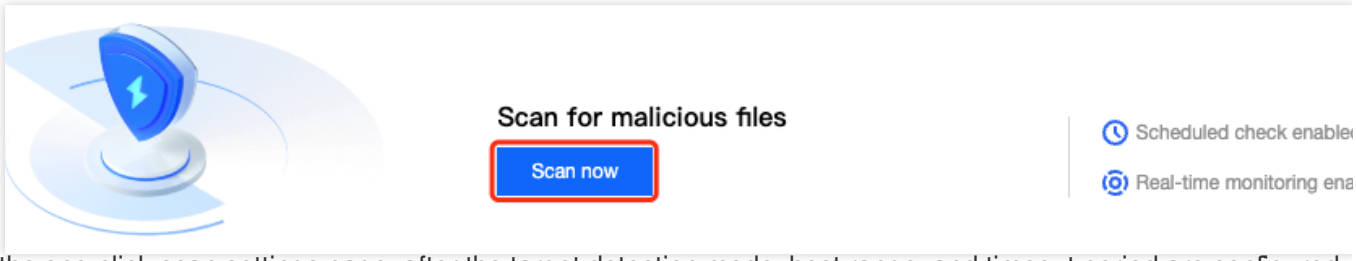
Note:

If false isolation occurs, recover the file from the isolated list. Configuring to enable or disable automatic isolation may take a few minutes to take effect.

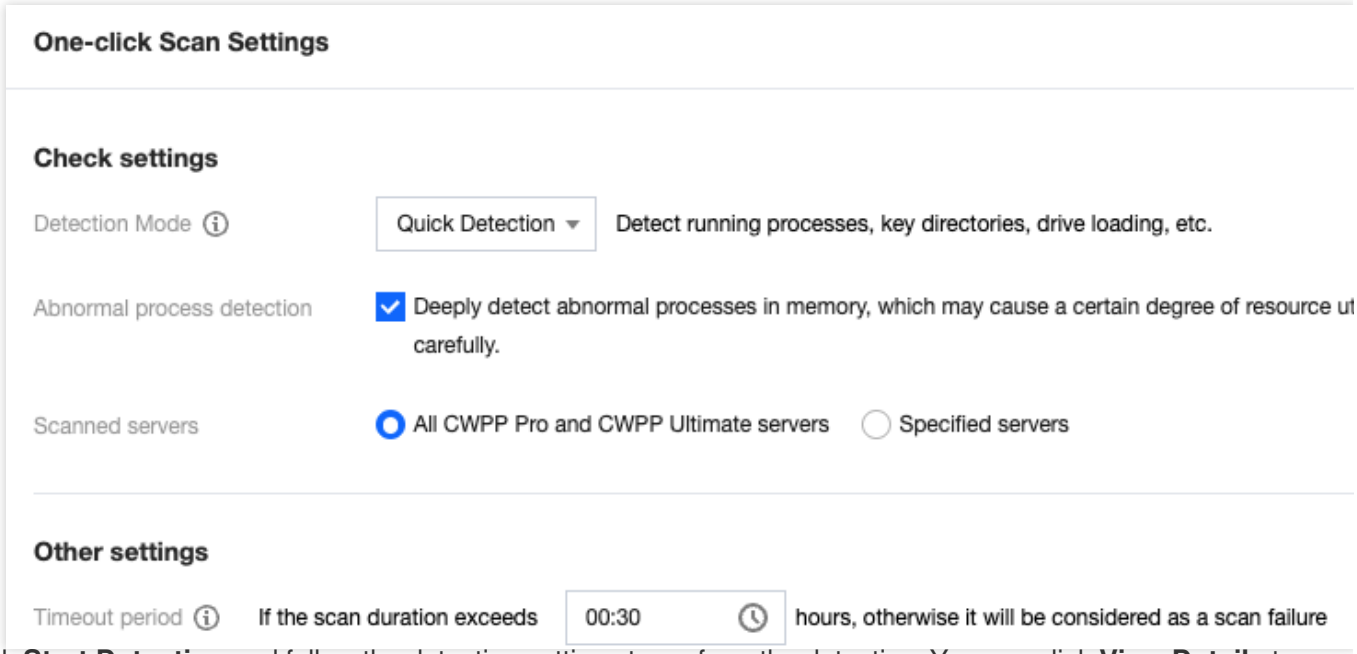


Detection Settings Overview

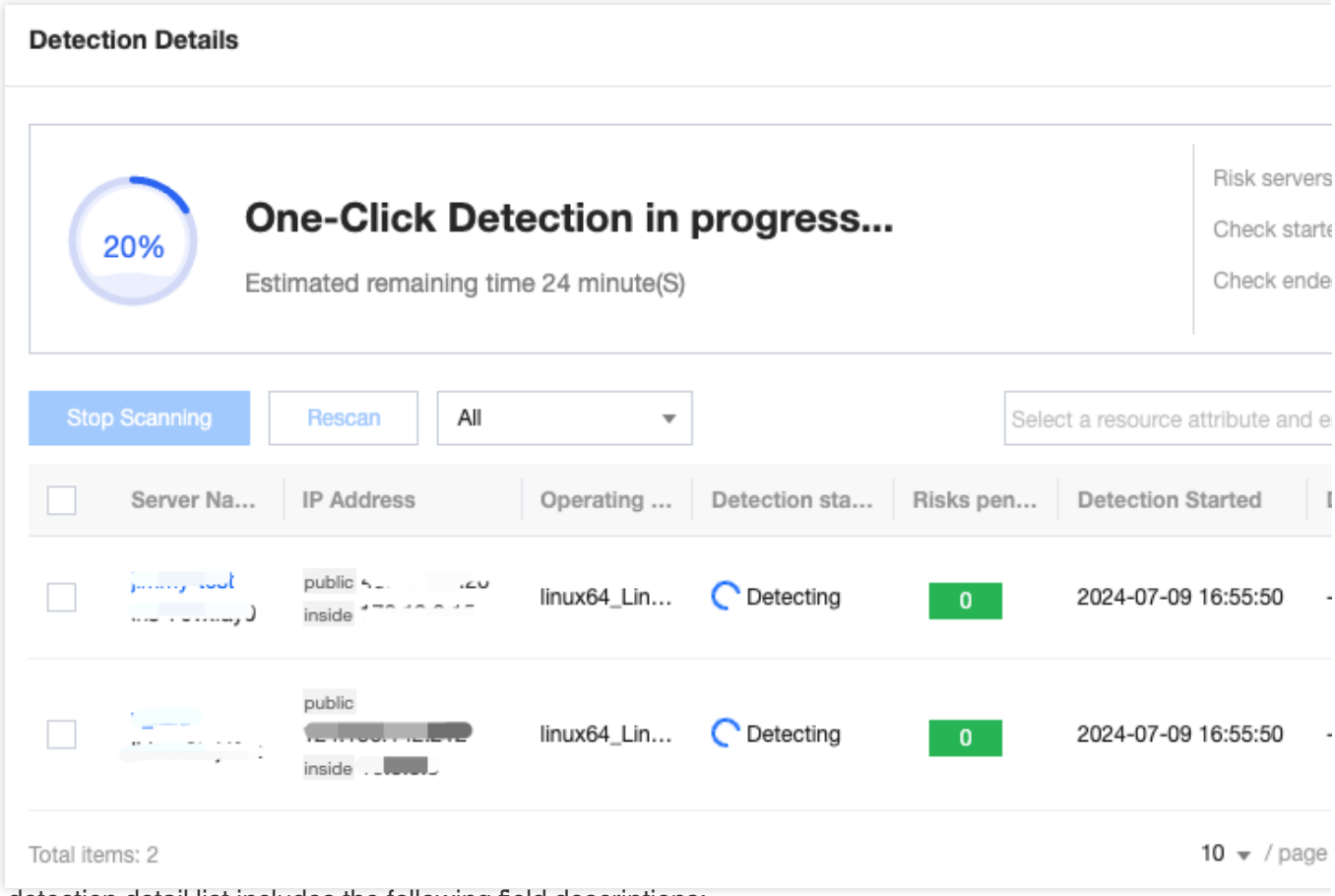
1. Log in to the CWPP console. In the left sidebar, choose **Intrusion Detection** > **File Scanning**.
2. On the malicious file scan page, click **Scan now** to start setting up manual detection mode.



3. On the one-click scan settings page, after the target detection mode, host range, and timeout period are configured, the detection might take a long time due to a large number of files and directories to scan. You can set a single scan duration, and if it exceeds the time, it will be considered a scan failure.



4. Click **Start Detection** and follow the detection settings to perform the detection. You can click **View Details** to see the detailed detection information.



The detection detail list includes the following field descriptions:

Affected Server: The target server's IP and name.

Operating System: The operating system of the target server.

Detection Status: The status of the target server's detection, including detection completed, under detection, and detection failed. The possible reason for the failed detection could be a timeout error on the target server. It is recommended to increase the timeout duration and retry. Also, the possible reason for the failed detection could be due to the client being offline. It is recommended to restart or reinstall the client and then retry the detection.

Pending Risks: The number of risk files detected on the target server that need to be addressed.

Detection Start Time: The start time of this detection.

Detection End Time: The end time of the target server's detection.

Operations:

Re-detect: If you want to re-detect a target server with a detection status of detection completed, detection stopped, or detection failed, you can click **Re-detect**.

Disable detection: If you want to stop detecting a target server with an under detection status, you can click **Stop Scan**.

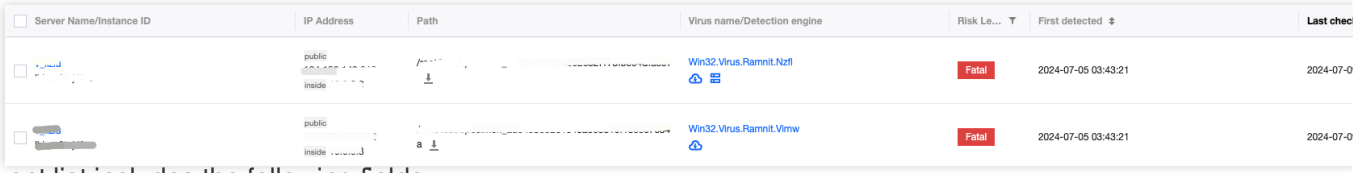
Note:

The chosen server will not be detected and potential risks will not generate alarm notifications. Proceed with caution.

View details: If you want to view the detection result details of a target server, you can click **View details**.

Viewing the Event List

1. Log in to the CWPP console. In the left sidebar, choose **Intrusion Detection** > **File Scanning**.
2. On the malicious file scan page, you can view the Trojan file detection status of the currently protected servers, as shown below:



The event list includes the following fields:

Server IP/name: The IP and name of the currently detected target server.

Path: The file path of the target risk file. Click

to copy the **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: When the target risk file was first detected.

Latest detection time: When the target risk file was most recently detected.

Processing status: The status of the target risk file. Events in pending status will indicate the presence of the file and processes from the latest detection.

Operations:

Isolation: If confirmed malicious, you can isolate a single file or batch choose files for one-click isolation. Upon successful isolation, the original malicious file will be encrypted and isolated. You can later filter **Isolated** files for recovery.

Trust: If the file is non-malicious, you can choose the trust operation. Trusted files will no longer be scanned by CWPP. You can manage trusted files by filtering **Trusted Files**.

Delete the record: This action only deletes log records, rather than the file. Once it is 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 detection result details of the target risky file, you can click **View Details**.

FAQs

Why Did the Trojan File Isolation Fail?

Trojan file isolation usually fails because the Trojan file resists security software. It is recommended to manually delete the alarm file from the server first. If the issue persists, you can submit a ticket to contact us for assistance. You can also try using Tencent PC Manager on Windows systems to remove it.

Subsequent Steps

For a Linux intrusion troubleshooting guide, refer to intrusions on Linux.
For a Windows intrusion troubleshooting guide, refer to intrusions on Windows.

Unusual Login

Last updated：2024-08-13 16:29:50

This document describes how to use the Anti-Unusual Login feature.

Overview

When log-in behaviors from a server do not meet the allowlist criteria (common source IP, common username, common log-in location, and common log-in time), an unusual log-in alarm will be generated. If the source IP of the unusual log-in is an overseas IP (including Hong Kong (China), Macao (China), and Taiwan (China)) or a malicious IP from threat intelligence, it will be marked as High-risk. Otherwise, it will be marked as Suspicious.

Important Notes

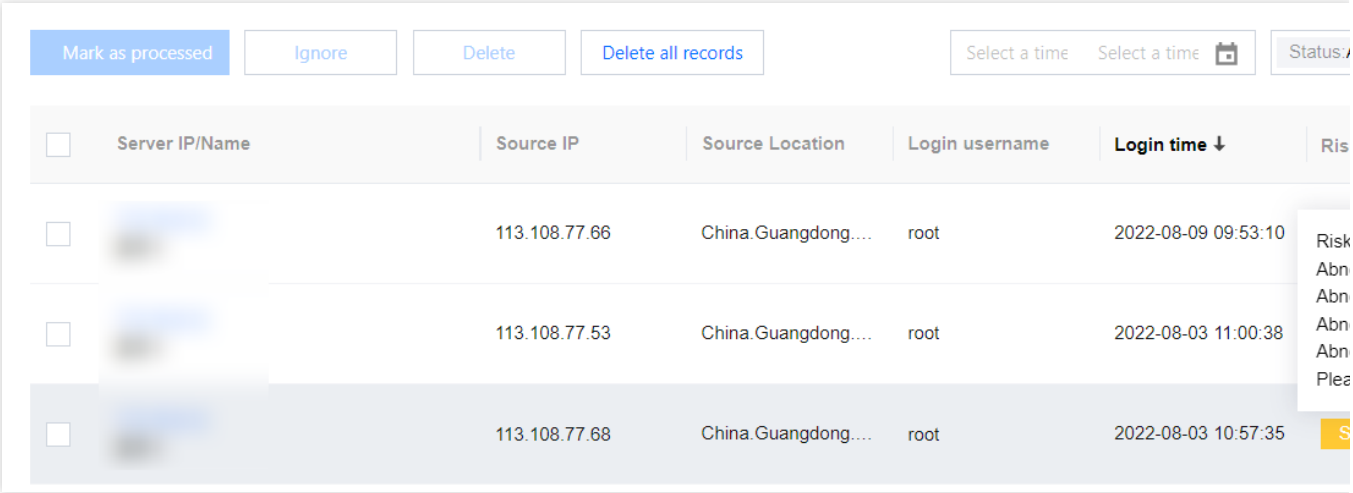
Hosts with CWPP agent installed (client online) will have unusual log-in behaviors monitored in real-time.
The CWPP console only retains the unusual login events for the last 6 months, and the event data generated 6 months ago is not displayed.

Operation Guide

1. Log in to the CWPP console.
2. Click **Intrusion Detection** > **Unusual Login** on the left sidebar. The fields and operations related to the feature are described as follows.

Event List

In the **Event List**, you can view and handle unusual login risks detected by CWPP.



Field description:

Server IP/Name: The target server of the unusual login attempt.

Source IP: Source IP of the unusual login attempt, which generally is an egress IP of a company's network or a proxy IP.

Source Location: The location where the login source IP is located.

Login Username: The username used by the user who successfully logged in to the server.

Login Time: The time when the user successfully logged in to the server (The time shown on the server).

Threat Level: Suspicious/High.

Status

Unusual Login: A login attempt from an unusual location, with an unusual user name, at an unusual time, or from an unusual IP.

Allowlisted: The login source has been added to the allowlist (login source IP, login username, login time, and usual login location).

Handled: The event has been handled manually and marked as Handled.

Ignored: This alarm event has been ignored.

Operation

Actions

Mark as processed: If the event has been handled manually, mark the event as "Handled".

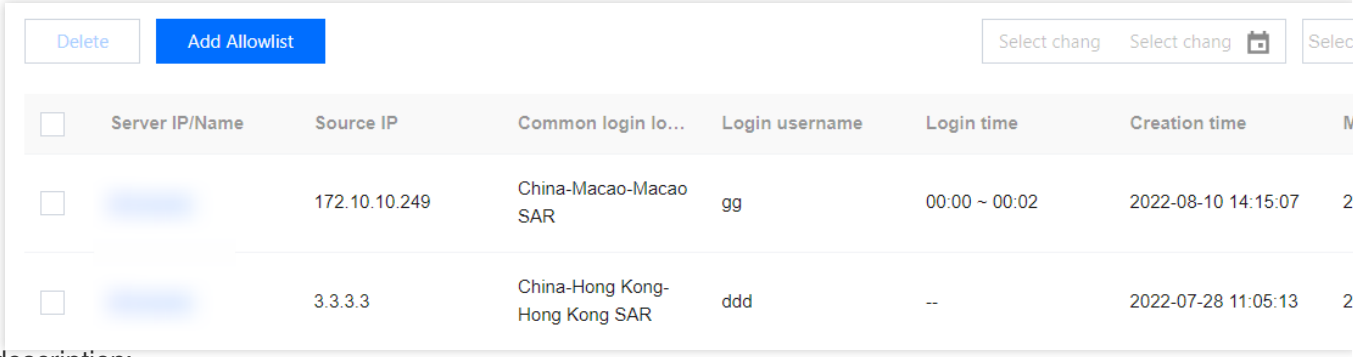
Add to Allowlist: Once an event is added to the allowlist, no alarm will be sent if the same event occurs again.

Ignore: Only ignore this alarm event. If the same event occurs again, an alarm will be sent again.

Delete Record: Once deleted, the event record will no longer be displayed on the console and cannot be recovered.

Allowlist Management

In **Allowlist Management**, 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 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 added to the allowlist.

Creation time: The time when the allowlist was created.

Update time: The time when the allowlist was last updated.

Operation

Edit: Re-edit the login source IP, login username, login time, usual login location, covered servers, etc.

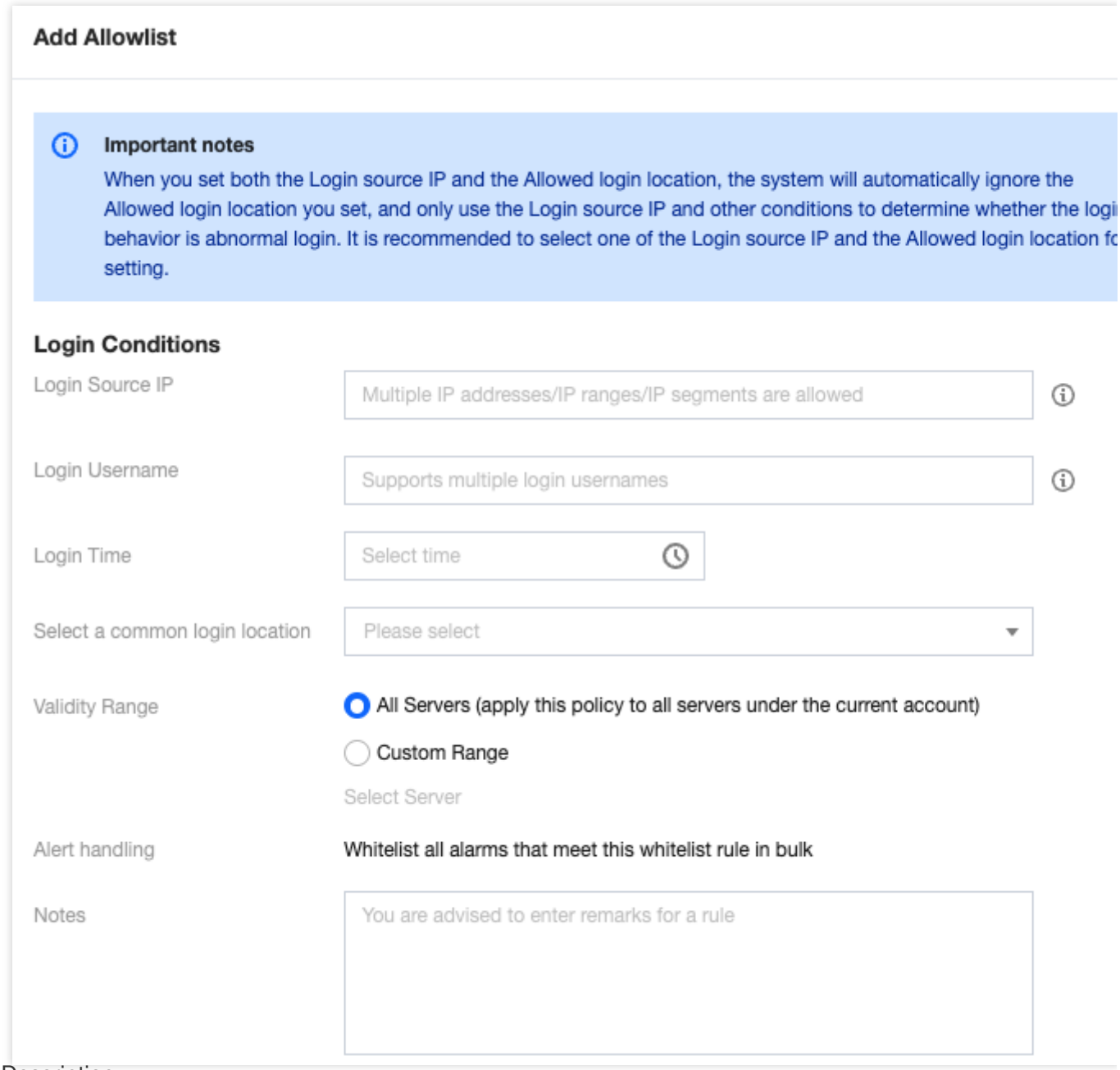
Delete: Delete items from the allowlist.

FAQs

How to Process Unusual Log-in Alarms?

Determine whether the log-in behavior is self-initiated.

If it is your own log-in behavior and you do not want to see the alarm again, click **Processing** , and select **Add to allowlist** to configure common log-in source IP, log-in username, log-in location, log-in time, and effective range.



Field Description:

Empty Log-in Source IP: Indicates that log-in attempts from any source IP to the server will not trigger an alarm.

Empty Log-in Username: Indicates that log-in attempts with any username to the server will not trigger an alarm.

Empty Log-in Location: Indicates that log-in attempts from any location will not trigger an alarm.

Empty Log-in Time: Indicates that log-in attempts at any time will not trigger an alarm.

Note:

Log-in source IP, log-in username, log-in location, and log-in time cannot be empty at the same time.

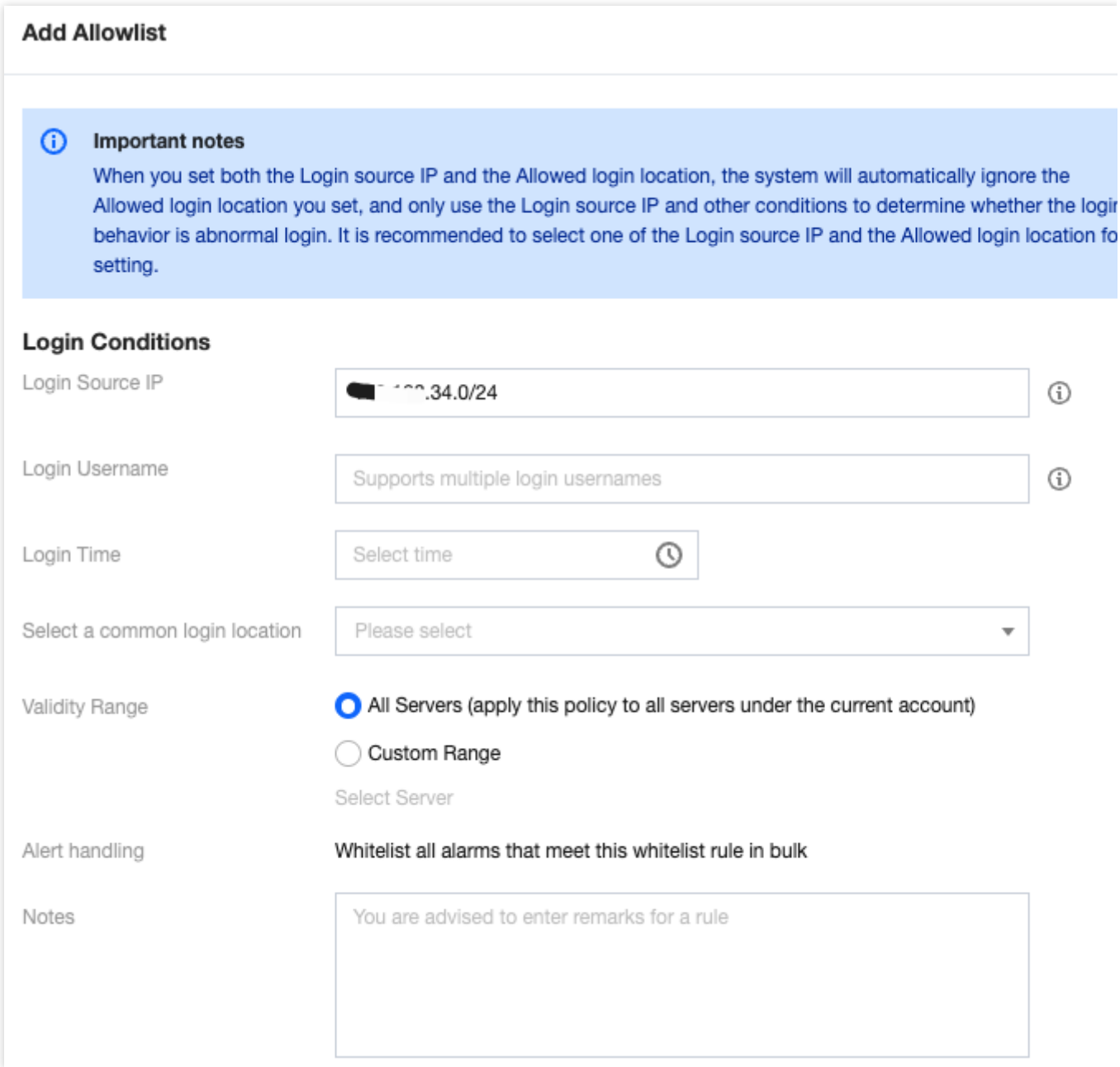
If the log-in behavior is not from you, immediately change the server log-in password (it is recommended to be more than 10 characters, including uppercase and lowercase letters and special characters for a strong password.).

The server has been logged in abnormally, and the intruder might have already intruded your server and left malicious files. It is recommended to immediately perform malicious file scan, vulnerability detection, baseline detection to enhance your server's security.

How to Set an Allowlist to Meet Most Users' Needs?

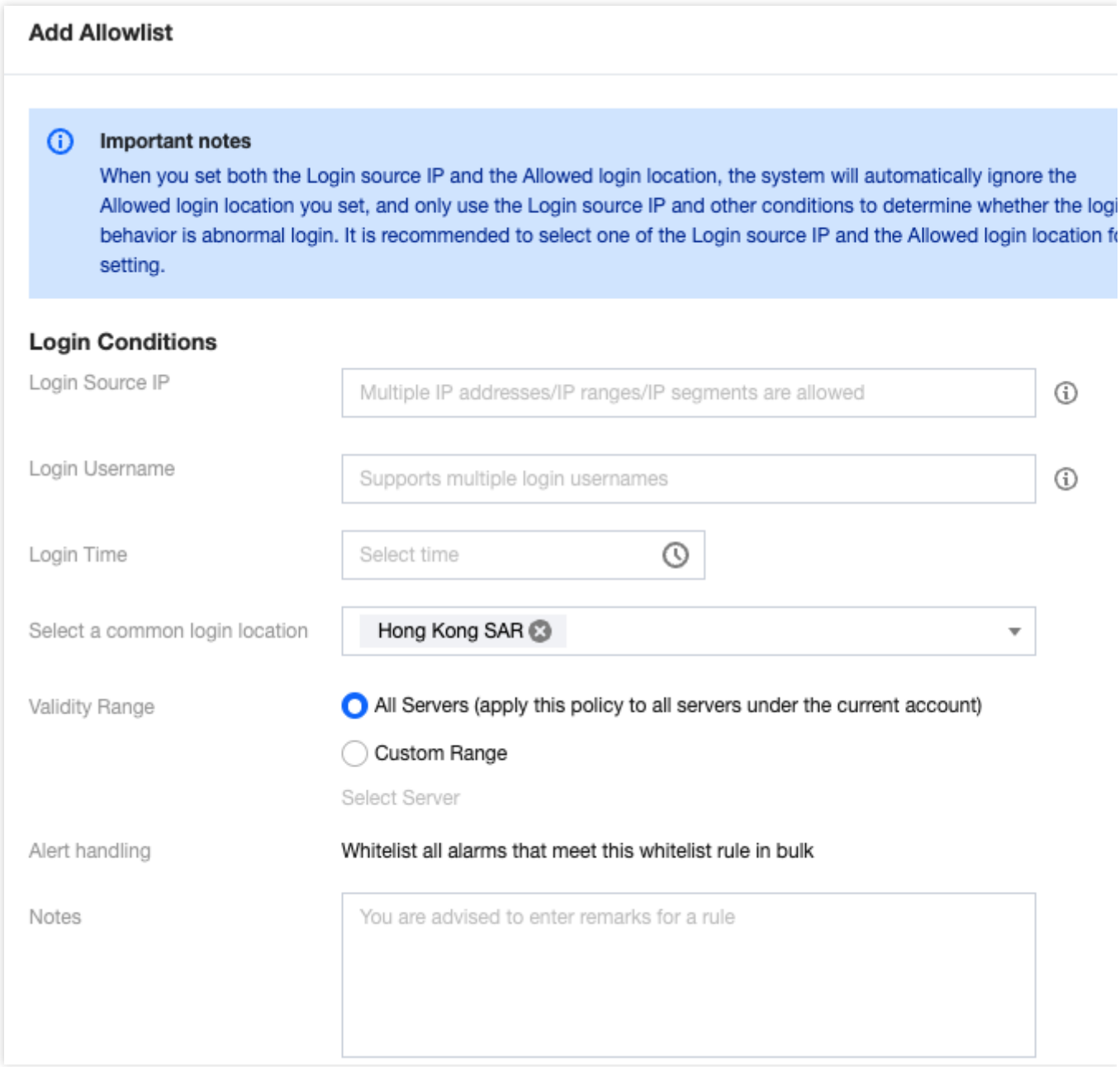
Scenario 1: The source IP is a fixed IP segment. Users using any username can log in to the server from this segment without triggering abnormal log-in alarms.

You can enter the IP segment in the log-in source IP and select the effective server range.



Scenario 2: The source IP is dynamic. Users from any location within Hong Kong (China) can log in to the server at any time using any username without triggering abnormal log-in alarms.

Select Hong Kong (China) Special Administrative Region in the list of common log-in locations and select the effective server range.

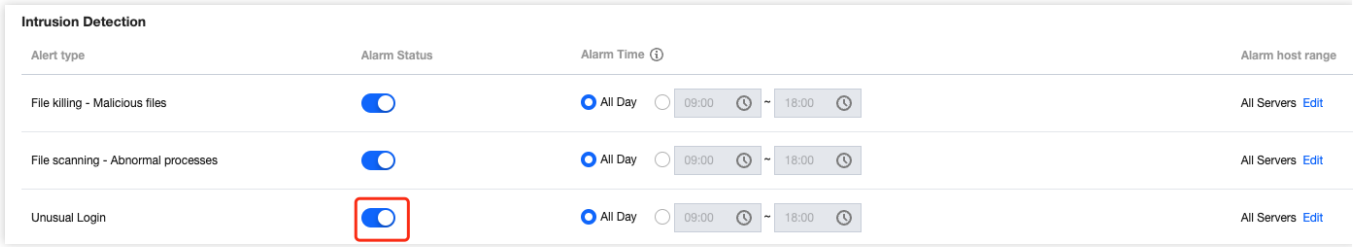


Note:

Combinations of log-in conditions are supported.

How to Disable Abnormal Log-in Alarms?

Go to alert settings to turn off the abnormal log-in alarm switch. If you keep the alarm switch on, it is recommended to select the high-risk option to only alarm on high-risk abnormal log-in behaviors.



Password Cracking

Last updated：2024-08-13 16:29:49

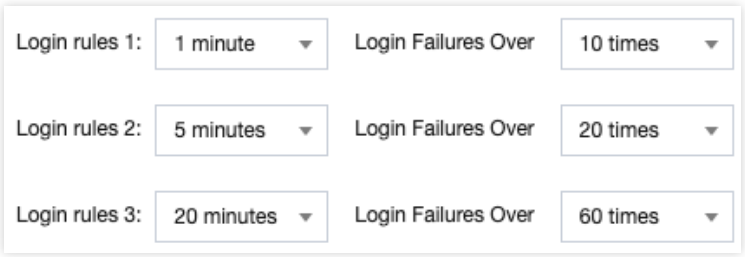
This document will introduce how to configure and use the password cracking monitoring feature to enhance system security.

Overview

CWPP password cracking, based on Tencent Cloud's network security defense and host intrusion detection capabilities, provides real-time monitoring of password cracking behavior for hosts, implements automatic blocking feature, and supports alarm querying, filtering, deletion, and batch export.

Restrictions

Monitoring scope: Monitors Basic/Pro/Ultimate Edition hosts (Linux systems and Windows systems) for log-in behavior via SSH protocol/RDP protocol.
Detection rules and block mode: The judgment rules and blocking scope for password cracking behavior are different across protection versions. See the table below.

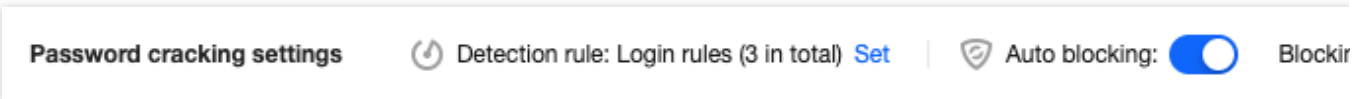
CWPP Protection Versions	Detection Rules	Blocking Mode
Basic Edition	Intelligence rules: Based on Tencent's security threat intelligence database, comprehensive recommendations of blocklisted IPs are made. When hitting a matching blocklisted IP, the behavior will be identified as password cracking. Detection rules: When any of the following log-in rules are hit, the behavior will be identified as password cracking.  Login rules 1: 1 minute Login Failures Over 10 times Login rules 2: 5 minutes Login Failures Over 20 times Login rules 3: 20 minutes Login Failures Over 60 times **Note:** The default detection rules for the Basic Edition are only the three shown above. Addition and modification are not supported.	Basic blocking refers to the measure of blocking password cracking activities from IPs listed in threat intelligence blocklists only. The default duration of blocking is

	If the paid Edition expires and reverts to the Basic Edition, the previously set detection rules will still be effective, but addition and modification are not supported.	set to 5 minutes. **Note:** If the paid Edition expires and reverts to the Basic Edition, the blocking mode will automatically switch to basic blocking.
Pro Edition/Ultimate Edition	Includes the above intelligence and detection rules. (Detection rules support addition and modification.)	Advanced blocking refers to the use of Tencent's security database to block both blocklisted IPs and password cracking activities that match detection rules.

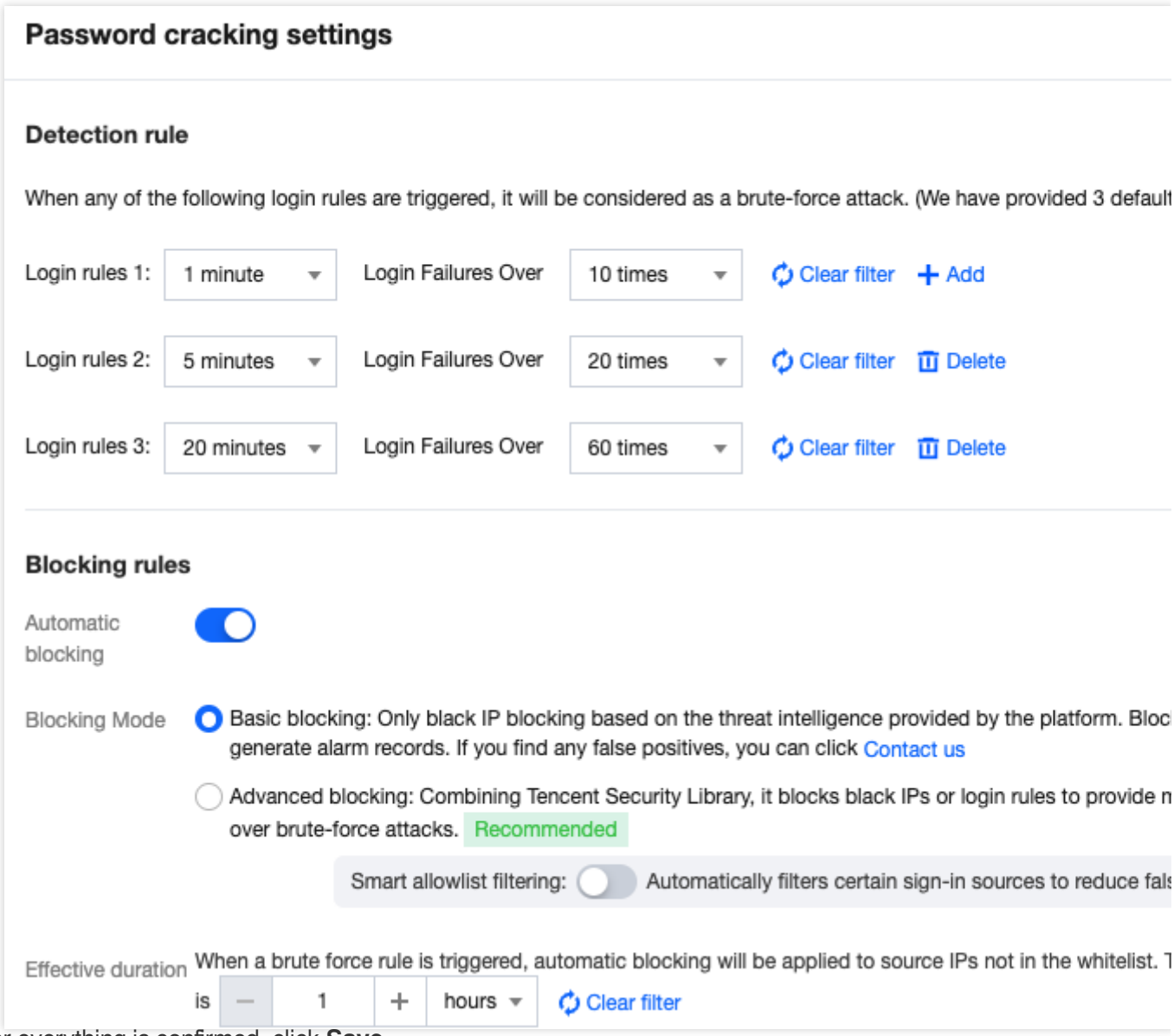
iptables rules: After blocking is enabled, when password cracking activities are detected on the host, the source IP will be automatically added to the iptables rules.

Password Cracking Settings

1. Log in to the CWPP console. In the left sidebar, choose **Intrusion Detection** > **Password Cracking**.



2. Click **Set** to configure the judgment and blocking rules for password cracking activities.



3. After everything is confirmed, click **Save**.

Configuring Allowlists

After the allowlist is configured, password cracking behavior from the source IP in the allowlist will not be blocked or alarmed. Follow these steps:

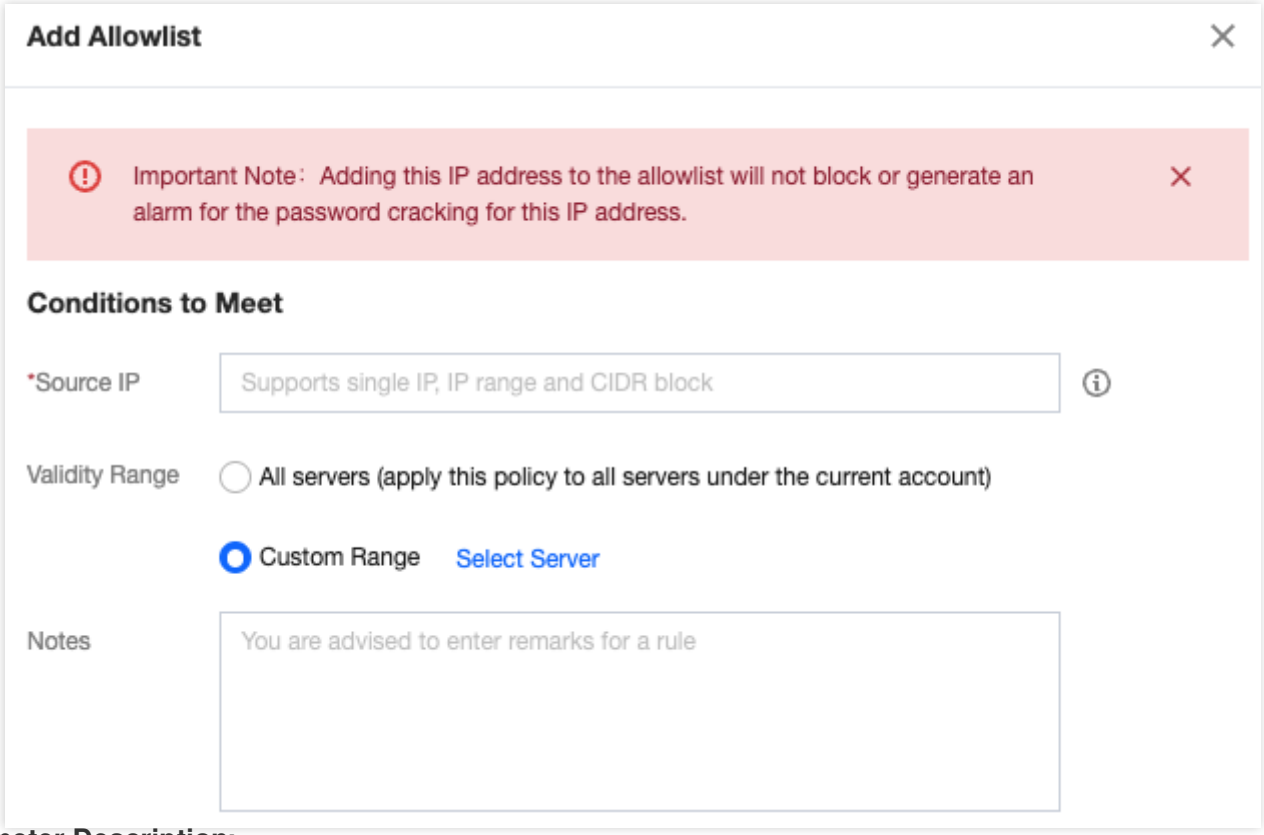
1. Log in to the CWPP console. In the left sidebar, choose **Intrusion Detection** > **Password Cracking**.
2. On the password cracking page, click **Allowlist Policies** > **Add Allowlist**.

3. On the add to allowlist page, enter the source IP and effective range, and then click **OK**.

Note

After it is added to the allowlist, password cracking behavior from that source IP will not be blocked or alarmed.

Proceed with caution. If a non-allowlist source IP attempts to log in and triggers brute-force cracking rules, the system will automatically issue an abnormal alarm or block.



Parameter Description:

Source IP: You can enter a single IP, an IP range (e.g., 1.1.1.1-1.1.1.10), or a IP segment (e.g., 1.1.1.0/24).

Validity Range:

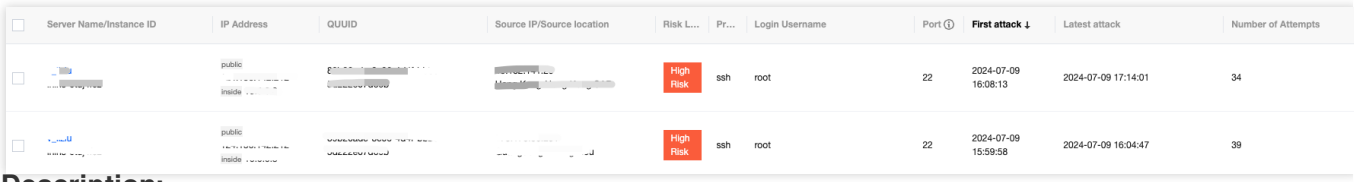
All servers (**choose with caution**): This will add the allowlist trust condition to all servers under the user's AppID.

Custom range: Allows for customizing servers to which the allowlist trust condition will be applied.

Notes: It is recommended to enter relevant rule remarks.

Viewing Password Cracking Events

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



Field Description:

Server IP/Name: The server currently being brute-force cracked.

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.

Log-in 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 CWPP first detected password cracking behavior.

Latest Attack Time: The time when the event occurred again recently.

Attack Time: The time the attacker initiated the brute-force crack.

Number of Attempts: The number of times the attack IP attempted brute-force attacks.

Cracking Status: Indicates whether the current server has been successfully or unsuccessfully brute-forced.

Blocking Status: Whether the auto blocking of the attack is successful or unsuccessful.

Operations:

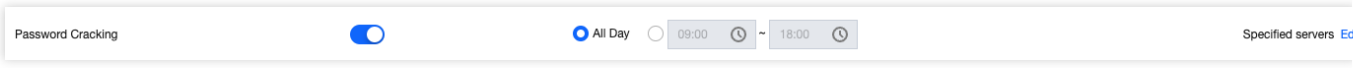
Upgrading Version: The current server is eligible for upgrading to CWPP Pro Edition. You can click **Upgrading Version** to upgrade.

Add to Allowlist: When an error blocking occurs, you can click **Add to Allowlist** to immediately unblock.

Delete the Record: You can delete the event record, and it will no longer be displayed.

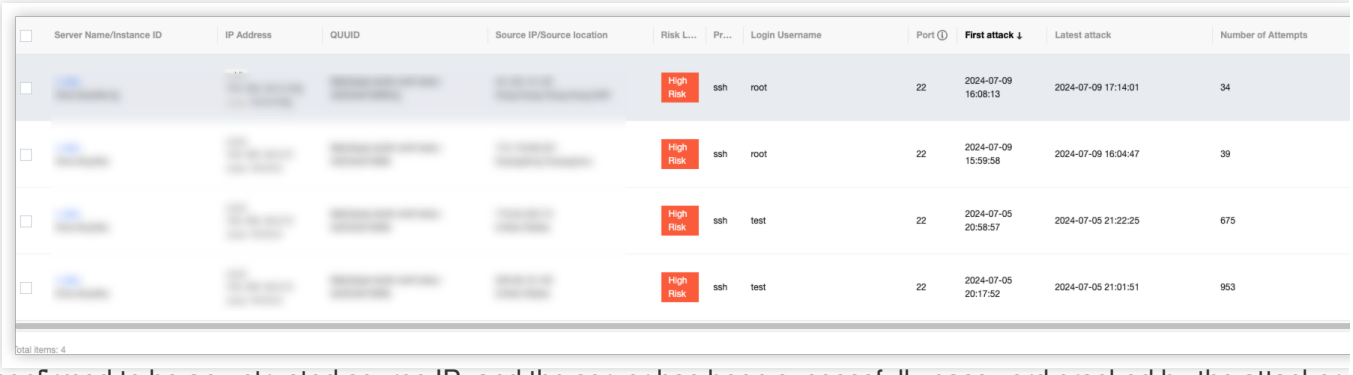
Enabling Alarm Notifications

Log in to the CWPP console. In the left sidebar, choose **Settings** > **Alarm Settings**. In alarm settings, enable the **Alarm Notification Switch**. When a password cracking event occurs, notifications will be sent via message center, SMS, email, WeChat, and WeCom.



Alert Handling

1. When the user receives a password cracking event alarm, the user needs to log in to the CWPP console. In the left sidebar, choose **Intrusion Detection** > **Password Cracking**.
2. In the alarm list page, view the attack source IP in the corresponding alarm event list.
If it is confirmed to be a trusted source IP, the user needs to click **Process** > **Add to allowlist** in the operation column on the right side of the event, and set the add allowlist conditions and effective range **(proceed with caution when adding to the allowlist)**. Once it is configured successfully, the configuration will take effect within 5 minutes. Subsequent password cracking activities from this source IP will no longer trigger alarms or be blocked.



If it is confirmed to be 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 CWPP has been upgraded to Pro Edition or Ultimate Edition. If not, it is recommended that the user click **Upgrading Version** in the operation column on the right side of the event to upgrade to Pro Edition or Ultimate Edition CWPP.
2.1.2 At the top of the alarm list, enable the automatic block switch**. It is recommended to choose the Standard Blocking** mode. Future attacks from the source IP will be automatically blocked for a default duration of 15 minutes. Users can define the duration as needed.
2.1.3 For servers that have been intruded by password cracking, it is recommended that users immediately set a complex password (12-16 characters consisting of uppercase letters, lowercase letters, special characters, and numbers). Check if there are any unknown accounts in the account list, and delete or disable unknown accounts. At the same time, check for system anomalies.

Malicious Requests

Last updated：2024-08-13 16:29:50

This document will introduce how to view and manage the alarm list and policy configuration of malicious requests.

Overview

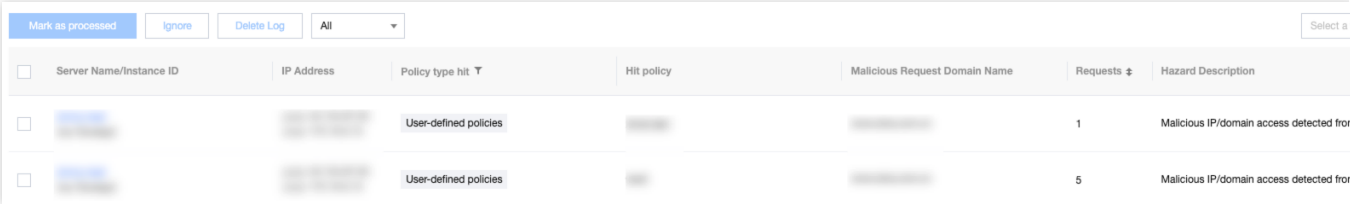
The malicious request feature provides the capability to monitor and handle external request behaviors in real-time, effectively identifying malicious request behaviors. If a host initiates requests to malicious domains, the behavior will be identified and recorded. Upon detecting such malicious request behaviors, the system will provide you real-time alarms.

Restrictions

Malicious request monitoring supports Pro Edition or Ultimate Edition hosts.
Malicious request interception is supported only for hosts of Ultimate Edition running Linux systems. It is limited to intercepting DNS queries made by the server. It does not support the interception of forwarded traffic.

Alert List

1. Log in to the CWPP console. In the left sidebar, choose **Intrusion Detection** > **Malicious Requests**.
2. On the malicious requests page, you can view the alarm list of malicious requests and perform related operations.



Filters: You can filter by policy type hit, status, last requested, entering the host name in the search box, instance ID, IP address, or malicious request domain name.
Custom display columns: Click

to set the fields displayed in the alarm list.
Export: Click

to export detailed information from the alarm list.

Field Description:

Server Name/Instance ID: The host name and instance ID initiating the request to the malicious domain.

IP Addresses: The host IP initiating the request to the malicious domain.

Policy Type Hit:

Preset Policy: The preset policy is a rule configuration that has been developed by Tencent's CWPP operation experts and algorithm experts through the accumulation of multiple models, and it is applicable for detecting most malicious requests.

User-defined Policies: Users set alarm/intercept/allow actions for relevant domains based on their business needs.

Hit Policy: The name of the policy hit when the host requests a malicious domain.

Malicious Request Domain Name: Domains or IP addresses.

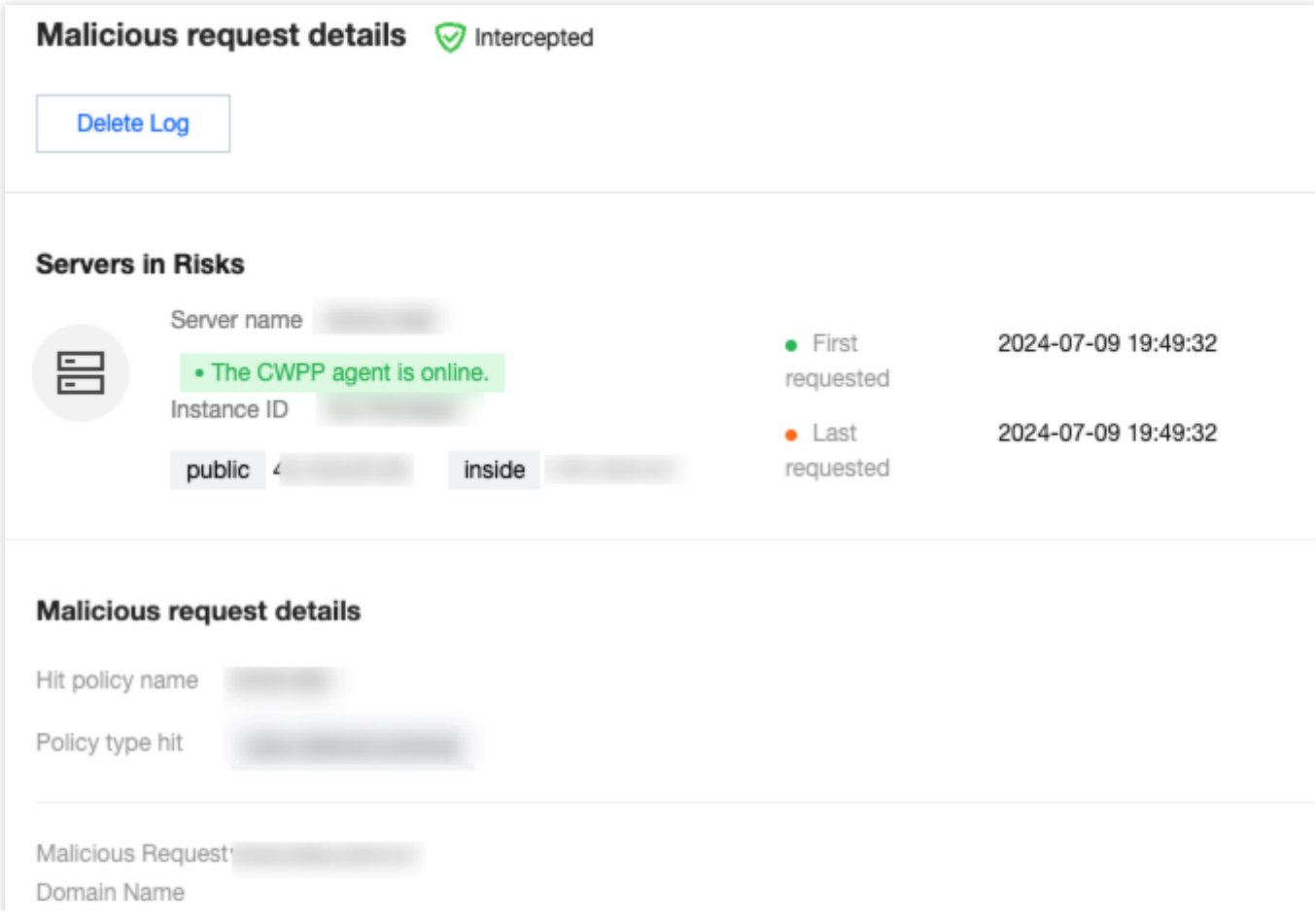
Requests: Number of times the host has made requests.

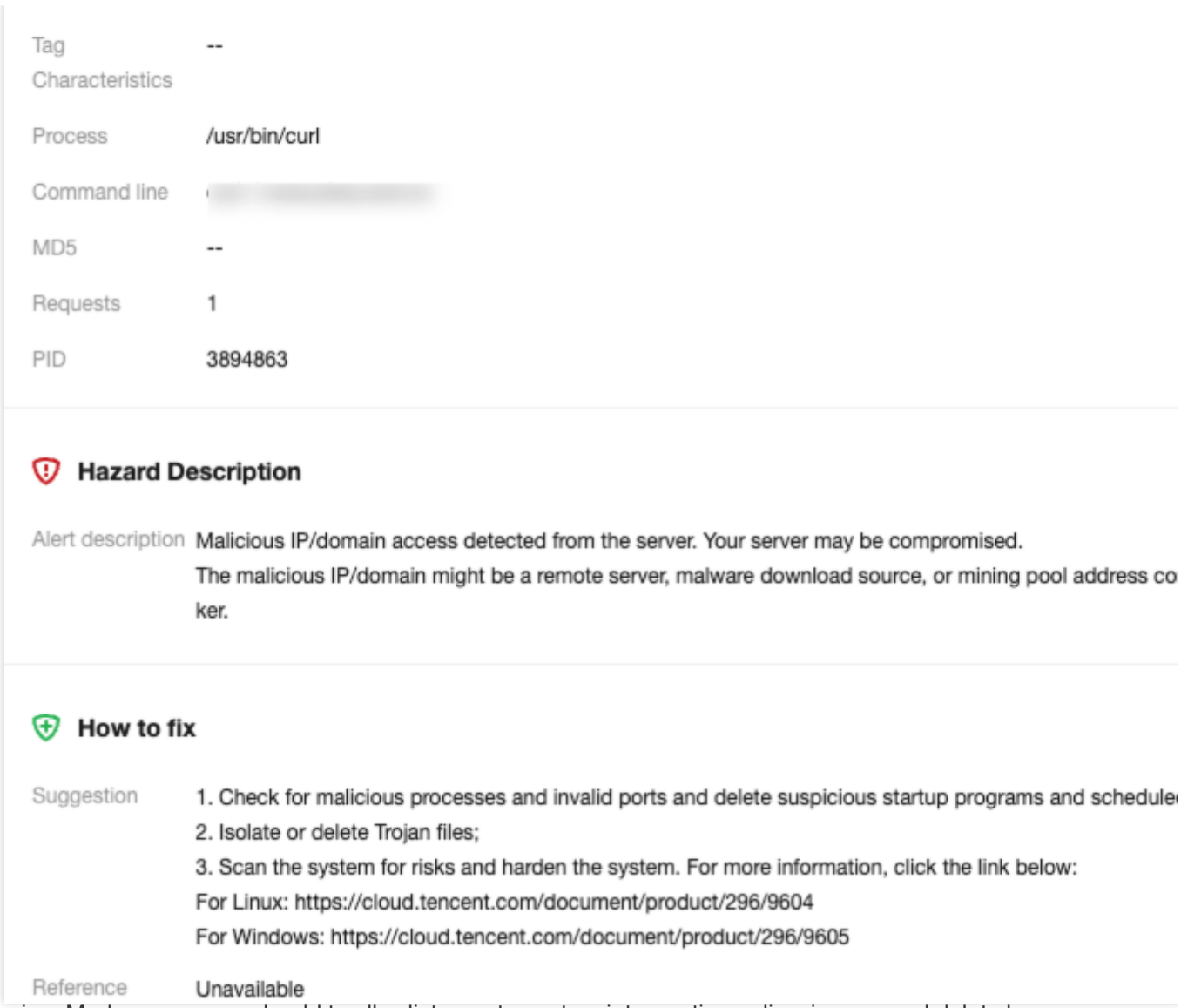
Hazard Description: Potential hazard that may result from requesting the malicious domain.

Last Requested: The last time the malicious domain was requested.

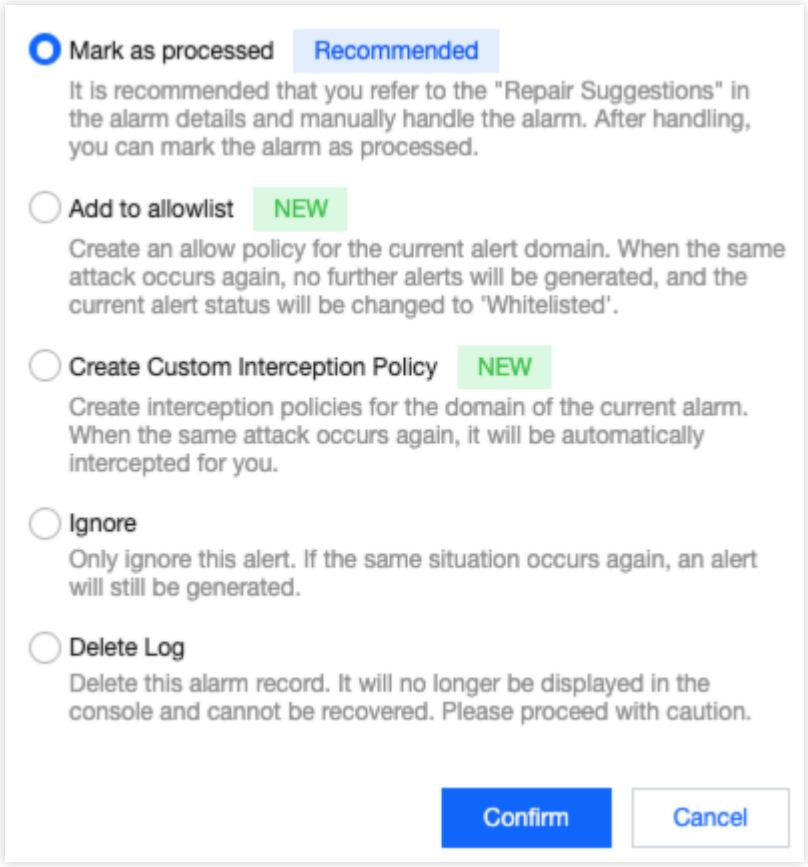
Status: Pending, allowlisted, processed, ignored, and intercepted.

Details: View detailed information on the malicious request event, including risk host information, malicious request details, hazard description, and fix suggestions.





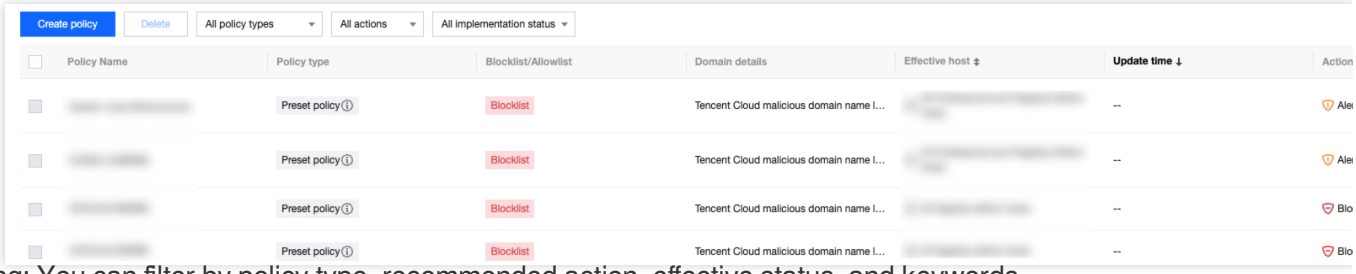
Processing: Mark as processed, add to allowlist, create custom interception policy, ignore, and delete log.



Policy Configuration

Managing a Policy

On the top of the malicious request page, select **Policy configuration** to enter the policy configuration page.



Filtering: You can filter by policy type, recommended action, effective status, and keywords.

Custom display columns: Click

to set the fields displayed in the policy list.

Export: Click

to export detailed information from the policy list.

Field Description:

Policy Name: Fixed preset policy names, including system rules (critical protection) and system rules (standard). For user-defined policies, the name will be as specified by the user.

Policy Type: Preset policy, and user-defined policy.

Blocklist/Allowlist: This policy belongs to the allowlist/blocklist.

Domain Details: IP/domain name or wildcard domain.

Effective Hosts: The range of hosts where the policy is effective.

Update Time: The time when the policy was last updated.

Action: Actions automatically performed when the policy is hit by the domain request (allow/alarm/intercept).

Implementation: Whether the policy is effective.

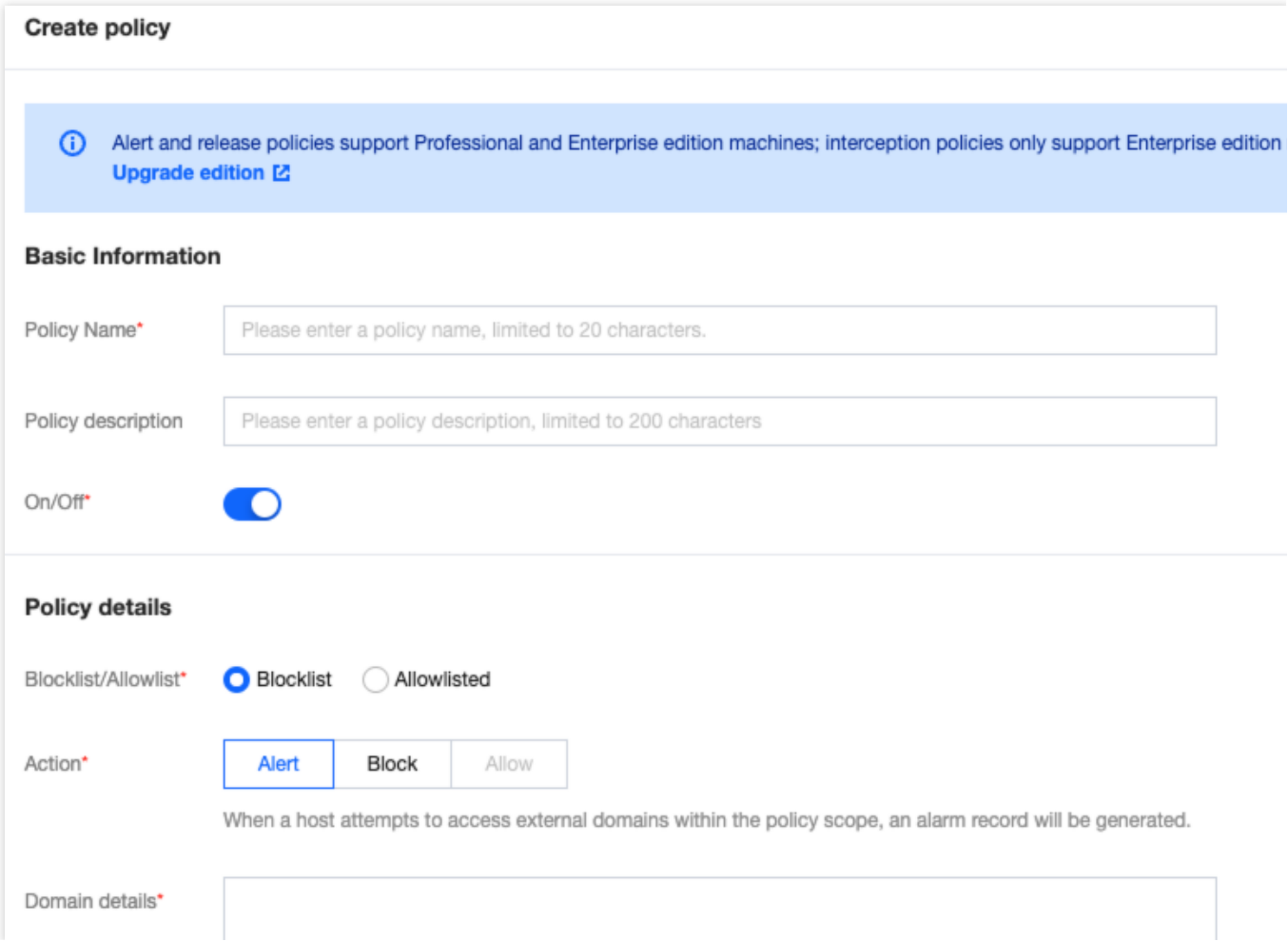
Edit: Edit the policy.

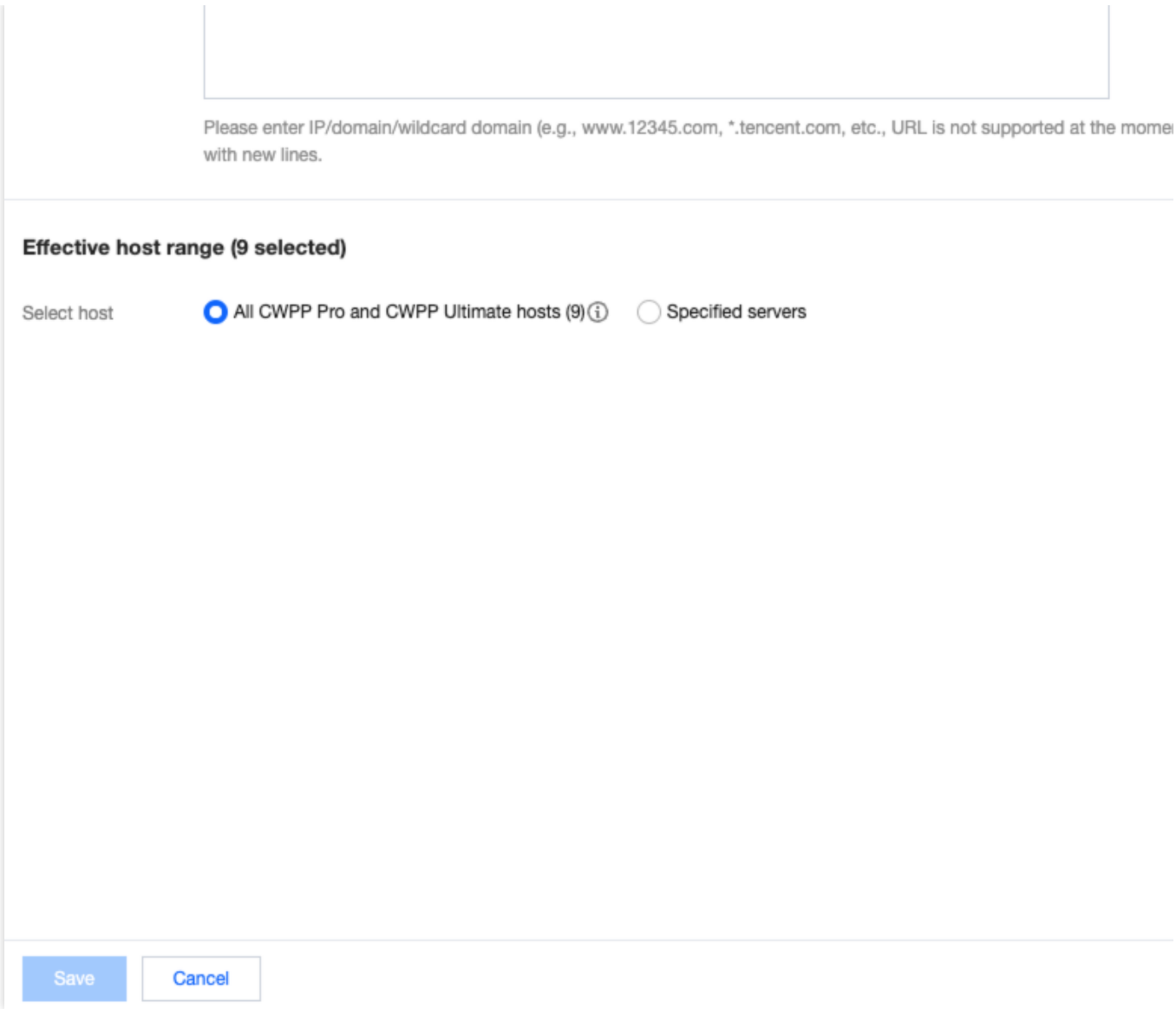
Delete: Delete the policy.

Create a Policy:

Blocklist: When the host requests a domain in the blocklist, an alarm/intercept action will be performed.

Allowlist: When the host requests a domain in the allowlist, an allow action will be performed.





Note:

Preset policies are built-in policies that do not support adding, editing, or deleting, and that only support Enable/Disable switching.

It is recommended to keep the preset policies (standard) enabled, and to make the preset policies (critical protection) enabled as needed during critical protection periods.

In user-defined policies, the interception policy is only effective for Ultimate Edition hosts.

System Auto-Interception Rules

The malicious request feature now includes system auto-interception rules. Once enabled, the system automatically intercepts detected malicious domains and IPs. However, some configurations still require your manual policy settings.

System blocklist domains and IPs: A list of domains and IPs refined by CWPP operation experts and algorithm experts. Domains and IPs on this list can be automatically intercepted.

Principles of Interception: Malicious requests refer to the termination of access requests to legitimate domains/IPs. It does not terminate the process but stops the access request.

Note:

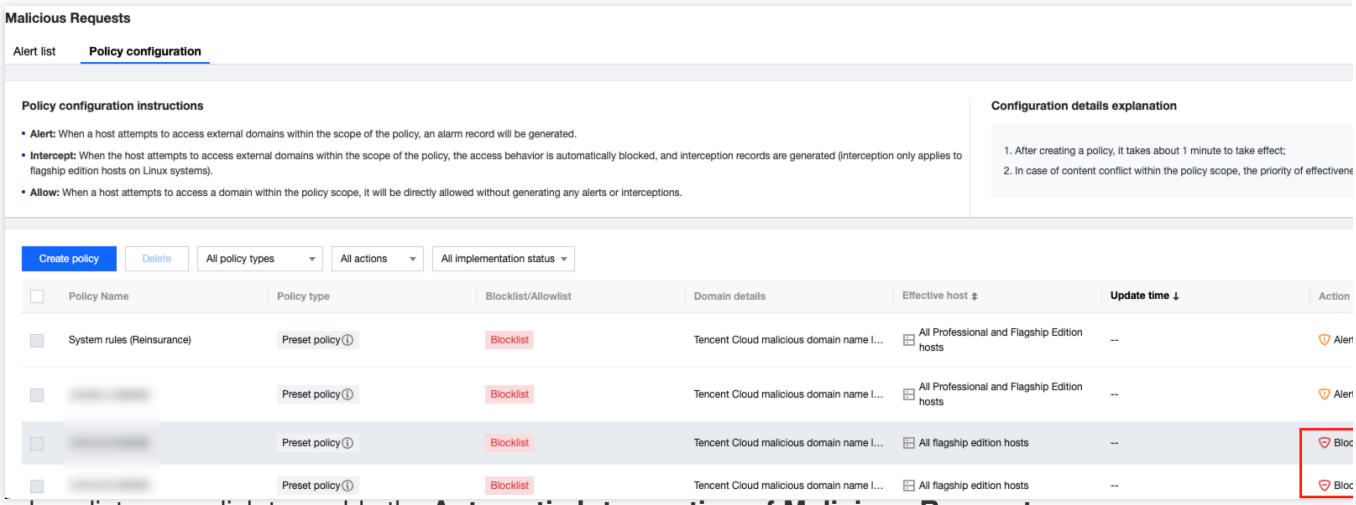
If you find any false interceptions, you can create a user-defined policy for allowlist processing or contact us.

System auto-interception rules are available only to **Ultimate Users**.

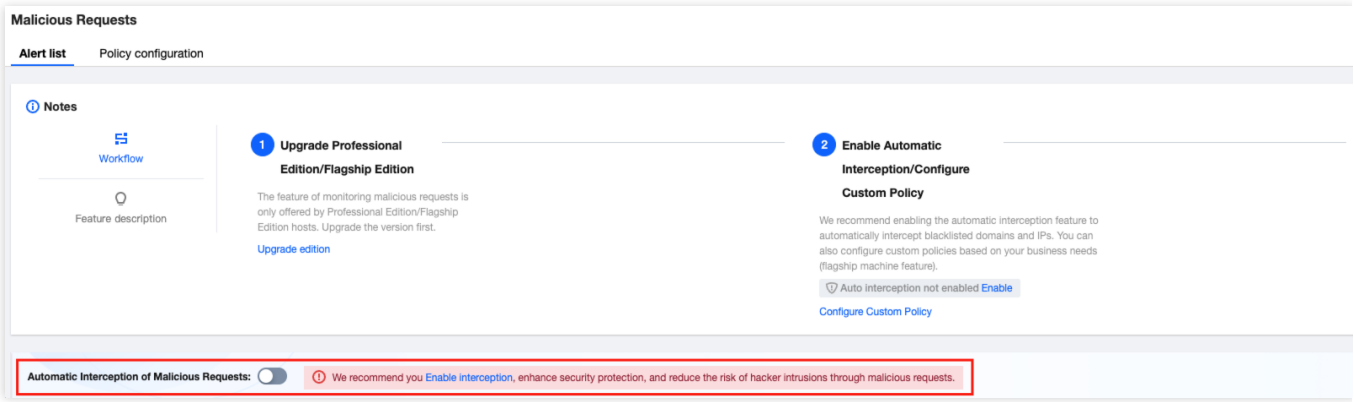
1. Log in to the CWPP console. In the left sidebar, choose **Intrusion Detection** > **Malicious Requests**.

2. On the malicious request page, the following two methods are supported to enable system automatic interception rules.

On the policy configuration page, click the **Implementation Switch** next to the system automatic interception rules policy.



On the alarm list page, click to enable the **Automatic Interception of Malicious Requests**.



High-risk Commands

Last updated：2024-08-13 16:29:50

This document will introduce how to view and operate the alarm list of high risk commands.

Overview

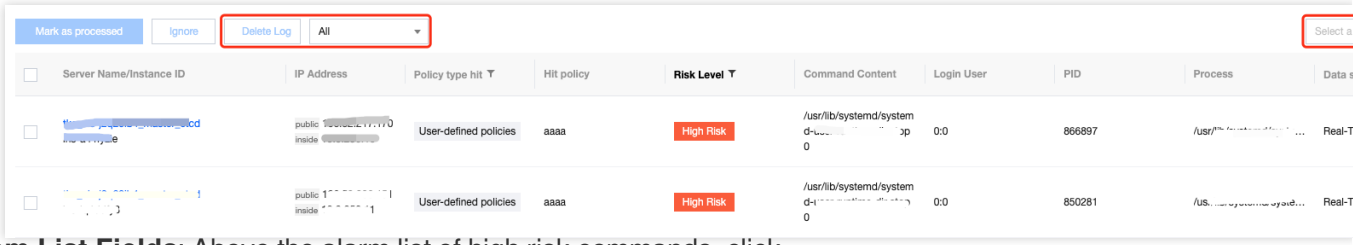
Based on Tencent Cloud's security technologies and multidimensional approaches, CWPP can monitor commands in the system in real time. If a high risk command is detected, the system will provide you with real-time alarm notifications. Additionally, you can configure policies to mark the risk level of threat commands and perform corresponding actions.

Prerequisites

High risk command feature is available only for hosts of Pro Edition and Ultimate Edition. Basic Edition and unprotected hosts need to upgrade to the Pro edition or Ultimate edition to use this feature.

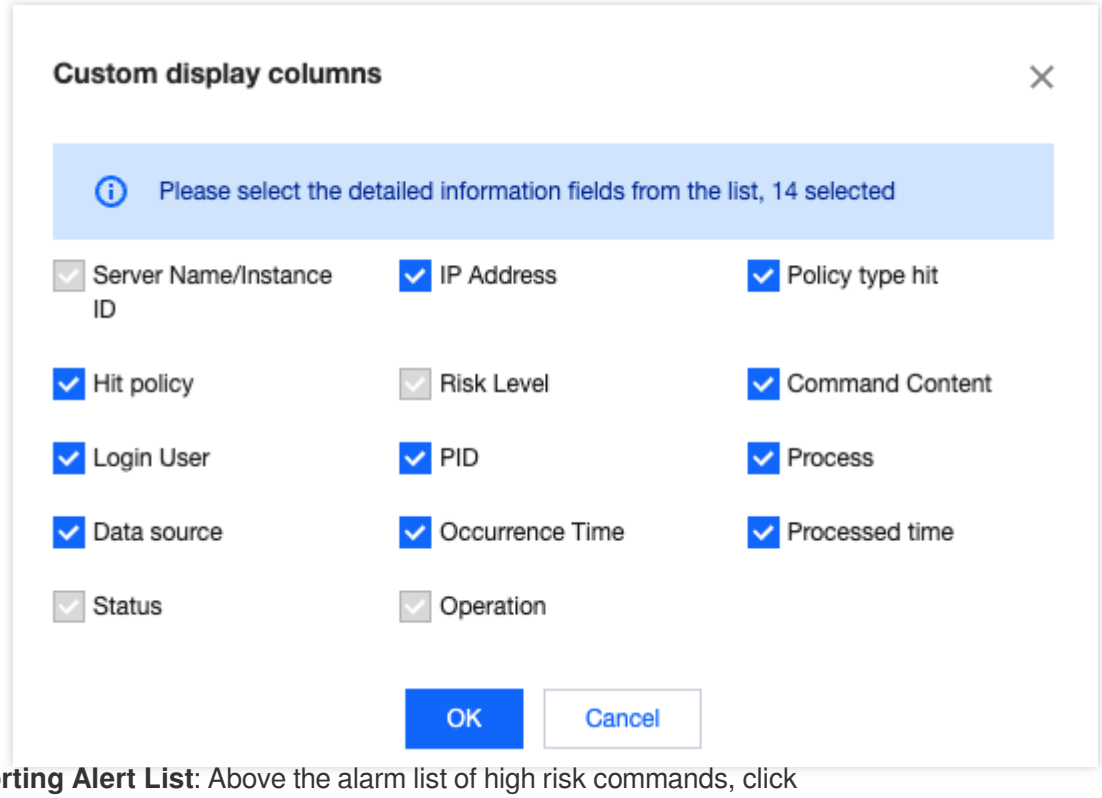
Alert List

1. Log in to the CWPP console. In the left sidebar, choose **Intrusion Detection** > **High Risk Commands** to enter the alarm list tab for high risk commands.
2. In the **Alert list** tab for high risk commands, you can view the alarm list of high risk commands and perform operations. The list interface displays 14 fields including server name/instance ID, IP address, policy type hit, hit policy, risk level, command content, log-in user, PID, process, data source, occurrence time, processed time, status, and operation. The displayed list fields can be user-defined.
Filtering: The event list of high risk commands supports choosing dates to view corresponding alarm information, and supports searching for events by keywords and tags (multiple keywords separated by a vertical bar (|), and multiple filter tags separated by hitting the Enter key). It also allows filtering alarm information by hit policy type, risk level, data source, and status.



Custom List Fields: Above the alarm list of high risk commands, click

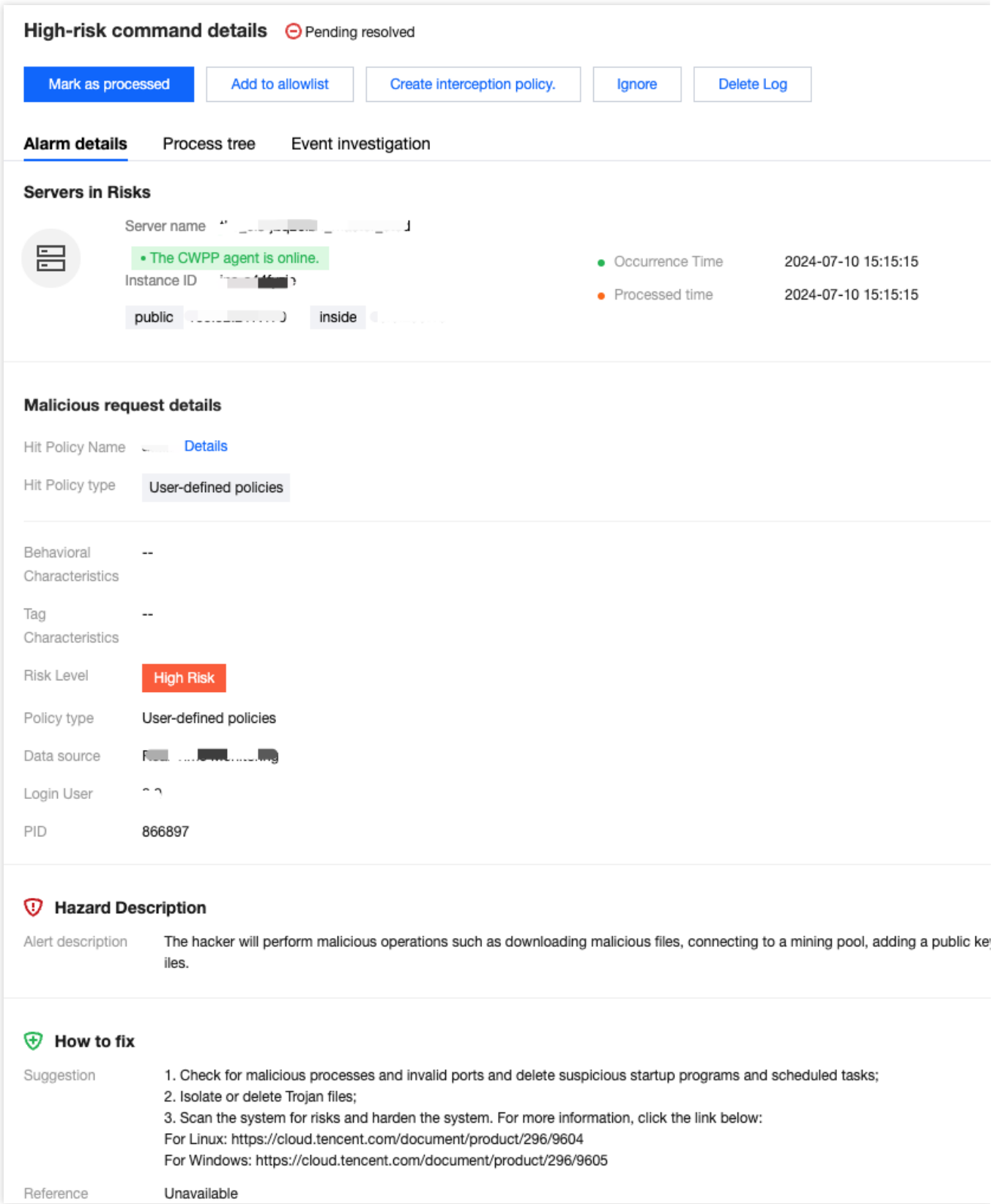
to set the fields displayed in the list. After selection, click **OK** to apply the settings.



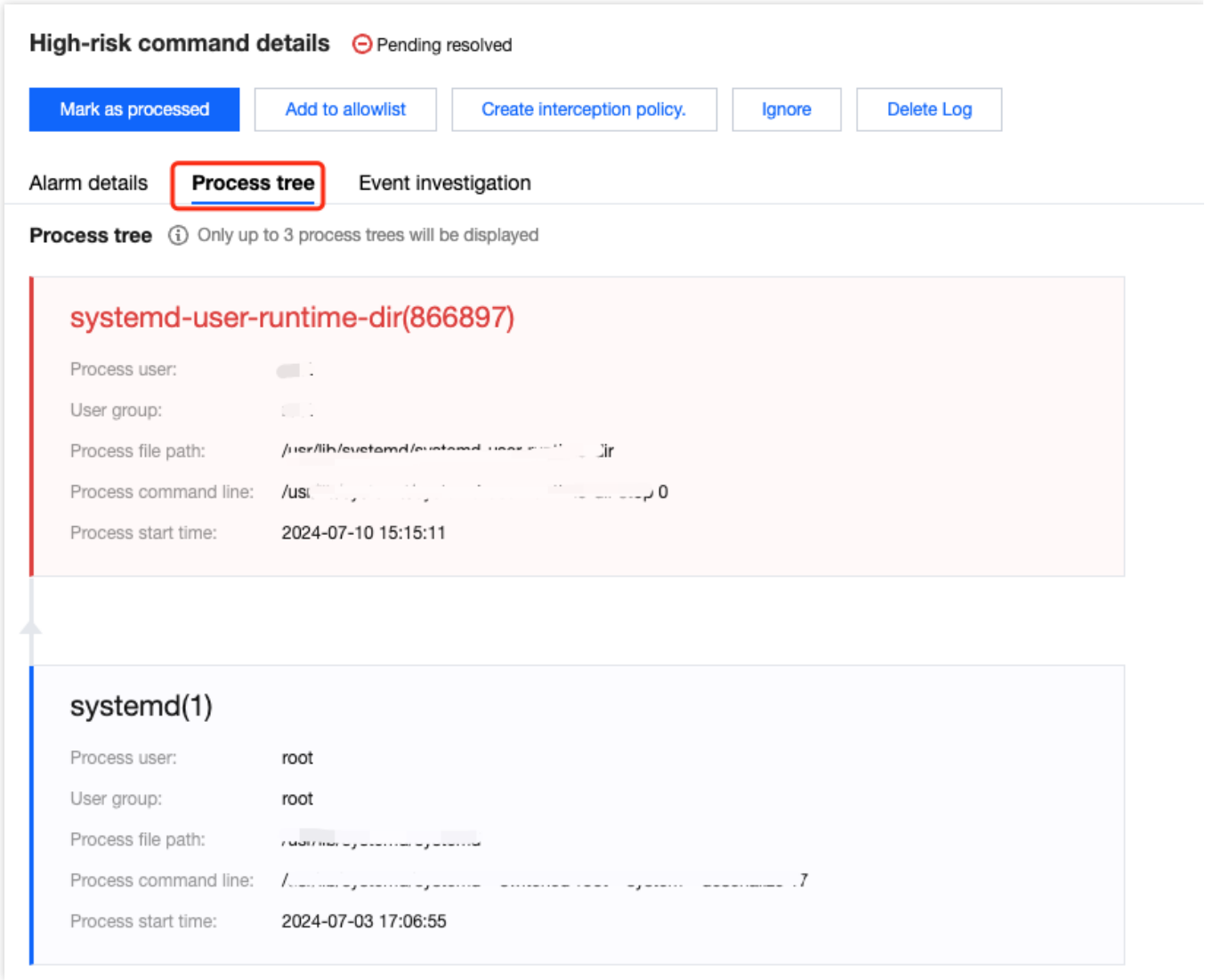
Exporting Alert List: Above the alarm list of high risk commands, click

to export the list information.

Details > **Alert details**: Click **Details** to view the alarm details page of high risk commands.



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



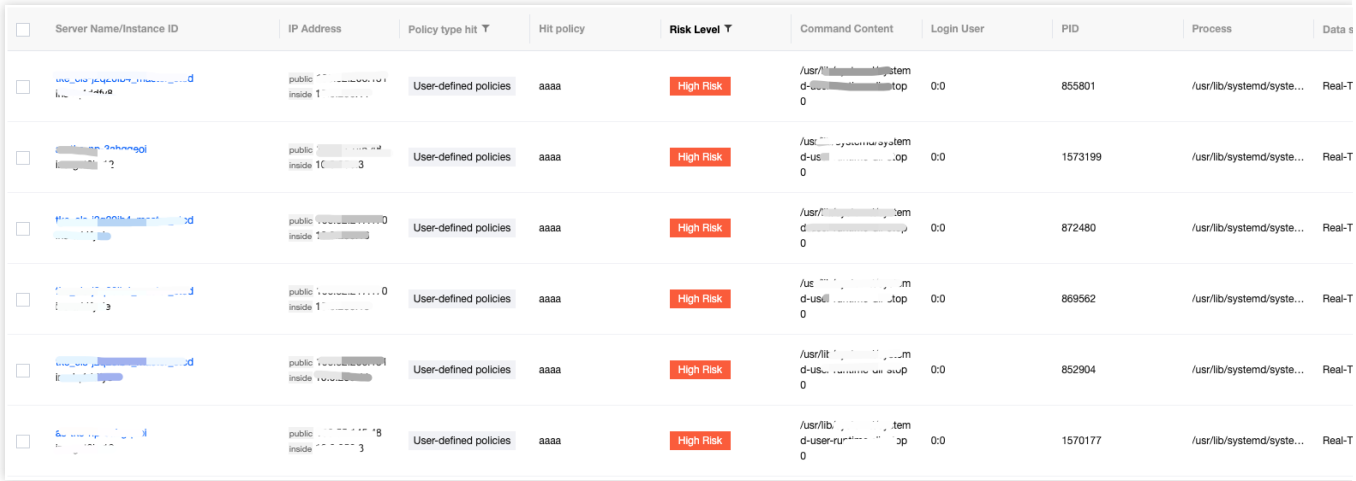
Details > **Event investigation**: In the right action bar of the alarm list of high risk commands, click **Details** to choose the **Event Investigation** tab to enter the corresponding host list for event investigation.

Note

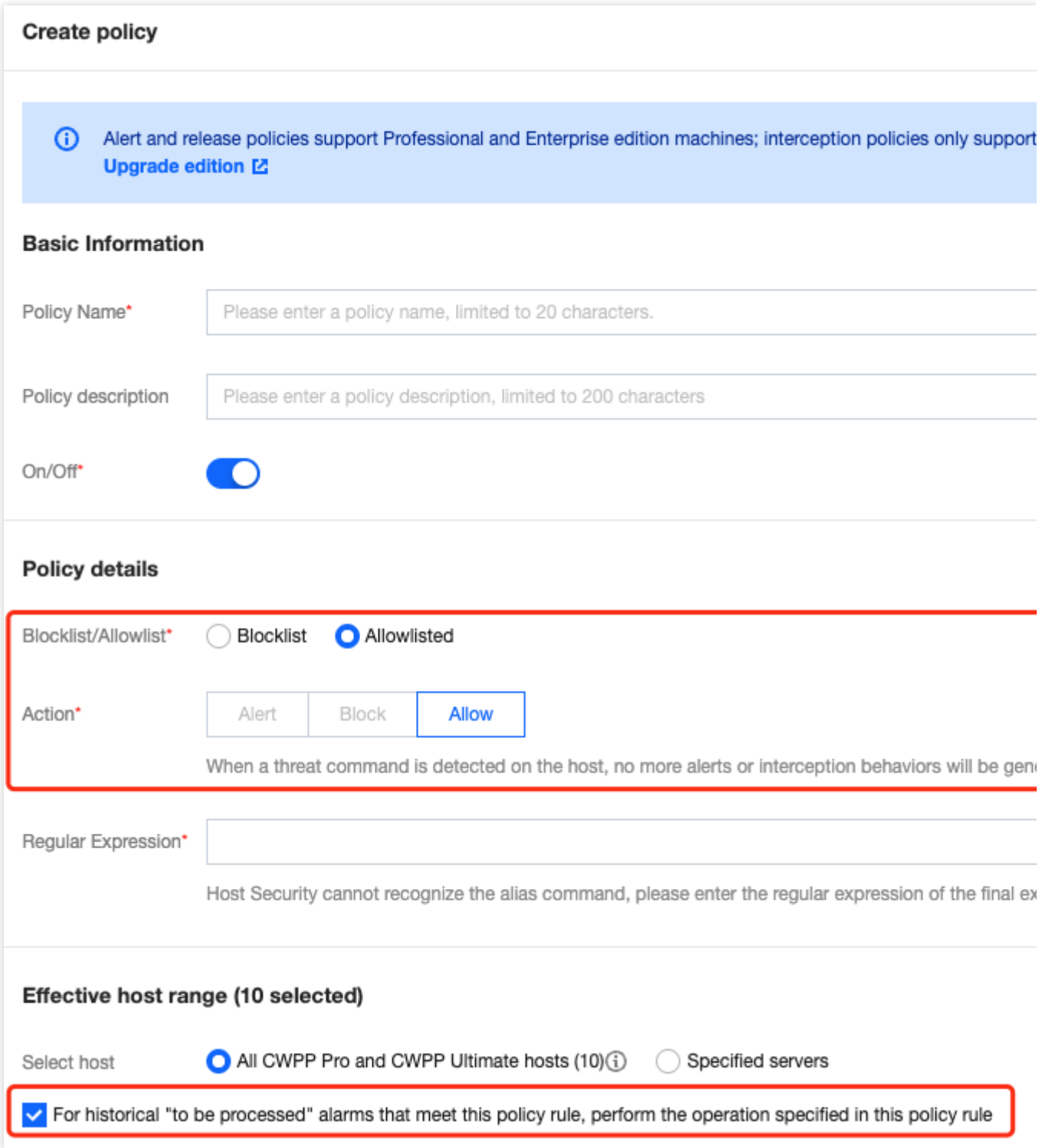
Windows machines do not support the event investigation feature.

Only the Ultimate Edition supports the event investigation feature.

Mark as Processed: Click **Process** > **Mark as processed**. If the user has manually handled the current high risk command alarm, they can mark this alarm as processed.



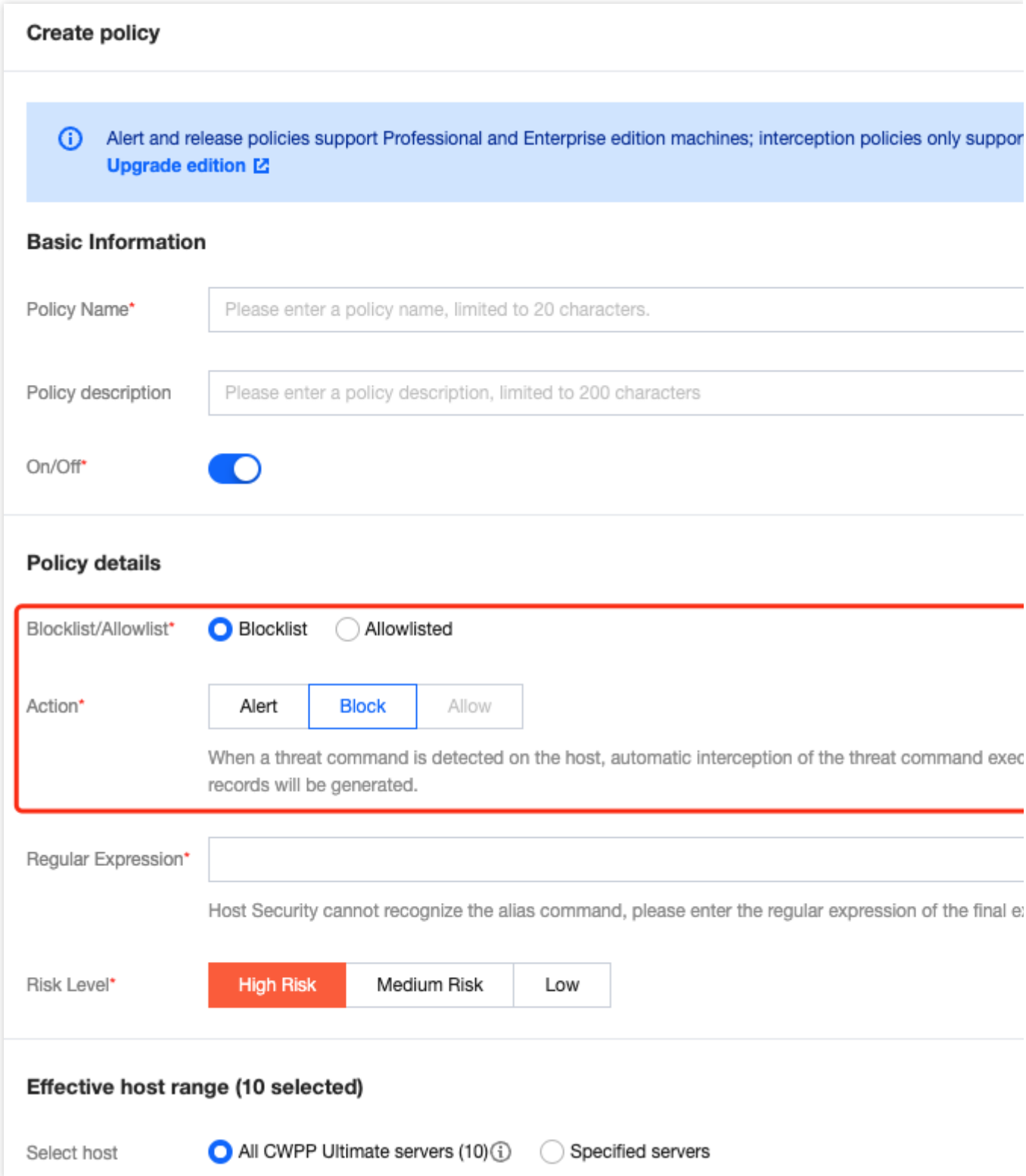
Add to allowlist: Click **Process** > **Add to allowlist** to add trusted commands to the allowlist, preventing future alarms or interceptions when the command is executed again.



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

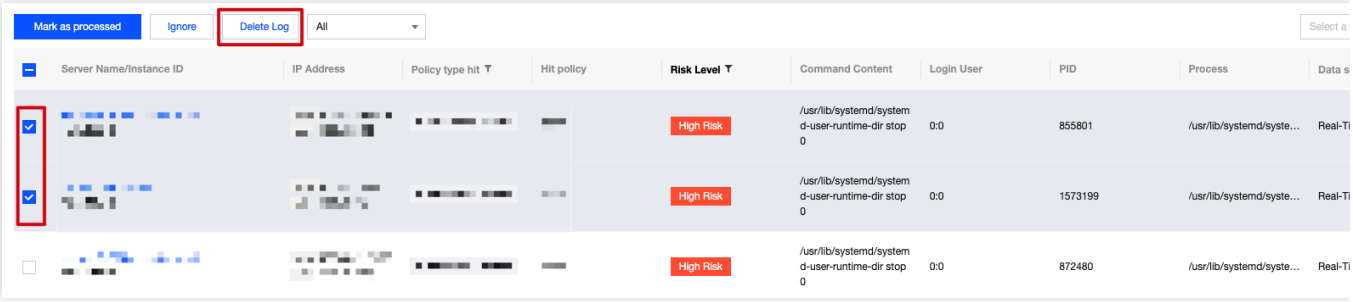
Note

Interception policy is supported only for hosts of Ultimate Edition. Basic and Pro Edition hosts need to upgrade to the Ultimate edition first.



Ignore: Supports single or multiple selections of high risk command alarm information. Only the selected alarms are ignored. If the same issue occurs again, alarms will still be triggered.

Delete Log: Supports single or multiple selections of high risk command alarm information. The selected alarm records are deleted.



Policy Configuration

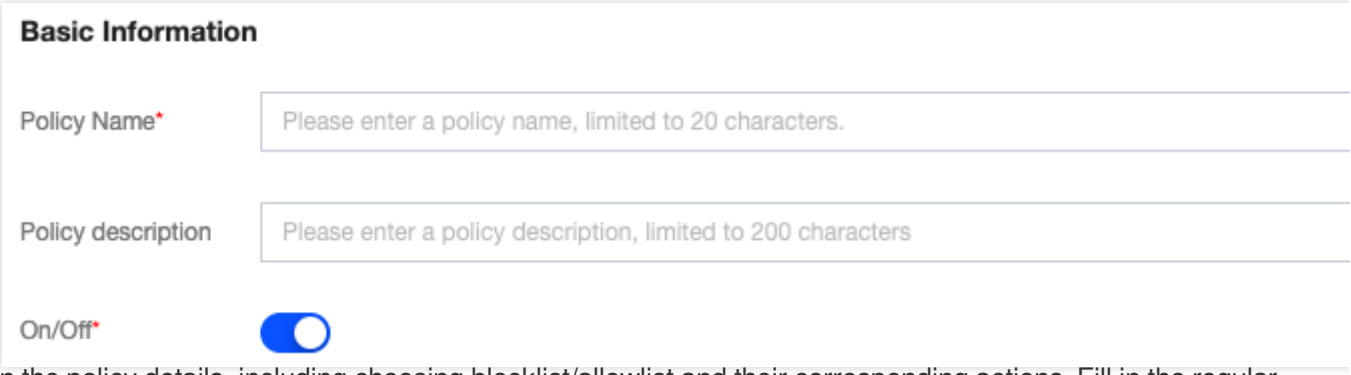
Create a Custom Policy

The high risk command feature supports creating a custom policy. Set the policy to handle threat commands accordingly.

1. Log in to the CWPP console. In the left sidebar, choose **Intrusion Detection** > **High Risk Commands** 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.



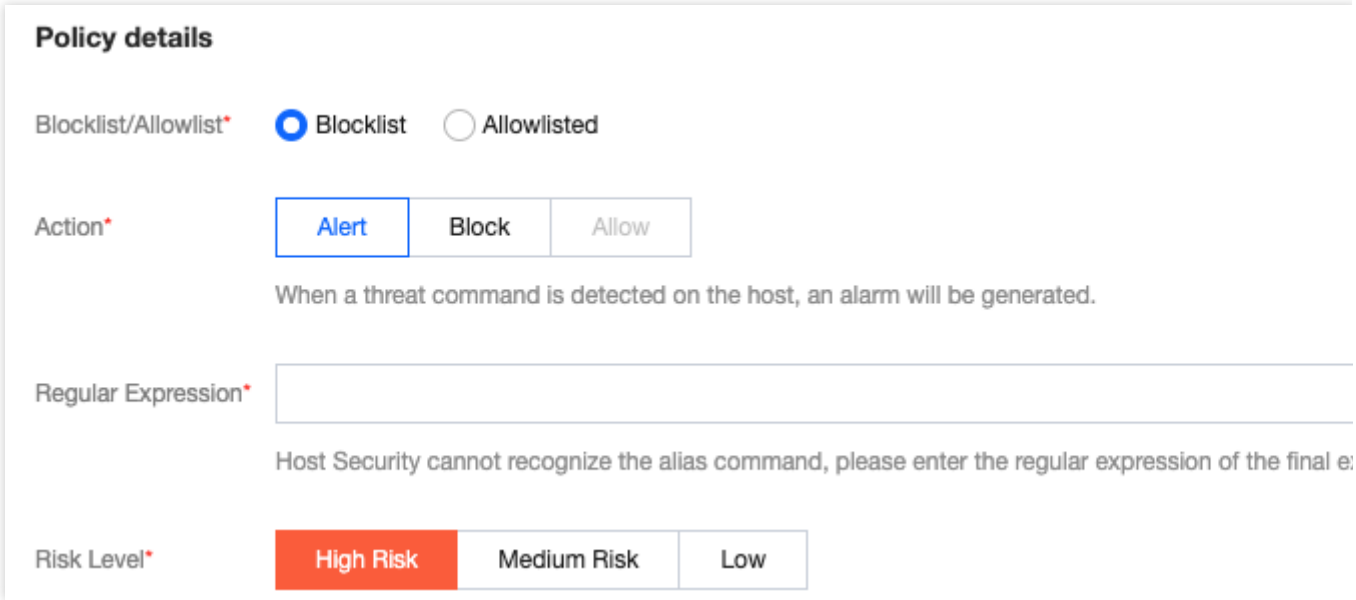
4. Fill in the policy details, including choosing blocklist/allowlist and their corresponding actions. Fill in the regular expression, select risk level, and select the effective host range.

The blocklist rule means that an alarm notification will be generated when a threat command is found on the host.

Note

Interception policy refers to automatically intercepting and sending alarms when a threat command is found on the host.

Interception policy is supported only for Ultimate Edition machines. Basic and Pro Edition hosts need to upgrade to the Ultimate edition to use this feature.

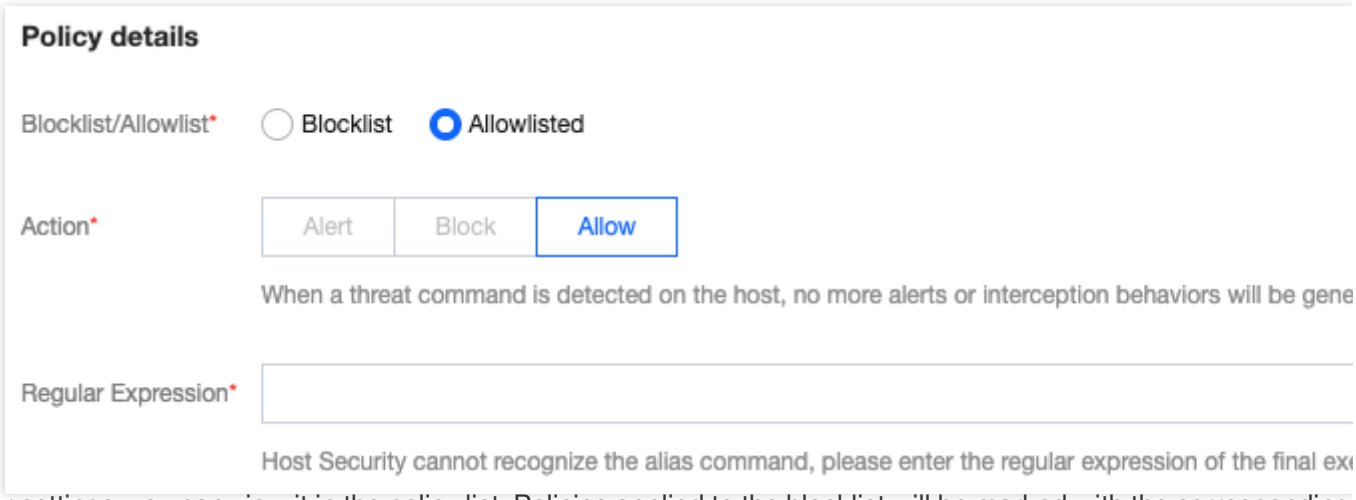


The allowlist rule means allowing threat commands without generating alarms or interception actions.

Note

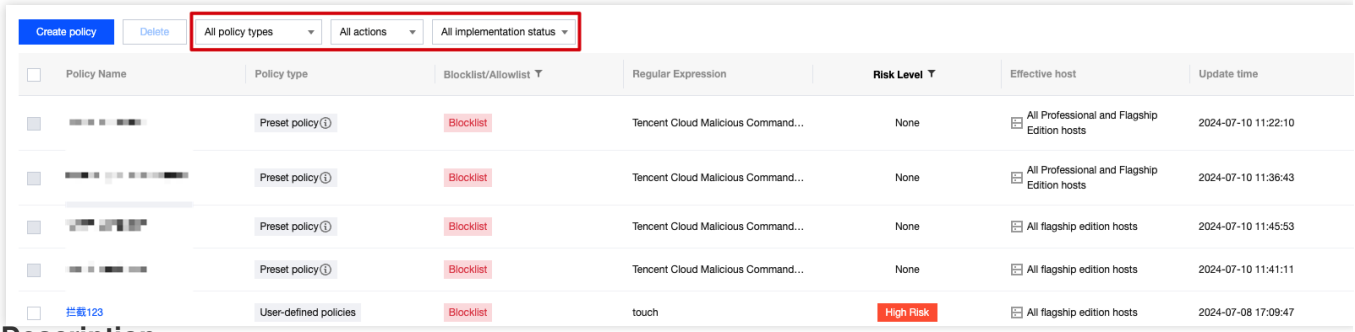
If all Pro Edition and Ultimate Edition hosts are selected for the effective host range, newly added Pro/Ultimate Edition hosts will be automatically included in the policy's effective range.

You can check to apply this policy rule's actions to historical Pending alarms that match this policy rule.



5. After settings, you can view it in the policy list. Policies applied to the blocklist will be marked with the corresponding threat level.

6. You can filter, edit, and delete policies in the policy list.



Field Description:

Filtering: Configured policies support searching by keywords and tags (multiple keywords separated by a vertical bar (|), and multiple filter tags separated by hitting the Enter key). They can also be filtered by risk level (all/high-risk/medium-risk/low-risk/none), by executed action (alarm/block/allow), and by effective status (effective/ineffective).

Custom List Fields: At the top of the policy list, click

to set display fields in the list. After selection, click **Confirm** to complete the settings.

Enable status: The list supports setting the enable status of policies. In the enable status column, click **Enable Switch** to decide whether to enable the policy.

Edit: In the action bar on the right side of the policy list, click **Edit** to edit the created policies.

Delete: In the policy list, configured policies can be deleted.

System Policies

The high risk command feature now includes system automatic interception rules. Once enabled, the system automatically intercepts detected high risk system commands. However, some configurations still require your manual policy settings.

High Risk System Commands: High risk system commands are refined by CWPP operation experts and algorithm experts. The commands in this list can be used for auto-interception.

Interception Principle Description: The automatic interception of high risk commands is performed as the process of detecting and killing hit rules. For example, if process A attempts to create a /bin/bash -i process (assuming bash -i is on the blocklist), then the attempted creation of the /bin/bash process will be terminated (or fail to create), while process A itself will not be affected.

Note:

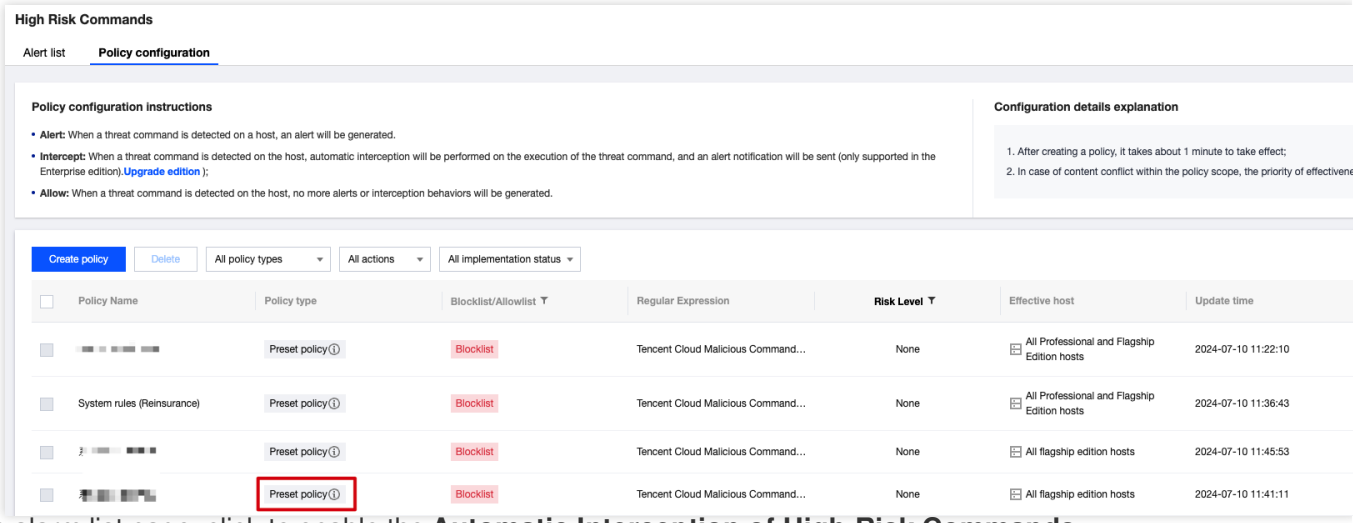
If you find a false interception, you can create a custom policy for allowlist processing or contact us.

System auto-interception rules are available only to **Ultimate Users**.

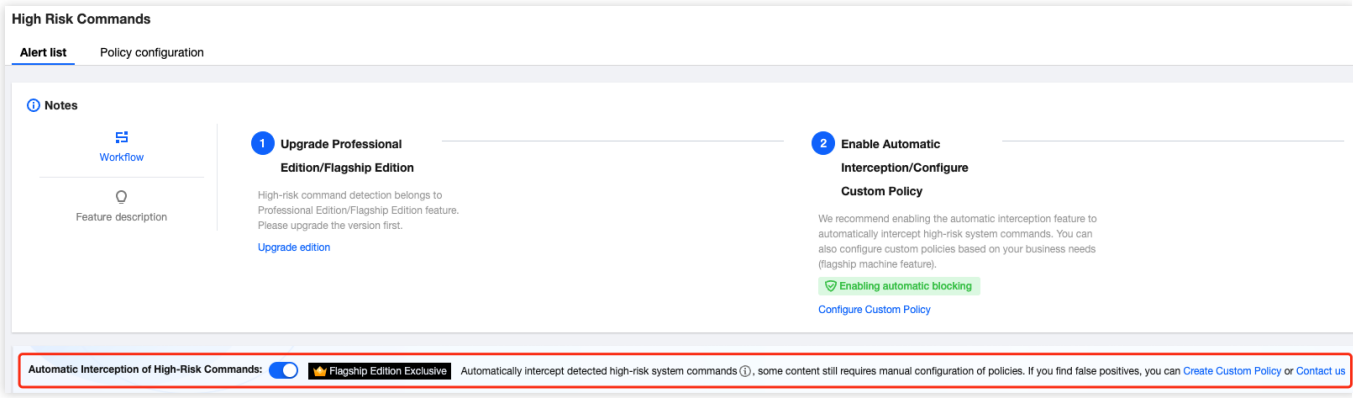
1. Log in to the CWPP console. In the left sidebar, choose **Intrusion Detection** > **High Risk Commands**.

2. On the high risk commands page, the following two methods are supported to enable the system's automatic interception rules.

On the policy configuration page, click the **Implementation Switch** next to the system automatic interception rules policy.



On the alarm list page, click to enable the **Automatic Interception of High-Risk Commands**.



Local Privilege Escalation

Last updated：2024-08-13 16:29:50

This document will introduce how to view and process privilege escalation event details. It also instructs you on how to create an allowlist for setting permitted privilege escalation behaviors.

Overview

If an event occurs where entry into the system is gained with low privileges which subsequently escalated to higher privileges through certain means, it is highly likely to be an act of hacking, posing a threat to the security of hosts. The local privilege escalation feature can monitor in real-time privilege escalation events on your CVMs, and allow you to view the event details, process the events, and create the allowlist of permitted privilege escalation events.

Prerequisites

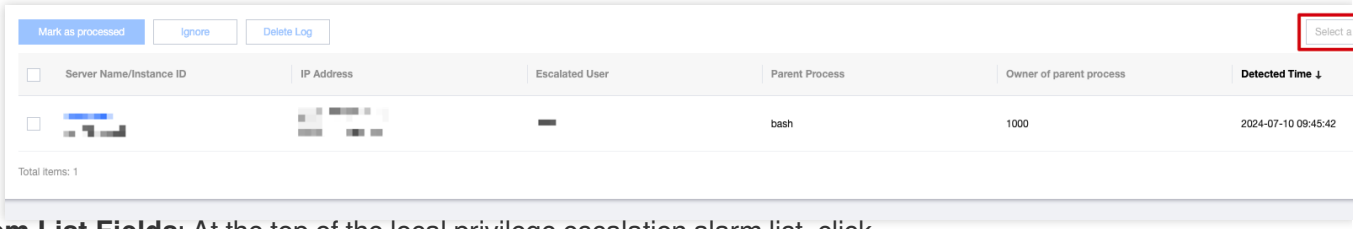
Local privilege escalation supports only the Pro Edition and Ultimate Edition hosts. Basic and unprotected hosts must upgrade to Pro edition or Ultimate edition to use this feature.

Directions

Alert List

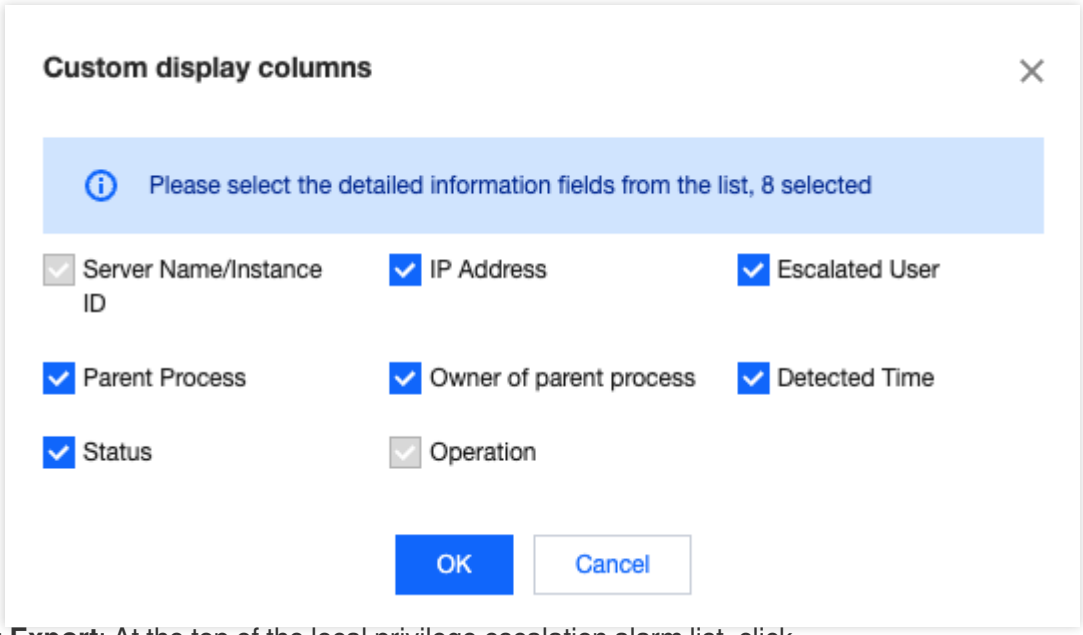
1. Log in to the CWPP console. In the left sidebar, choose **Intrusion Detection** > **Local Privilege Escalation** to enter the local privilege escalation **Alert list** tab page.
2. On the local privilege escalation **Alert list** tab page, you can view the list of alarm events of local privilege escalation and perform related operations. The list includes eight fields: Server Name/Instance ID, IP Address, Escalated User, Parent Process, Owner of Parent Process, Detected Time, Status, and Operation (Details | Process). The details displayed in the list can be user-defined.

Filter/Query: The local privilege escalation alarm list supports choosing dates to view corresponding alarm information. It also supports searching events by keywords and tags (multiple keywords separated by a vertical bar (|), and multiple filter tags separated by hitting the Enter key). Additionally, you can filter events by status.



Custom List Fields: At the top of the local privilege escalation alarm list, click

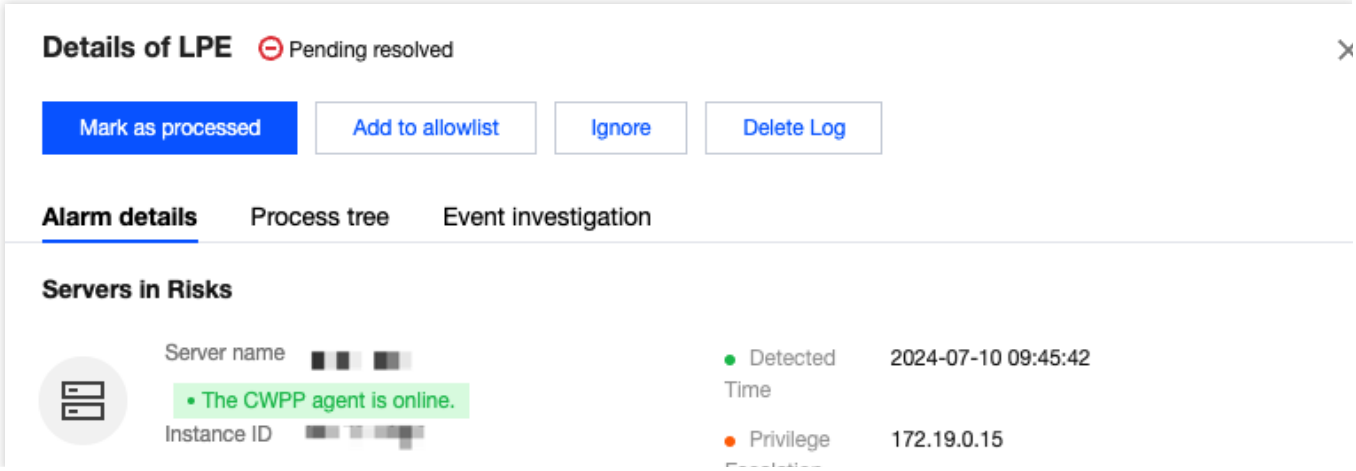
to set the columns to display in the list. After making your choices, click **OK** to save your settings.

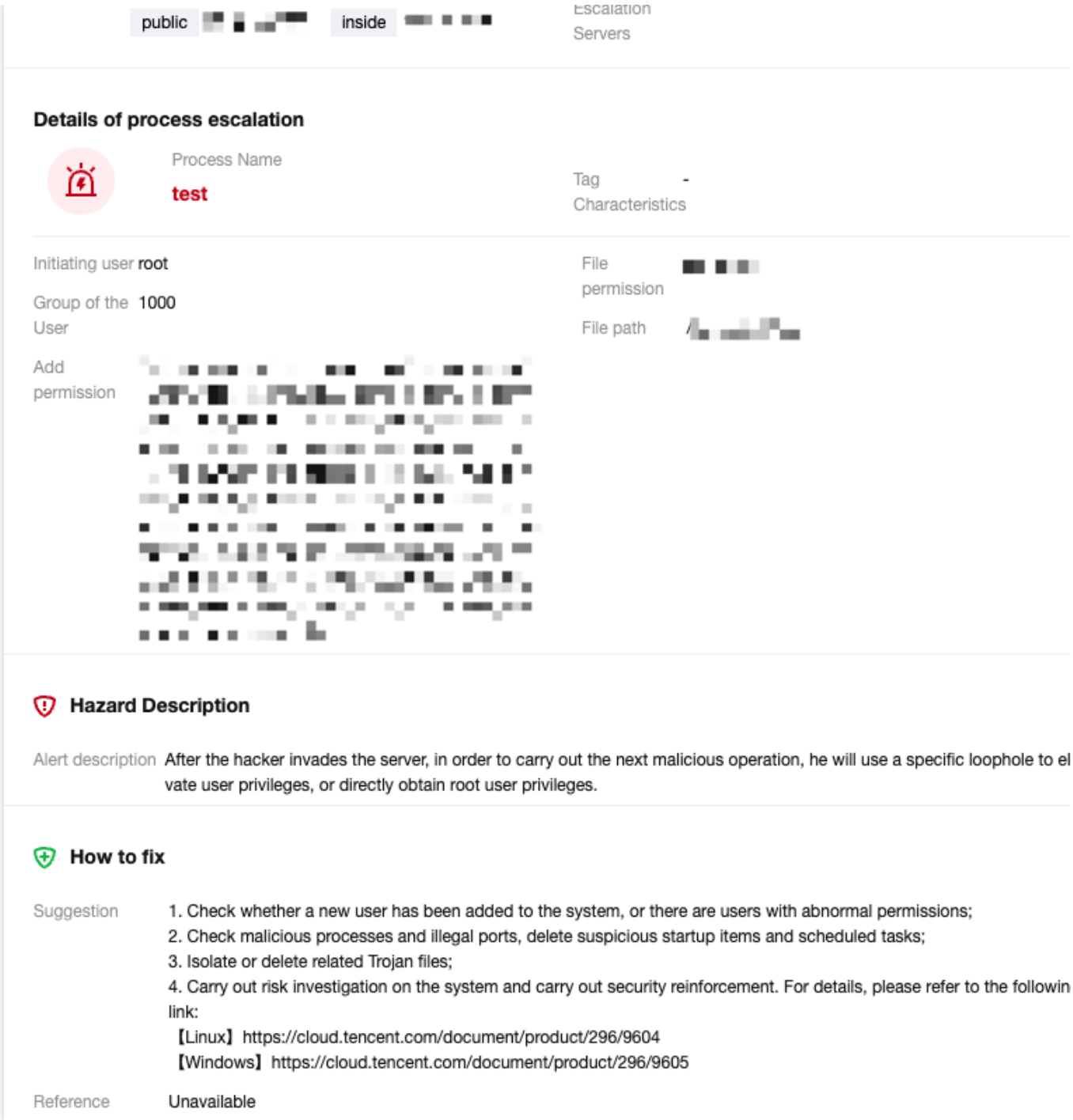


Event Export: At the top of the local privilege escalation alarm list, click

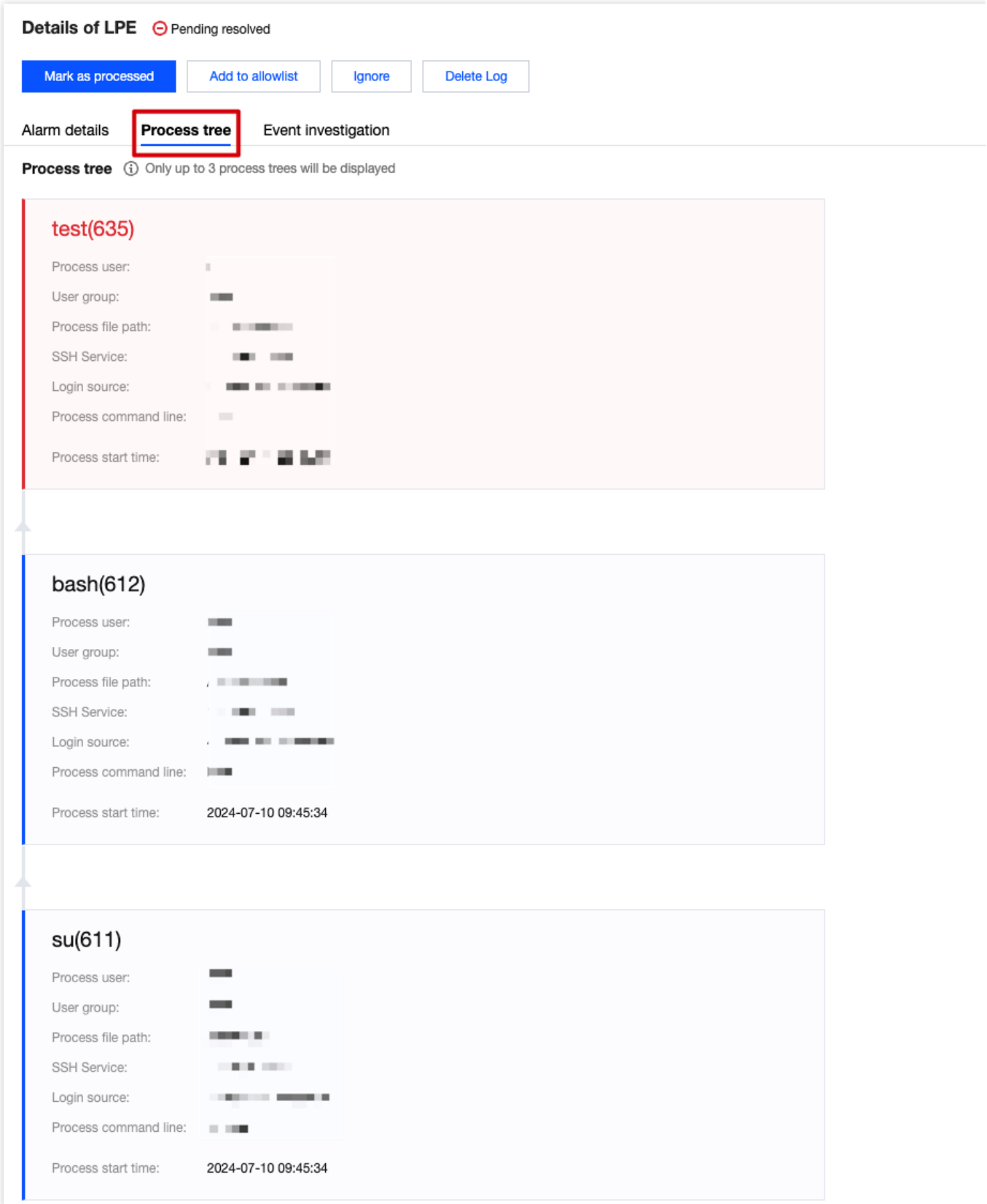
to export the list.

Details > **Alert details**: In the right action bar of the local privilege escalation alarm list, click **Details** and choose the **Alert details** tab to view the alarm details.





Details > **Process tree**: In the right action bar of the local privilege escalation alarm list, click **Details** and choose the **Process tree** tab to view details of the three most recent processes in reverse chronological order.



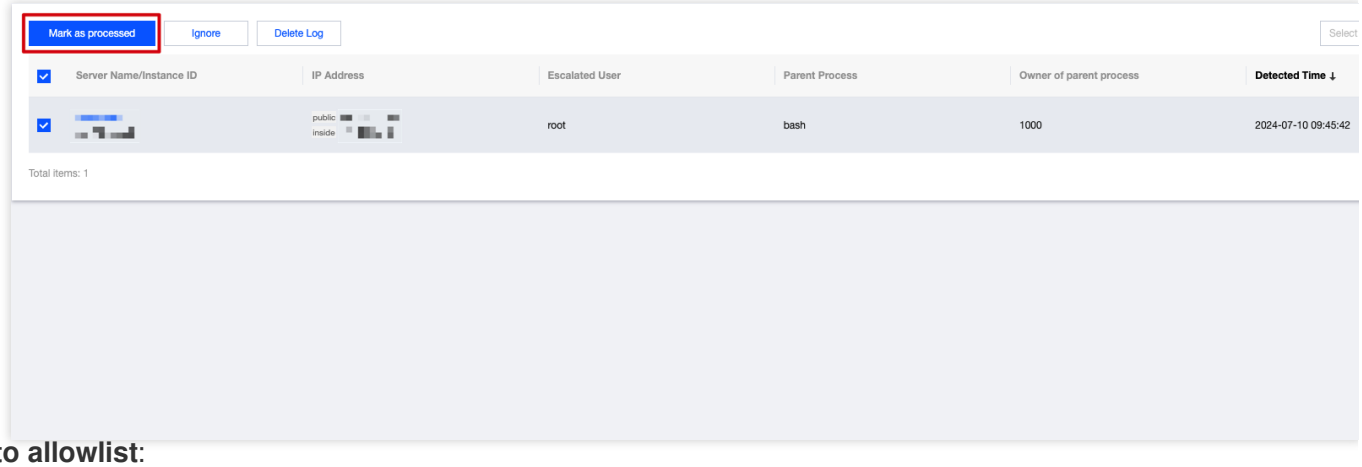
Details > **Event investigation**: In the right action bar of the local privilege escalation alarm list, click **Details** and choose the **Event Investigation** tab to enter the event investigation of the corresponding host list.

Note

Windows machines do not support the event investigation feature.

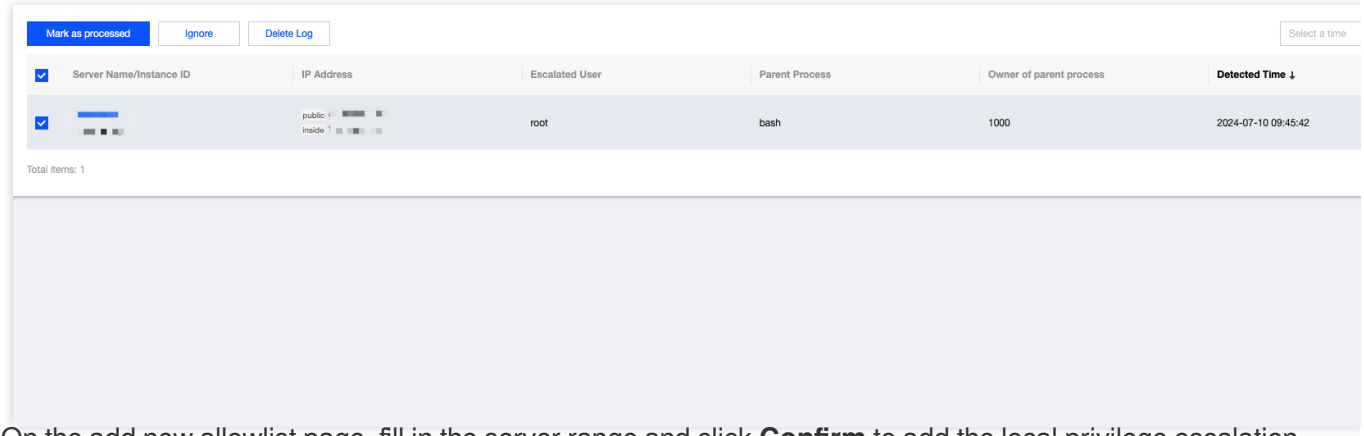
Only the Ultimate Edition supports the event investigation feature.

Marked as processed: Supports single or multiple selections of local privilege escalation alarm information. After the alarm is manually processed, it can be marked as processed.

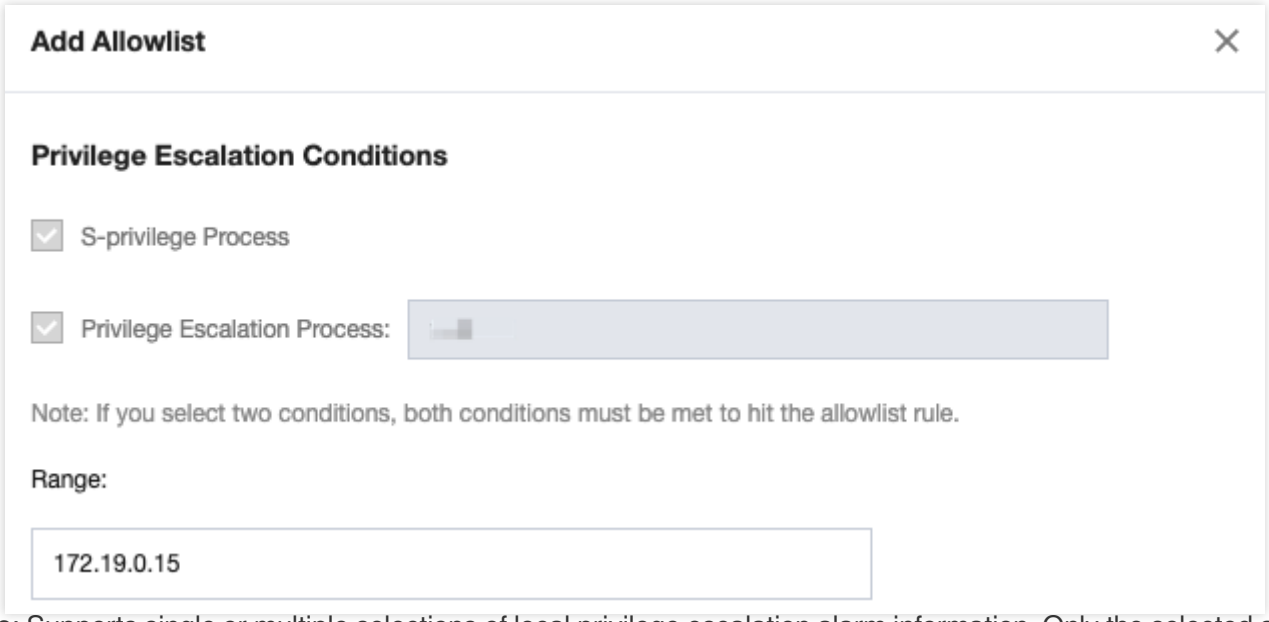


Add to allowlist:

2.1.1 To add a local privilege escalation alarm event to the allowlist, you can click **Process** > **Add to allowlist** in the right action bar of the alarm information list, or click **Add to allowlist** on the details page.

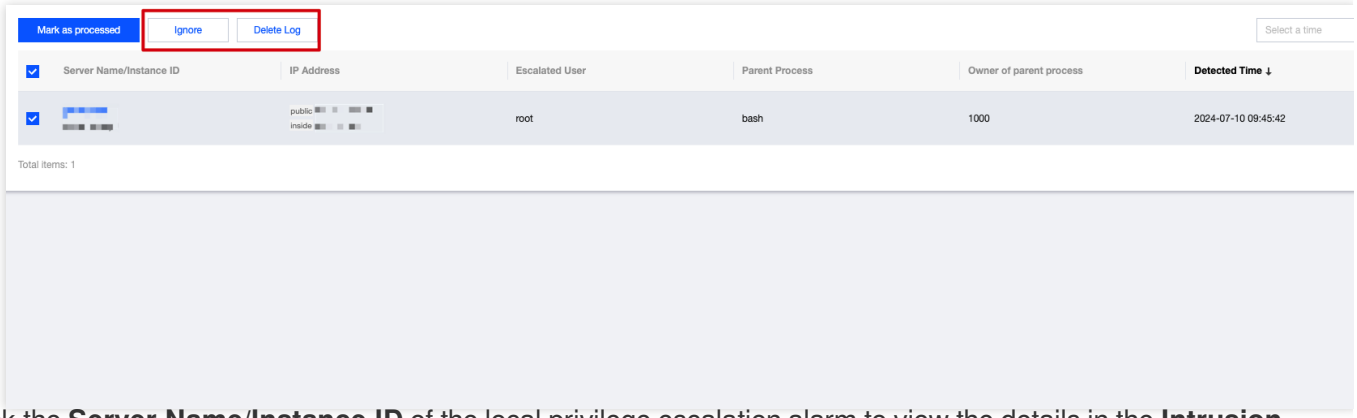


2.1.2 On the add new allowlist page, fill in the server range and click **Confirm** to add the local privilege escalation alarm to the allowlist.

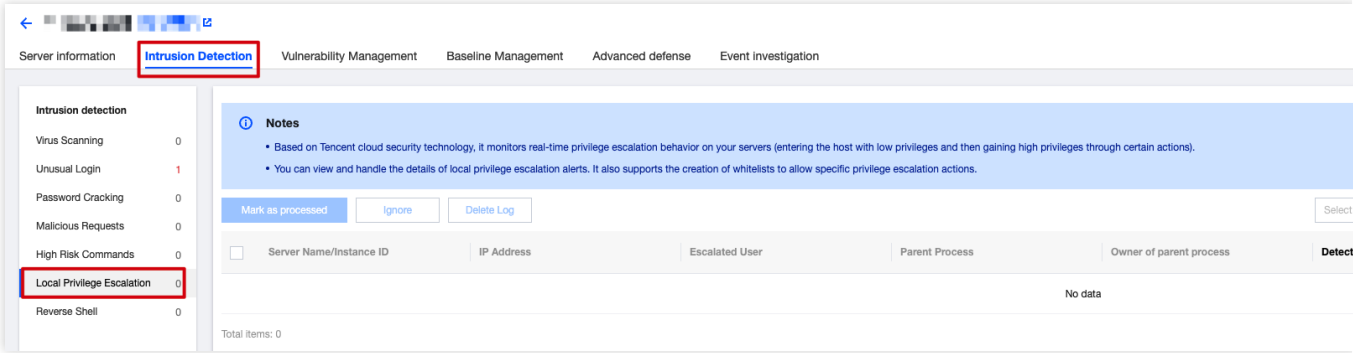


Ignore: Supports single or multiple selections of local privilege escalation alarm information. Only the selected alarms will be ignored. If the same situation occurs again, an alarm will still be triggered.

Delete Log (Proceed with Caution) : Supports single or multiple selections of local privilege escalation alarm information. If you delete the selected alarm records, they will no longer be displayed on the console and cannot be recovered.



3. Click the **Server Name/Instance ID** of the local privilege escalation alarm to view the details in the **Intrusion Detection** tab of the host list.



Allowlist Management

The local privilege escalation feature supports adding to the allowlist. If you set the allowlist conditions for privilege escalation, events that meet the conditions will be added to the allowlist.

1. Log in to the CWPP console. In the left sidebar, choose **Intrusion Detection** > **Local Privilege Escalation**.

2. On the **Local Privilege Escalation** page, click **Allowlist Policies** > **Add Allowlist**.

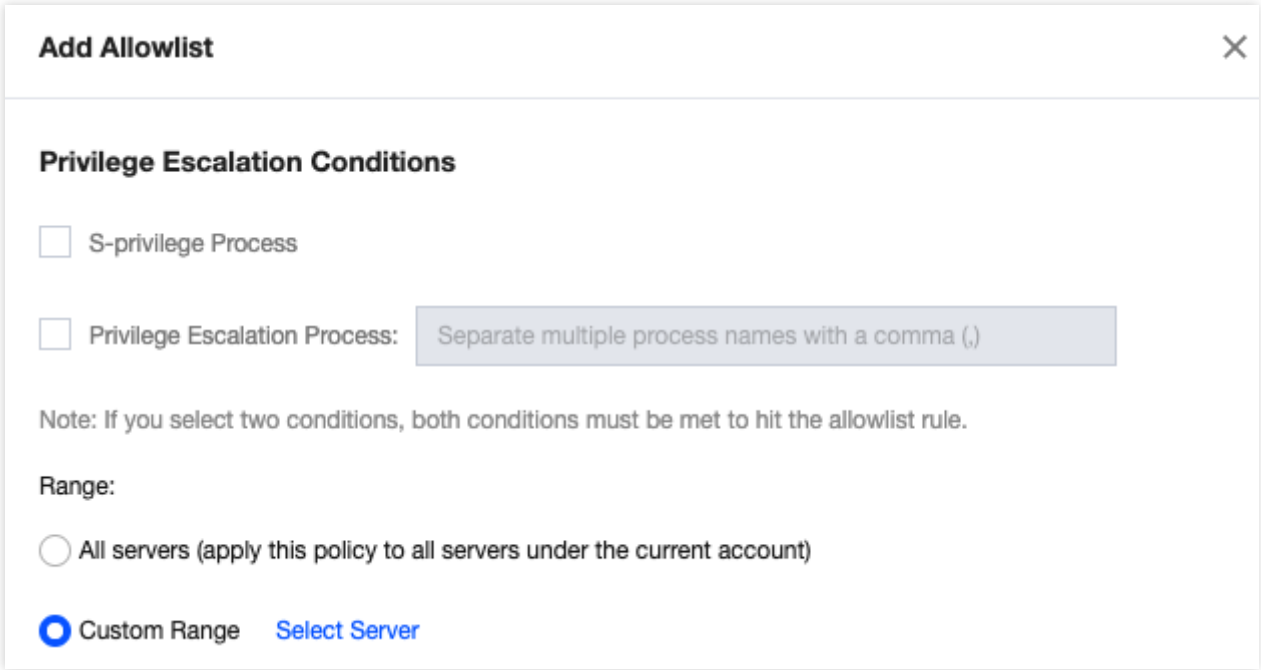
3. On the add allowlist page, set the privilege escalation conditions, including: S-privilege process, custom privilege escalation process (supporting multiple process names, separated by commas, e.g., 123.exe,test.exe), and also select the server range covered by the conditions. Click **OK**.

Caution

S-privilege: Set the file to have the privileges of the file owner during the execution, which is equivalent to temporarily assuming the identity of the file owner.

When both conditions are checked, both must be met to hit the allowlist.

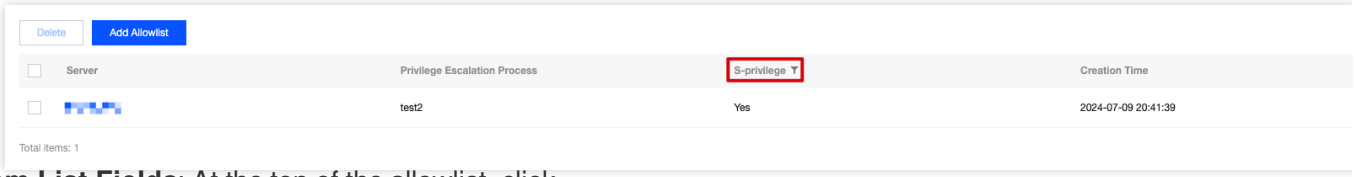
If the server range is set to all servers, this allowlist condition will be trusted for all servers under the user's APPID. Proceed with caution.



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

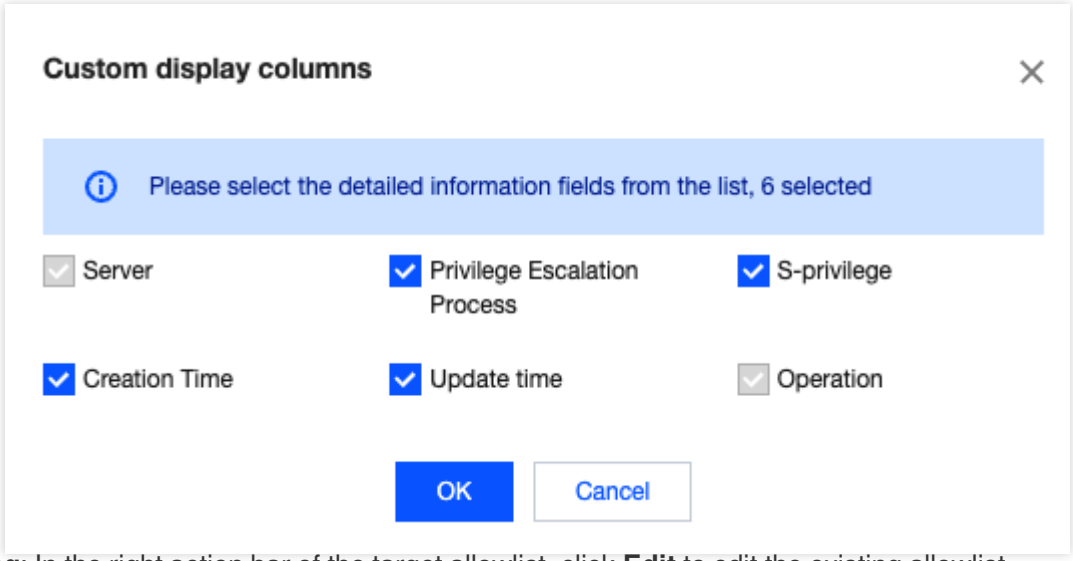
5. On the allowlist management page, you can filter and delete the allowlist.

Filtering: Configured allowlists support searching by keywords and tags (multiple keywords separated by a vertical bar (|), and multiple filter tags separated by hitting the Enter key). Filtering by S-privilege is also supported.



Custom List Fields: At the top of the allowlist, click

to set the columns to display in the list. After your selections, click **OK** to save your settings.



Editing: In the right action bar of the target allowlist, click **Edit** to edit the existing allowlist.

Delete: In the allowlist, you can select one or multiple configured allowlists for deletion.

Reverse Shell

Last updated：2024-08-13 16:29:50

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

Overview

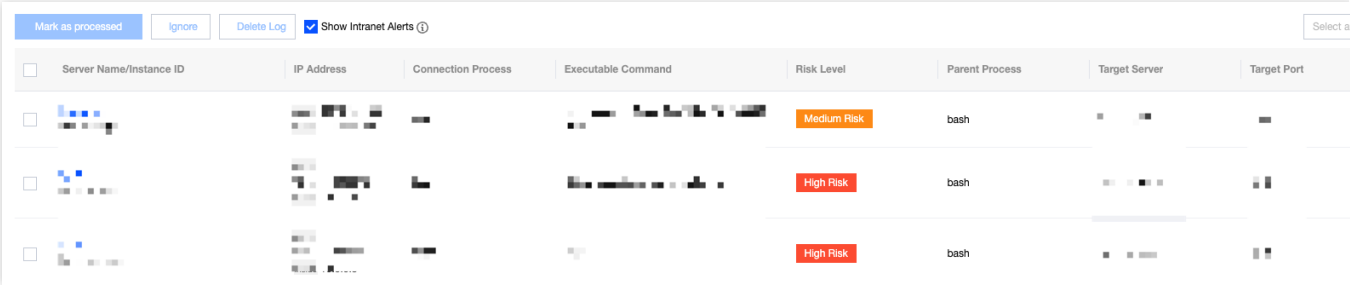
The reverse shell feature is powered by Tencent Cloud's advanced security technologies and multidimensional approaches, enabling the identification and recording of reverse shell connections on the servers and providing real-time monitoring capabilities for reverse shell behaviors on your CVMs.

Prerequisites

The reverse shell feature is only supported by hosts of Pro or Ultimate Edition. Basic Edition hosts need to upgrade to Pro edition or Ultimate edition to use this feature.

Alert List

1. Log in to the CWPP console. In the left sidebar, choose **Intrusion Detection** > **Reverse Shell** to enter the alarm list page of the reverse shell.
2. On the alarm list page, you can view the alarm events of the reverse shell and perform related operations.



Filter: Supports filtering by detected time, status, and keywords.
Custom display columns: Click

to set the fields displayed in the alarm list.
Export: Click

 to export detailed information from the alarm list.

Field Description:

Server Name/Instance ID: The host name/instance ID controlled by the attacker's reverse shell.

IP Address: The host IP controlled by the attacker's reverse shell.

Connection Process: Processes on the host that establish reverse shell connections.

Executable Command: Commands executed by the host for reverse shell connections.

Risk Level: High-risk (target host IP is a public IP), and medium-risk (target host IP is a LAN IP).

Parent Process: The parent process of the connecting process.

Target Server: The target host of the reverse shell connection.

Target Port: The target port of the reverse shell connection.

Detected Time: The time at which the reverse shell behavior was detected.

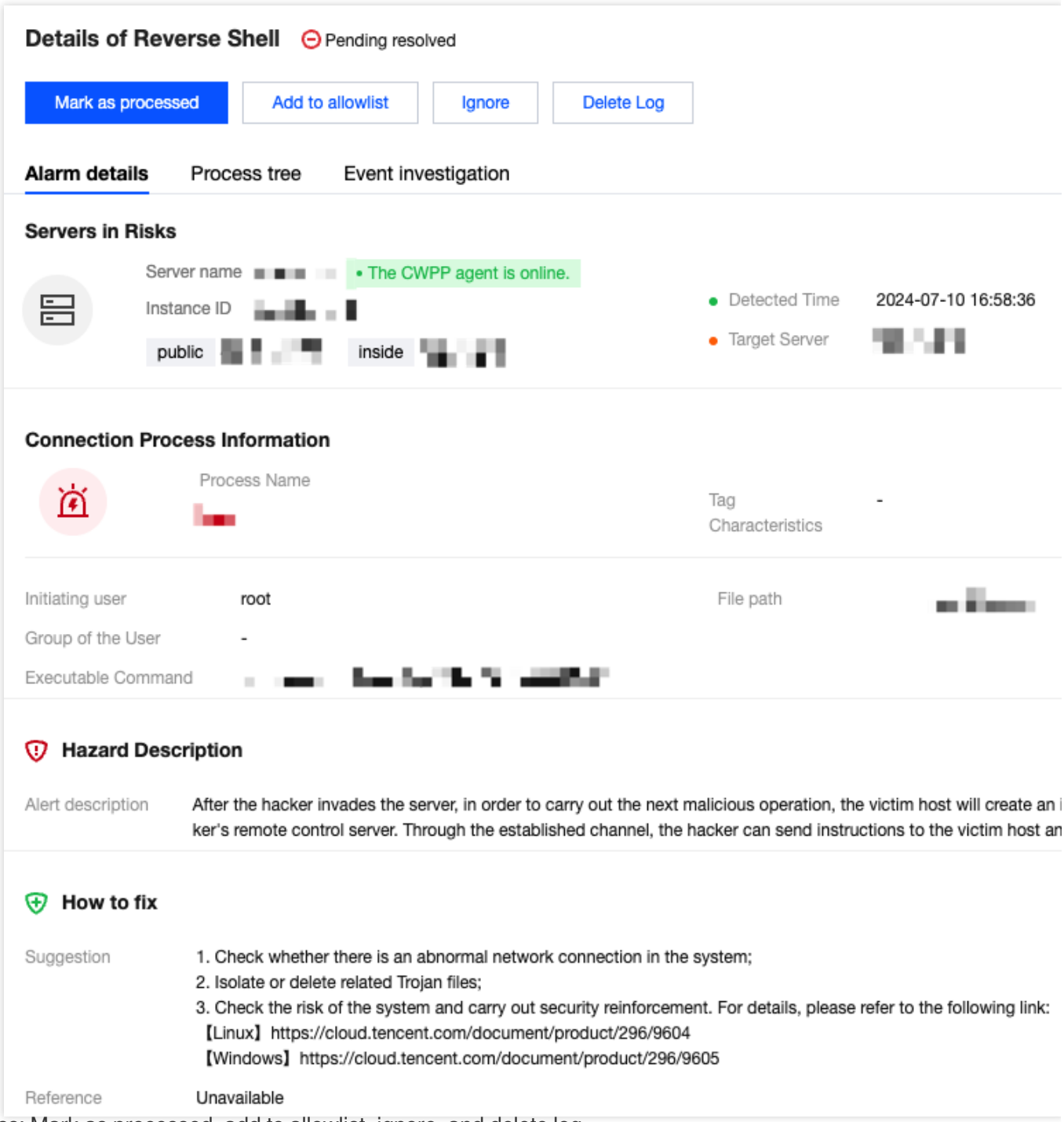
Check Method:

Behavior analysis: Detect potential threats or abnormal behaviors through monitoring systems and network activities.

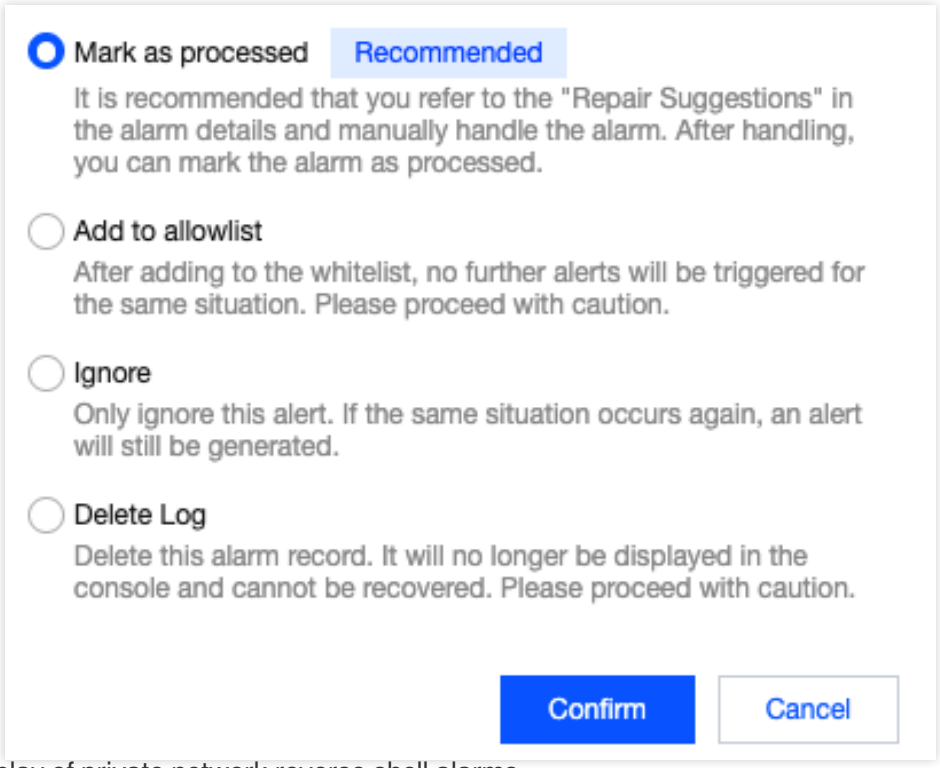
Command feature detection: Identify and monitor command behaviors that may be related to reverse shells by analyzing commands (e.g., high-privilege commands, unconventional commands, and anomalous parameters).

Status: Pending, allowlisted, processed, and ignored.

Details: View detailed information about the reverse shell, including risk host information, connection process information, danger description, and fix suggestions.



Process: Mark as processed, add to allowlist, ignore, and delete log.

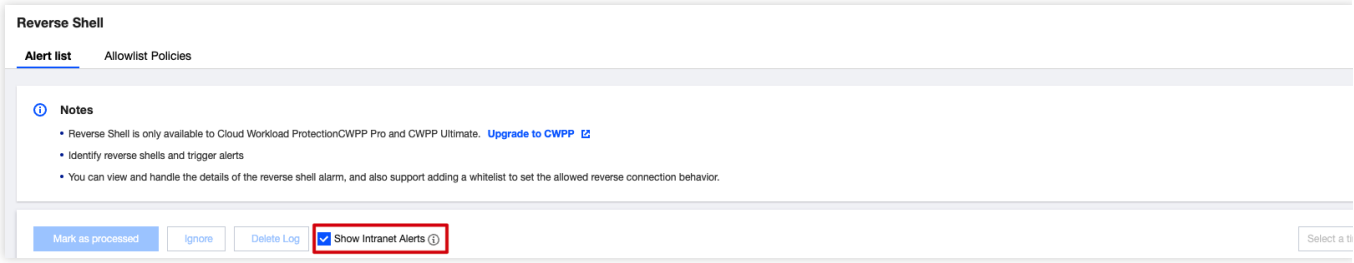


3. Display of private network reverse shell alarms.

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** in the upper right corner of the page to configure.

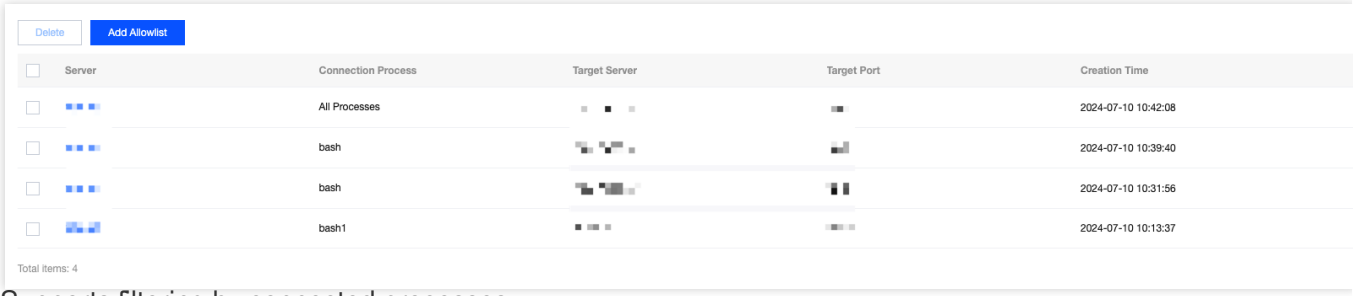
3.2 On the reverse shell settings page, you can define whether to enable private network reverse shell detection. If enabled, the system will support detection and report alarm data. If disabled, the system will stop detection.

3.3 Additionally, you can set whether to display private network alarm data in the reverse shell configuration page drawer or at the top of the alarm list. If checked, the alarm list will display private network alarm data. If unchecked, it will not display private network alarm data.



Allowlist Management

At the top of the reverse shell page, select **Allowlist Policies** to enter the allowlist management page.



Filter: Supports filtering by connected processes.

Custom Display Columns: Click

to set the fields displayed in the policy list.

Field Description:

Server: Servers on which the allowlist is effective.

Connection Process: Connection processes added to the allowlist.

Target Server: The target host of the reverse shell.

Target Port: The target port of the reverse shell.

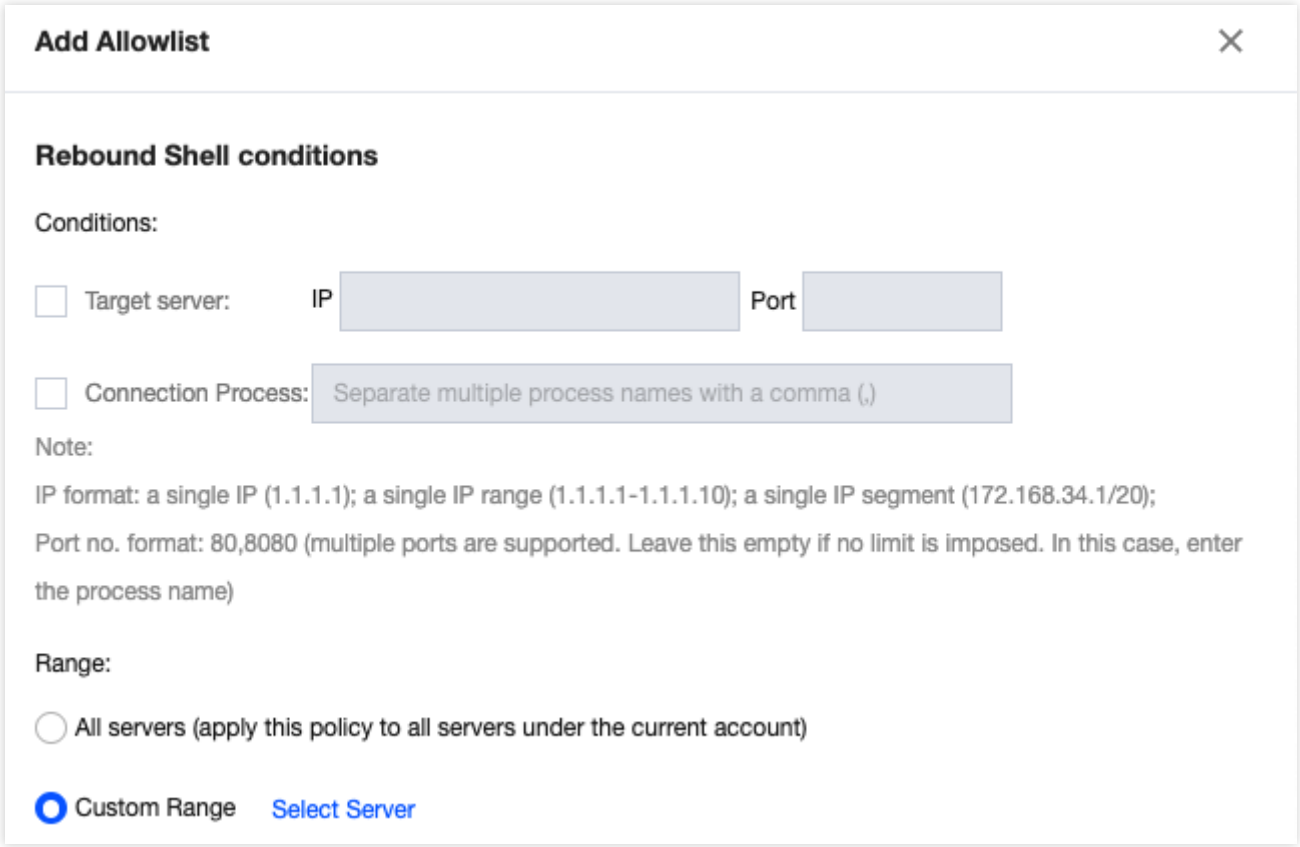
Creation Time: The creation time of the allowlist.

Update Time: The update time of the allowlist.

Edit: Edit the allowlist.

Delete: Delete the allowlist.

Add Allowlist:



Note:

IP format: Single IP (127.0.0.1), IP address (127.0.0.1-127.0.0.254), and IP range (127.0.0.1/24).

Port format: 80, 8080 (supports multiple ports separated by commas. Leave empty if there is no limit).

When both conditions are checked, both must be met to hit the allowlist.

If all servers are chosen in the server range, this allowlist will be added to all servers under the user's APPID. Proceed with caution.

Java Webshell

Last updated：2024-08-13 16:29:50

This document will introduce how to use the Java Webshell feature.

Overview

CWPP supports real-time monitoring, capturing unknown classes present in the memory of Java Web Service processes. It automatically identifies Webshells by using Tencent Cloud's offensive and defensive experiences along with expert knowledge. If a Java Webshell is detected, the system will provide you with real-time alarm notifications.

Prerequisites

The Java Webshell feature falls under the CWPP Ultimate Edition. To use this feature, you can upgrade to Ultimate Edition.

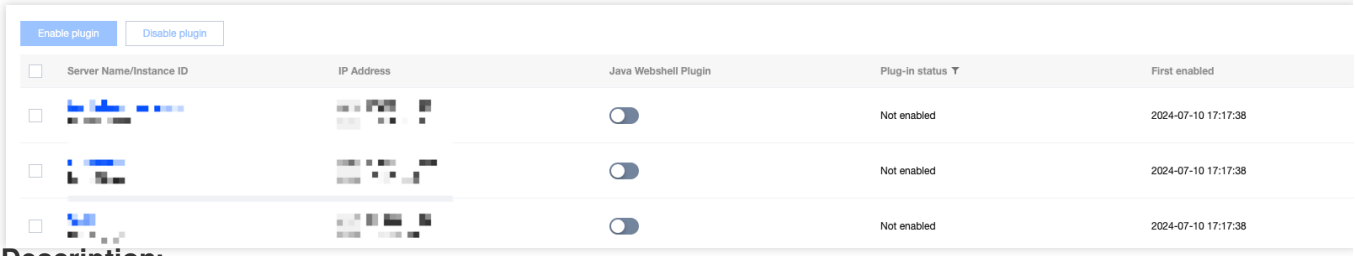
Directions

1. Log in to the CWPP console. In the left sidebar, choose **Cyber Defense** > **Java Webshell** to enter the Java Webshell page.
2. Choose **Plugin configuration**. Plugin configuration is a prerequisite for detecting Java Webshell. You can enable and disable plugins on your Ultimate Edition hosts and observe their specific running status.

Note:

Once the Java Webshell plugin is enabled, CWPP will automatically scan the host for Java Web Service processes and inject detection probes into these services. Therefore, it can monitor in real-time any Java Webshells injected by hackers via vulnerabilities or shells.

Hosts with the Java Webshell plugin deployed will continuously monitor and capture unknown classes existing in the memory of Java Web Service processes. Using Tencent Cloud's offensive and defensive experiences along with expert knowledge, it will automatically identify Webshells. If a Java Webshell is detected, the system will provide you with real-time alarm notifications.



Field Description:

Enable/Disable Plugin: The Java Webshell plugin is disabled by default. Users can manually set the switch, either for a single host or in batches for multiple hosts.

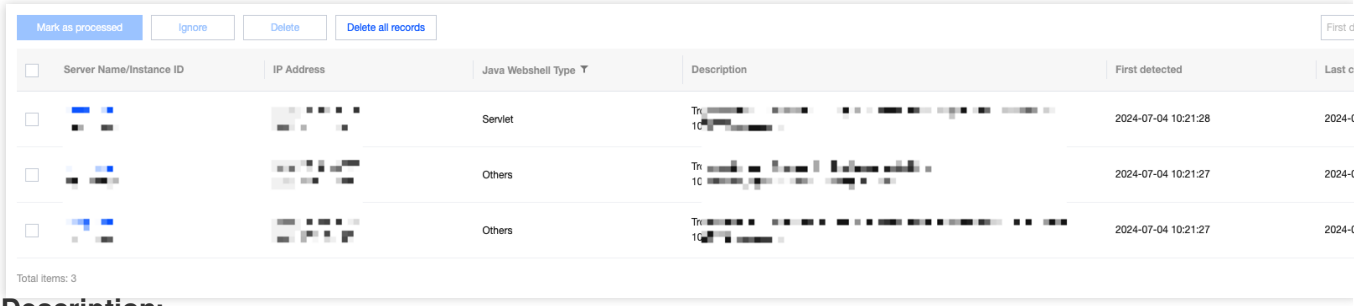
Plugin Status: All normal, has anomalies, and not enabled.

First Enabled: Indicates the first time the plugin was enabled.

Update Time: Indicates the most recent time the plugin was enabled or disabled.

Details: View the running status of the currently injected Java Webshell plugin, including process PID, main class name of process, plugin status (injecting, injection successful, plugin timeout, insertion and exit, and injection failed), and error log.

3. After enabling the Java Webshell plugin, you can choose **Alert List** to view detected Java Webshell events and perform related handling operations.



Field Description:

Java Webshell Type: Includes filter type, listener type, servlet type, interceptors type, agent type, and others.

Description: Summarize the overview of the Java Webshell.

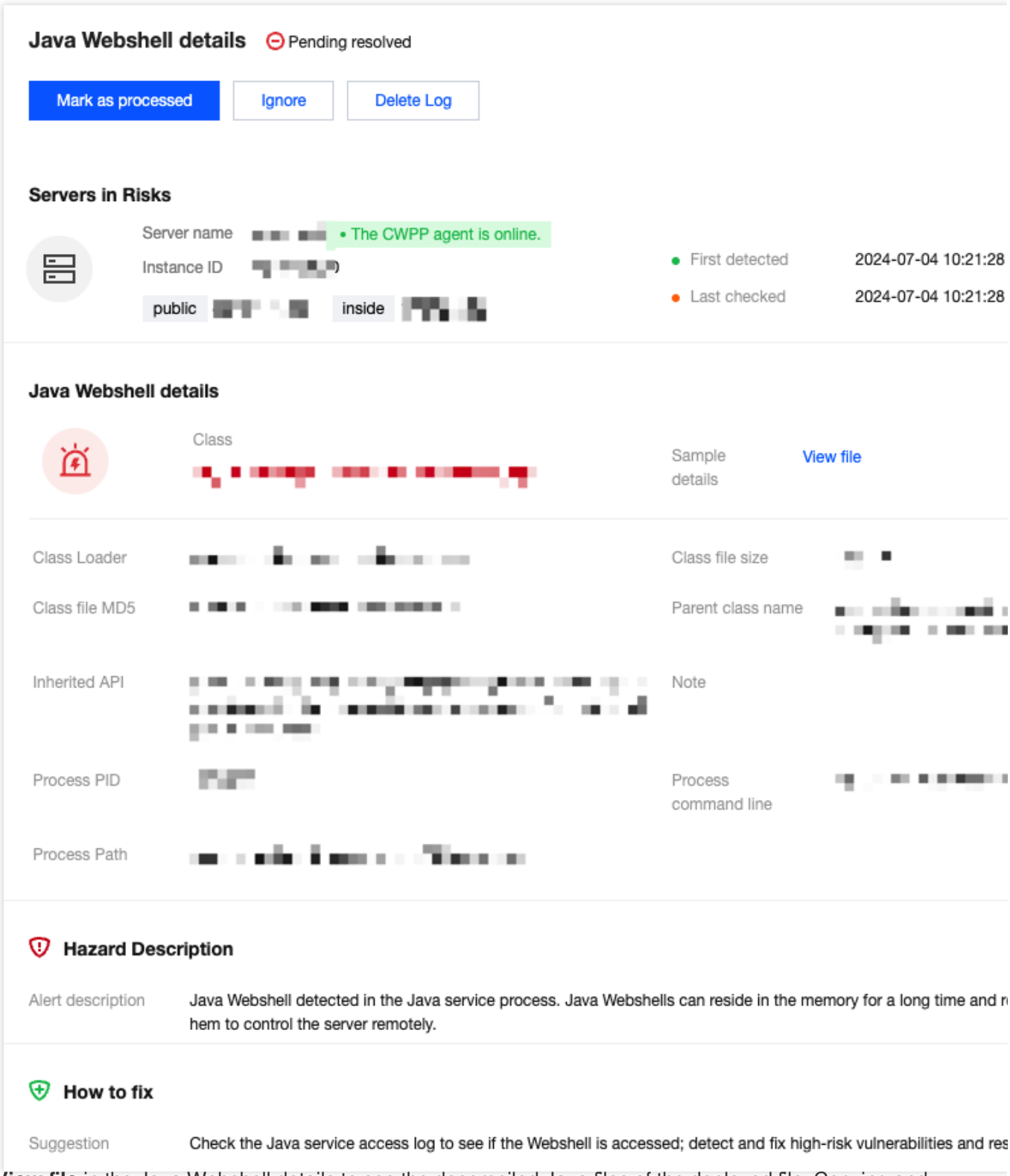
First Detected: The time when the Java Webshell was first detected.

Last Checked: The last time the Java Webshell was detected.

Status: Pending, processed, and ignored.

Operation:

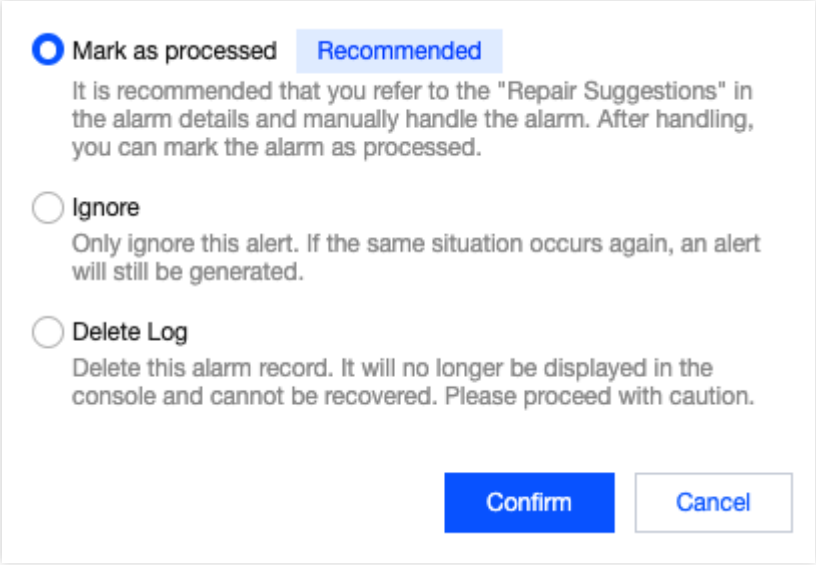
Click **Details** to view the details of the Webshell event.



Click **View file** in the Java Webshell details to see the decompiled Java files of the deployed file. Copying and downloading the decompiled Java files or the original class files are supported.

```
/*
 * Decompiled with CFR 0.152.
 *
 * Could not load the following classes:
 *  javax.el.ExpressionFactory
 *  javax.servlet.Servlet
 *  javax.servlet.ServletConfig
```

Click **Process** to perform operations such as Mark as processed, Ignore it, or Delete the record on the event. You can process the event individually or in batch.



Critical File Monitor
Monitoring Rules Configuration

Last updated：2024-08-13 16:29:50

The monitoring rules for core file monitoring are divided into system rules and custom rules. System rules are configurations set by Tencent CWPP operation experts and algorithm experts through multi-model refinement, suitable for most tamper-proof user configuration monitoring requirements. You can also create custom rules based on your business needs. Custom rules support editing, copying, and deleting.

Note:

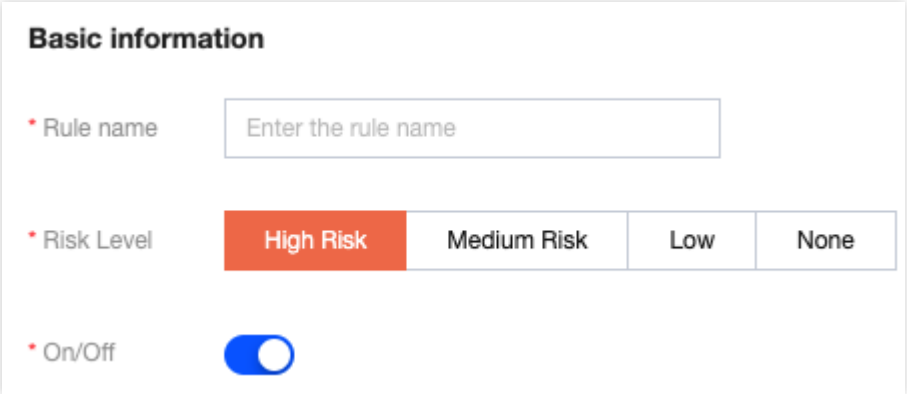
Core file monitoring is a feature of Ultimate Edition of CWPP. It is recommended to upgrade to Ultimate edition to protect CWPP.

Currently, core file monitoring is only available on Linux operating systems with kernel versions 3.10 and above.

Adding Rules

1. Log in to the CWPP console. In the left sidebar, choose **Cyber Defense** > **Corefile Monitor** > **Configure monitoring rules**.
2. On the configure monitoring rules page, click **Add Rule** at the top left.
3. On the add rule page, configure the basic settings, rule content settings, and effective server range parameter in sequence.

Basic information



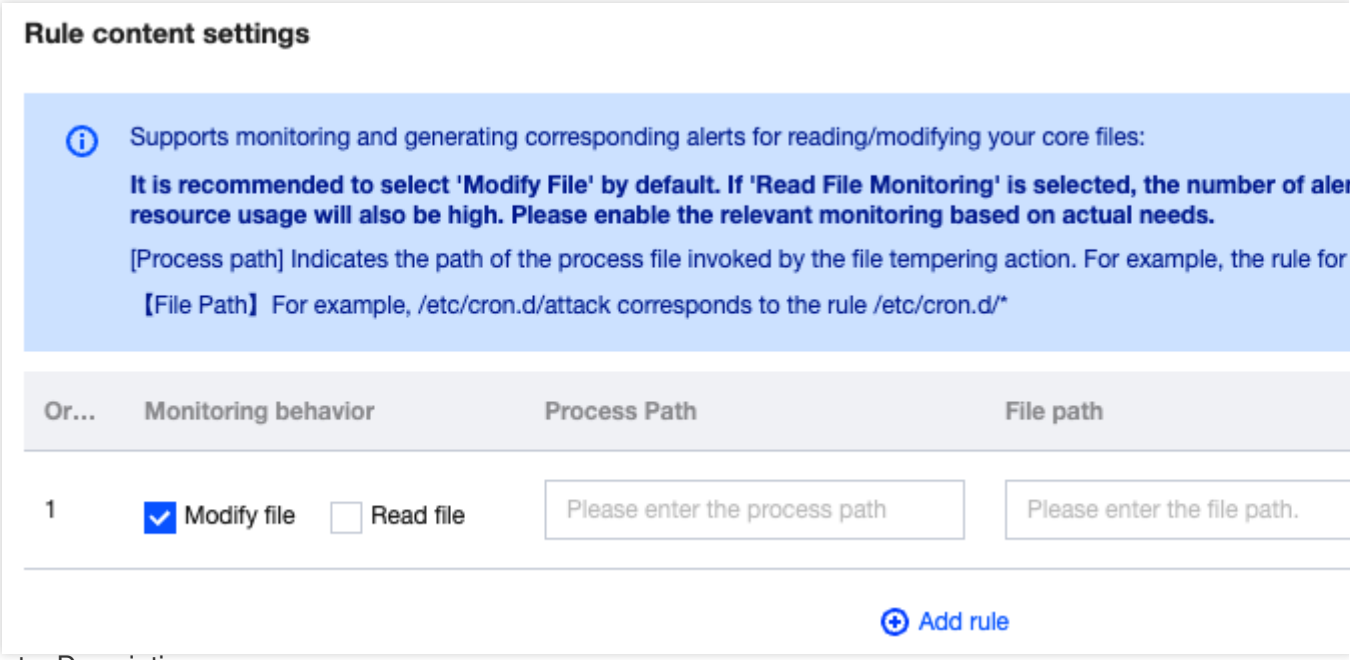
Parameter Description:

Rule Name: Custom name.

Risk Level: Depending on actual needs, you can select high-risk, medium-risk, low-risk, or none.

Enable/Disable: You can enable or disable this new rule.

Rule content settings: Click **Add rule**. You can 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, with a corresponding rule that could be */vi.

File Path: For example, /etc/cron.d/attack corresponds to a rule that could be /etc/cron.d/*.

Action: An alarm refers to the automatic generation of an alarm event in response to file system changes, with detailed event logging. Allowing refers to the operation of allowing file system change events, also with detailed event logging.

Note:

When the alarm and allowing respectively apply to the process path or the accessed file path, and there is an overlap in the effective servers, the overlapping servers will not generate alarms (meaning the allowing takes precedence).

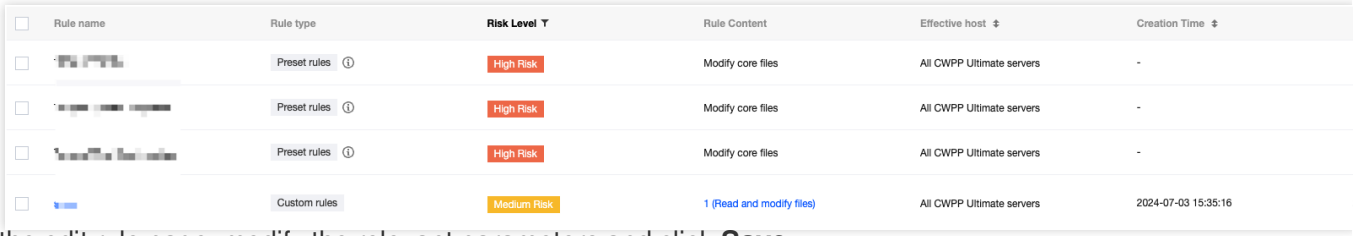
Effective host range: You can select all servers or selected servers based on actual needs.

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

Managing Rules

Editing Rules

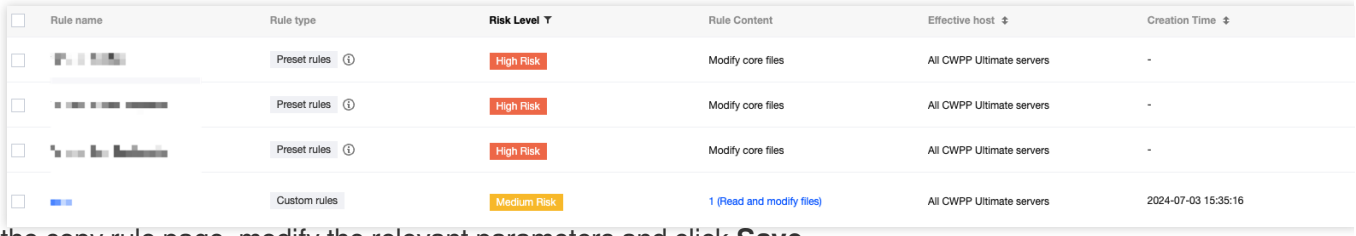
1. On the core file monitor > **Configure monitoring rules** page, choose the required rule and click **Edit** in the action bar.



2. On the edit rule page, modify the relevant parameters and click **Save**.

Copying Rules

1. On the core file monitor > **Configure monitoring rules** page, choose the required rule and click **Copy** in the action bar.

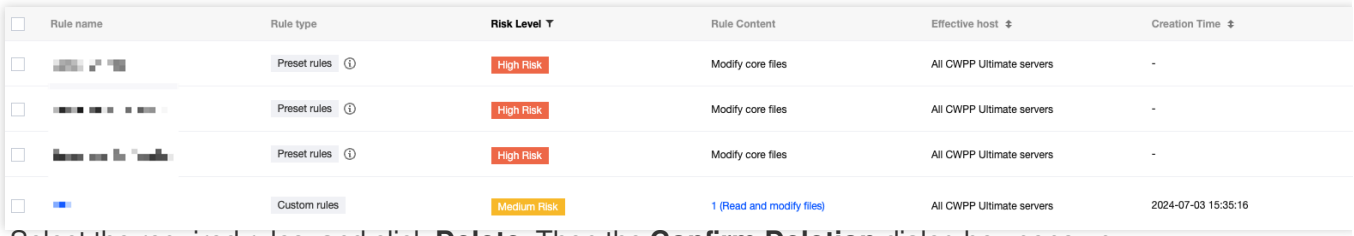


2. On the copy rule page, modify the relevant parameters and click **Save**.

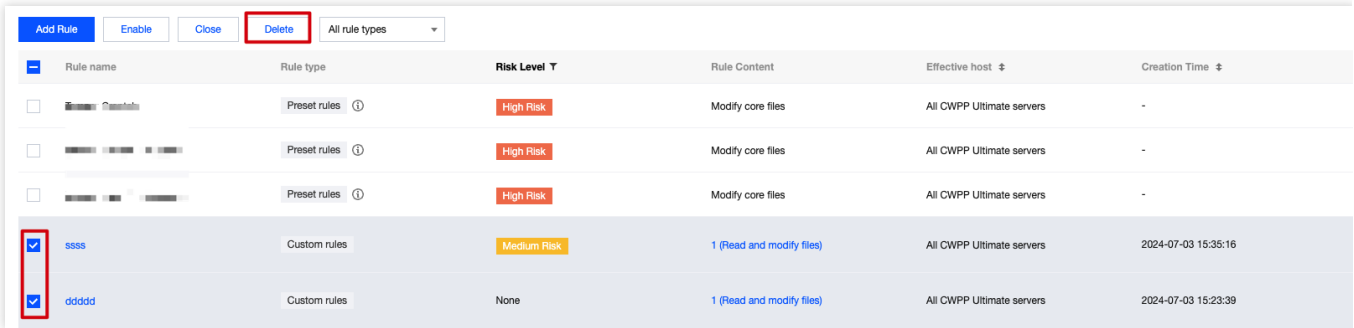
Deleting Rules

1. On the core file monitor > **Configure monitoring rules** page, single rule or batches of rules can be deleted as follows.

Single: Choose a single rule, and click **Delete** in the action bar. Then the **Confirm Deletion** dialog box pops up.



Batch: Select the required rules, and click **Delete**. Then the **Confirm Deletion** dialog box pops up.



2. In the **Confirm Deletion** dialog box, click **Confirm** to complete the deletion of the rules.

Note:

After deletion, the rules cannot be recovered. Proceed with caution.

Alarm List

Last updated：2024-08-13 16:29:50

The alarm list supports viewing alarm records of core file anomalies, enabling users to process (mark as processed, add to allowlist, or ignore) these alarm records and to delete these alarm records.

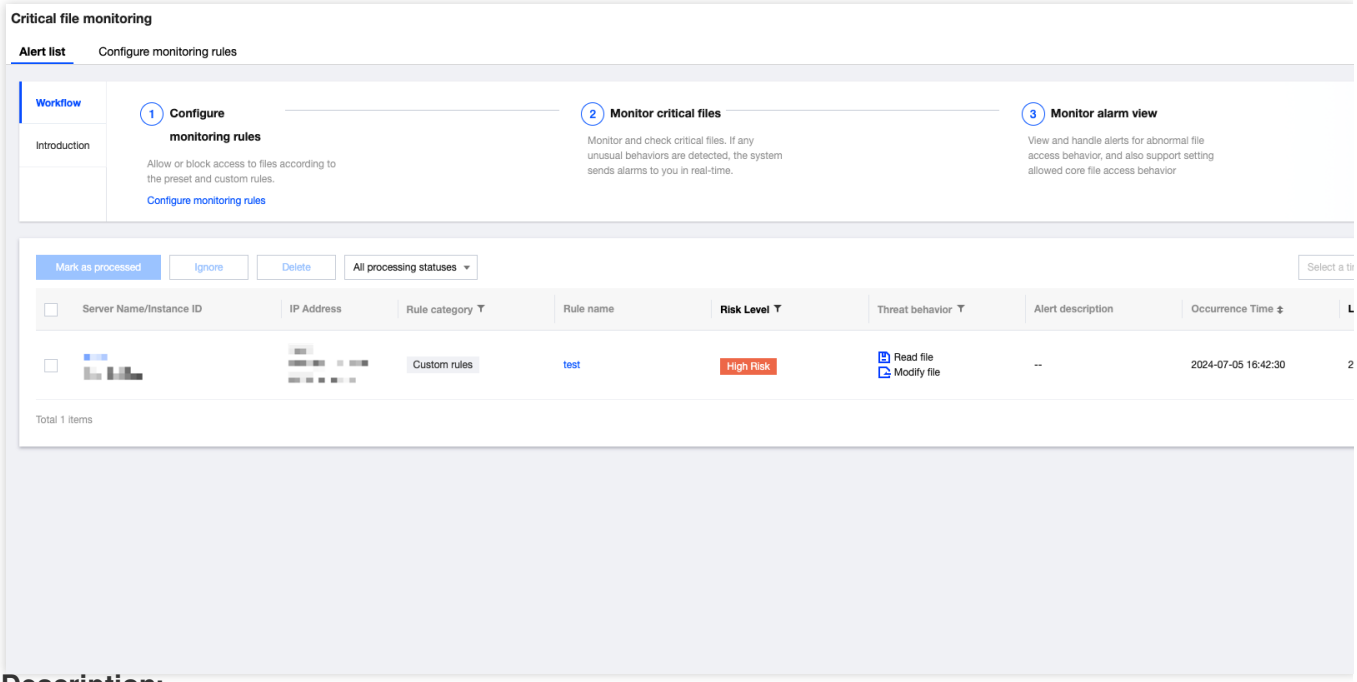
Note:

Core file monitoring is a feature of Ultimate Edition of CWPP. It is recommended to upgrade to Ultimate edition to protect CWPP.

Currently, core file monitoring is only available on Linux operating systems with kernel version 3.10 and later.

Processing Alarm Records

1. Log in to the CWPP console. In the left sidebar, choose **Cyber Defense** > **CoreFile Monitor** > **Alert list**.
2. On the alarm list page, choose the required alarm record, click **Process**, and choose Mark as processed, Add to allowlist, Ignore, or Delete the record.



Field Description:

Mark as Processed: You can manually process the alarm, and after that, it can be marked as processed.

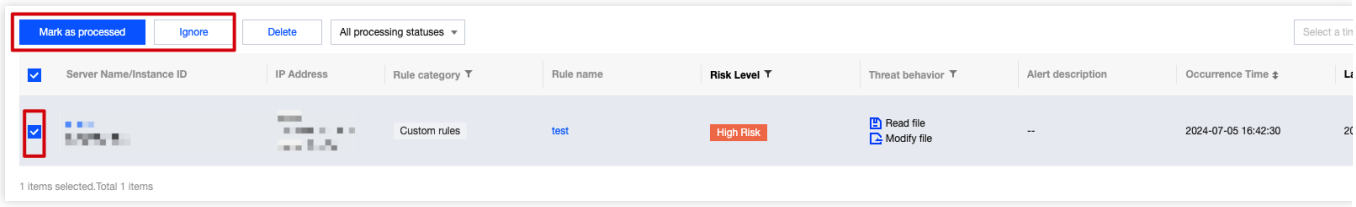
Add to Allowlist: Add the current file path to the allowlist. Subsequent read/modification actions will not trigger alarms. Proceed with caution.

Ignore: Only ignore this alarm. If the same situation occurs again, an alarm will still be triggered.

Delete the Record: Delete the alarm record. It will no longer be displayed on the console and cannot be recovered. Proceed with caution.

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

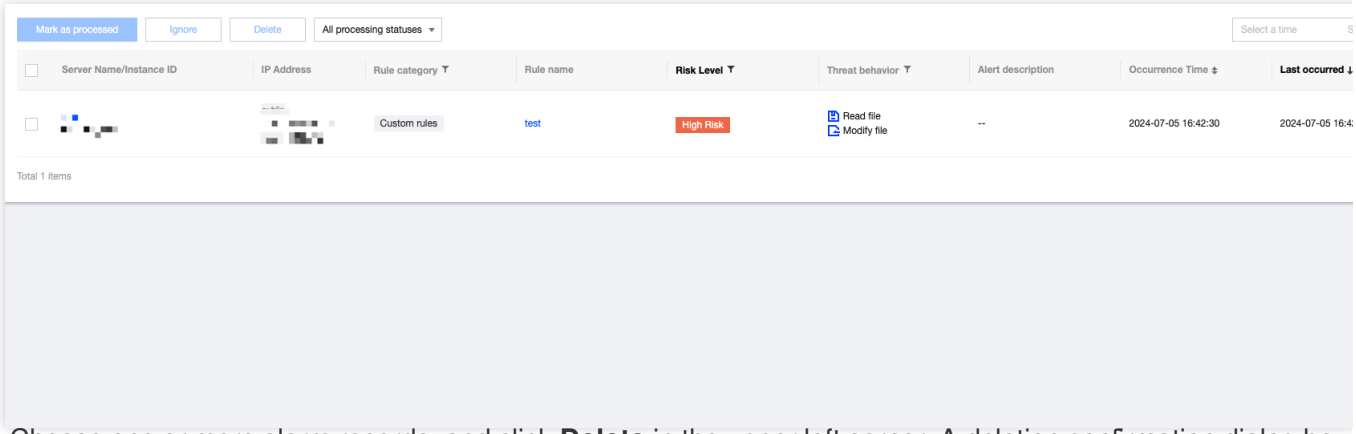
4. The alarm list also supports batch processing of alarm records. After choosing one or more alarm records, click **Mark as processed** or **Ignore** in the upper left corner. After a secondary confirmation, the chosen alarm records can be processed.



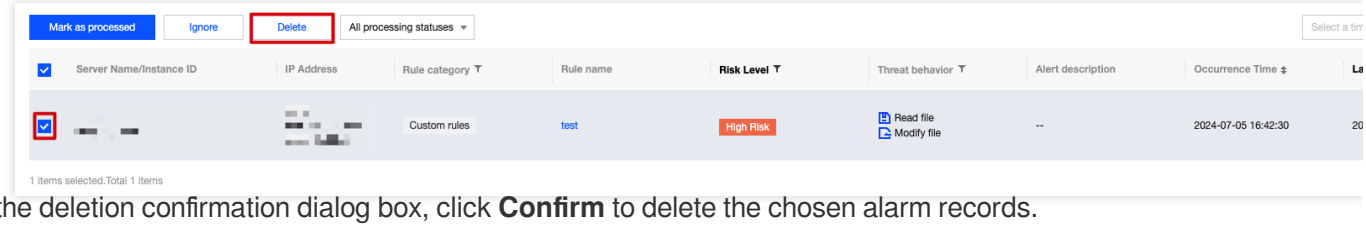
Deleting Alarm Records

1. On the alarm list page, you can delete alarm records individually or in batch.

Single: Choose the required alarm record, and click **Process** > **Delete**. A deletion confirmation dialog box will pop up.



Batch: Choose one or more alarm records, and click **Delete** in the upper left corner. A deletion confirmation dialog box will pop up.



2. In the deletion confirmation dialog box, click **Confirm** to delete the chosen alarm records.

Note:

Once the chosen alarm records are deleted, they will no longer be displayed in the console and cannot be recovered. Proceed with caution.

Network Attack

Last updated：2024-08-13 16:29:50

Network attacks are based on technical support from Tencent Cloud's security offensive and defensive Team, providing the automatic monitoring of malicious traffic for you. It combines malicious behaviors generated during the intrusion process. It performs real-time automatic correlation analysis of attacks and alarms, outputs attack traffic data, and notifies attack events. This document will introduce how to view and process network attack alarms.

Limits

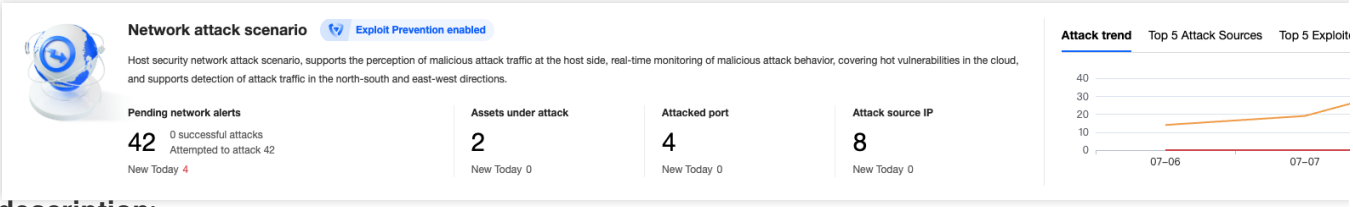
Detection targets: Only Pro edition/Ultimate edition Linux hosts are supported.
Detection range: Only detects some of the hotspot vulnerability attack behaviors that involve EXPs with proven successful attack instances in the cloud.
Vulnerability defense: Only supported for Ultimate edition Linux hosts.

Defense Status Description

Supports vulnerability defense (disabled): CWPP supports defending against this vulnerability, but this host has disabled the defense for it.
Supports vulnerability defense (enabled): CWPP supports defending against this vulnerability, and this host has enabled the defense for it.
Vulnerability defense not supported: CWPP does not support defending against this vulnerability.
Note:
Possible reasons for vulnerability defense disabled: Defense switch is not turned on, the host is not an Ultimate edition, or it is not within the defense host range.
An attack event indicates that hackers are using attack methods that exploit this vulnerability, but it does not mean that the current machine has this vulnerability.

Alarm Statistics

1. Log in to the CWPP console. In the left sidebar, choose **Cyber Defense** > **Network Attack**.
2. On the network attack page, you can view the status of vulnerability defense, pending alarm data statistics, and the top 5 situations.



Field description:

Vulnerability Defense Status: Indicates the status of the vulnerability defense switch.

Pending Network Alarms: The current number of pending alarms.

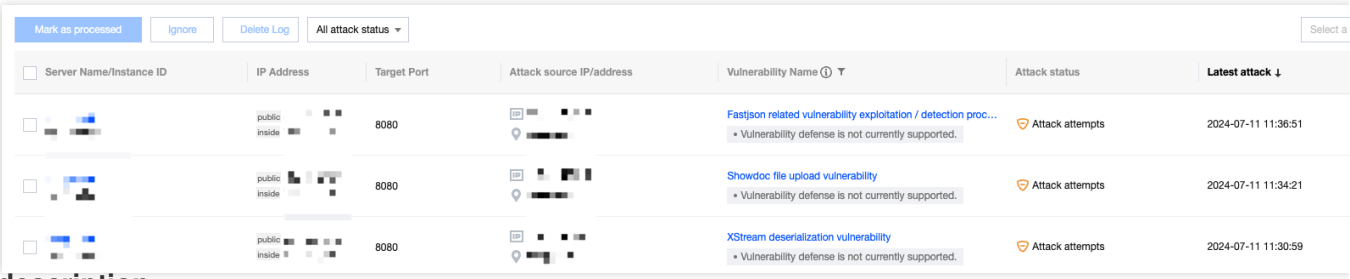
Attacked Assets: The number of attacked assets involved in the current pending alarms.

Attacked Port: The number of attacked ports involved in the current pending alarms.

Attack Source IP: The number of attack source IPs in the current pending alarms.

Viewing Alarms

On the network attack page, you can view network attack details, including server name/instance ID, IP address, and template port.



Field description:

Server Name/Instance ID: The name and instance ID of the attacked host.

IP Address: Refers to the public/private IP of the attacked host.

Target Port: The attacked port.

Attack Source IP/Address: Refers to the attacker's source IP and location.

Vulnerability Name: Refers to the attacker's use of an attack method for a specific vulnerability and the current enabled/disabled status of vulnerability defense.

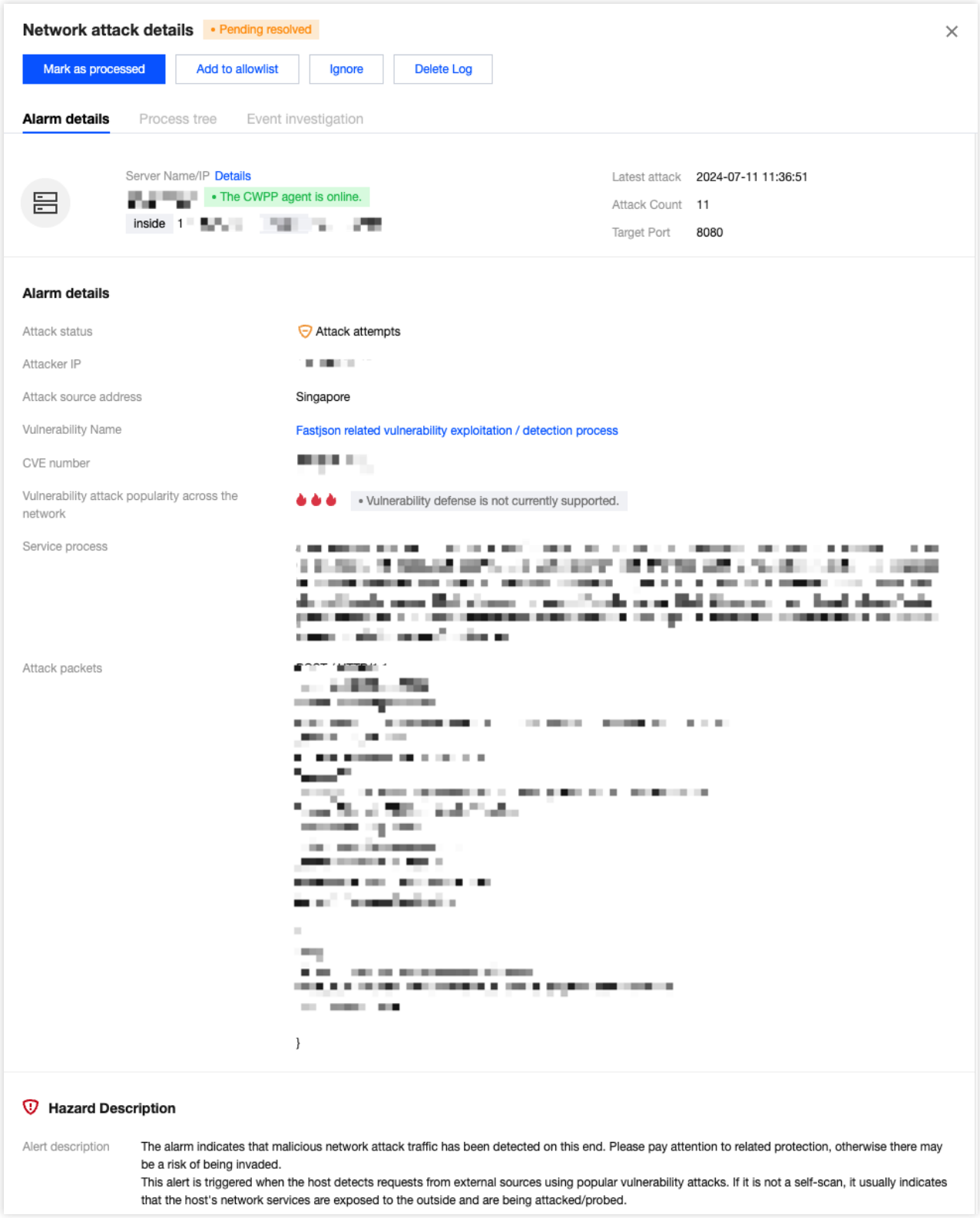
Attack Status: Refers to the outcome of the attacker's attack. Either an attempted attack (attacked but not successfully compromised) or a successful attack (confirmed compromise).

Latest Attack: The time when the attack was last detected.

Attack Count: The total number of times the same attack has been detected.

Processing Status: Pending, processed, allowlisted, and ignored.

Details: Supports viewing alarm details, hazard description, and solutions.

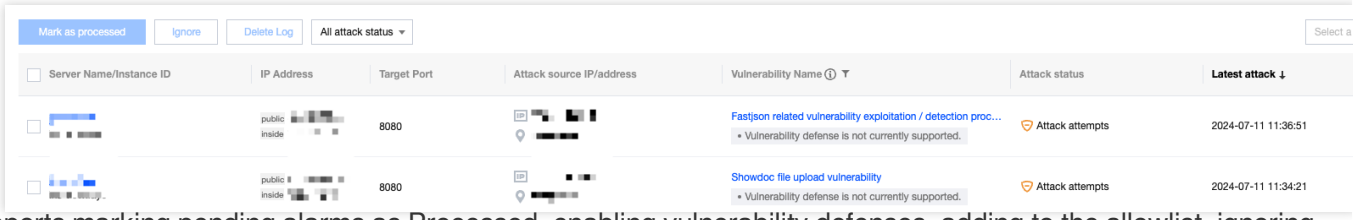


Processing Alarms

1. On the network attack page, choose the required alarm and click **Process** in the action bar.

Note:

Select one or more alarms and click **Marked as Processed**, **Ignore**, or **Delete Log** in the top left corner for batch operations.

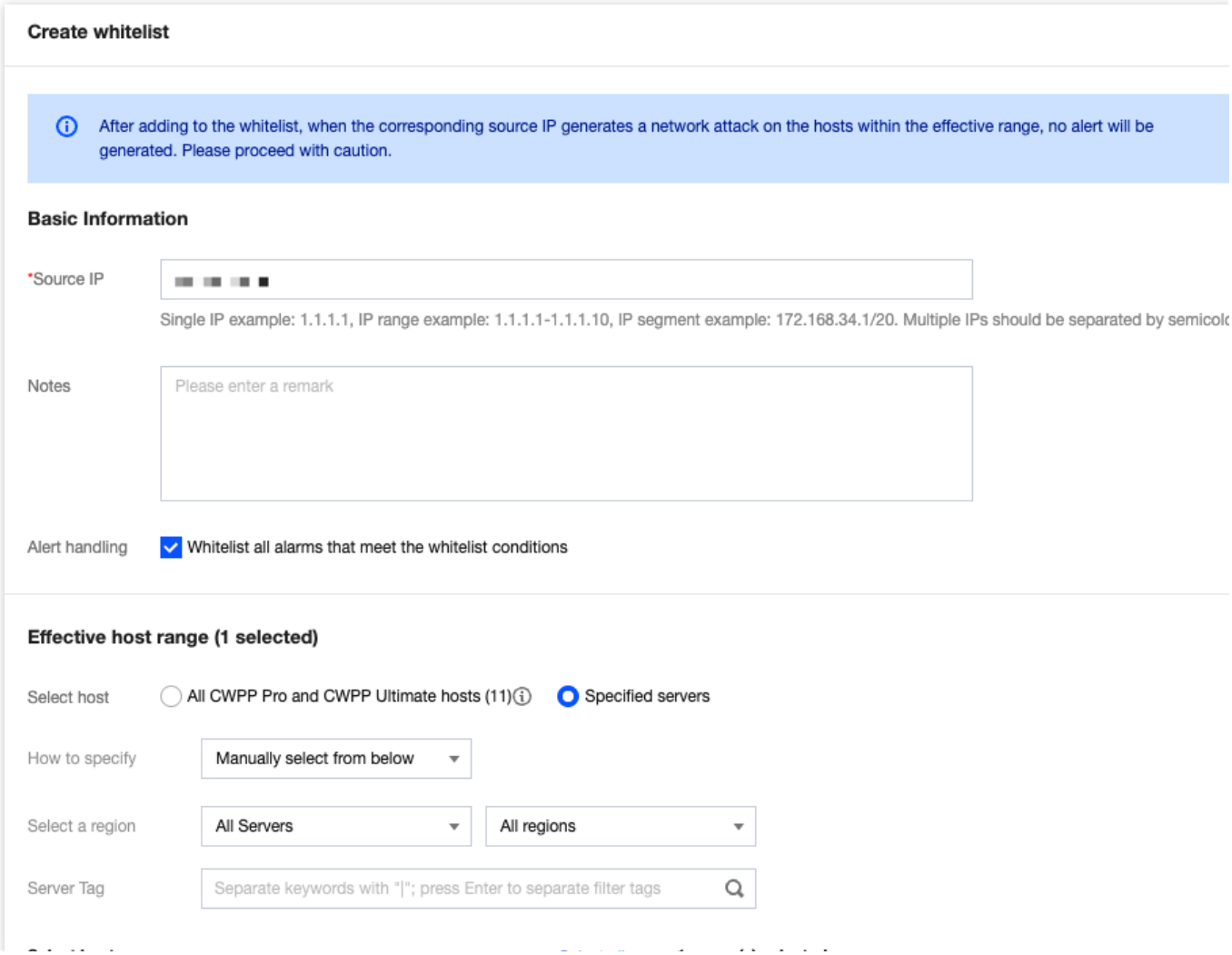


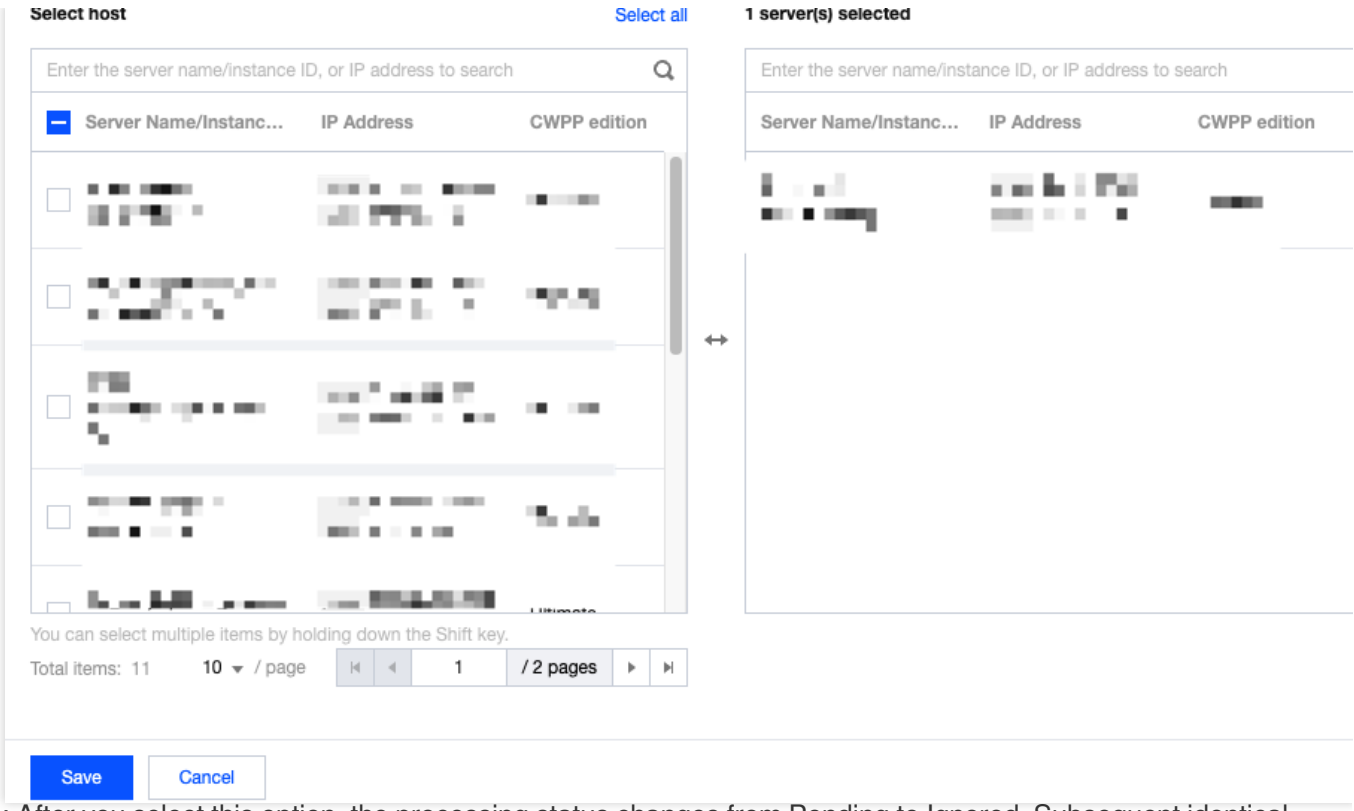
2. Supports marking pending alarms as Processed, enabling vulnerability defenses, adding to the allowlist, ignoring, and deleting logs.

Marked as processed: Manually process the alarm and mark it as Processed after completion.

Enable vulnerability defense: After the operation is complete, the processing status will be automatically changed to Processed. Supports checking to mark all pending alarms related to the host covered by this vulnerability defense as Processed.

Add to allowlist: The attack source IP can be allowlistd and the effective host range can be edited. After operation is complete, the processing status will be automatically changed to Allowlisted. Supports batch allowlisting historical alarms.





Ignore: After you select this option, the processing status changes from Pending to Ignored. Subsequent identical attacks will still trigger alarms.

Delete log: Delete the current alarm record, and it cannot be recovered.

A Ransomware Defense

Last updated：2024-08-13 16:29:50

Ransomware is a type of malware that encrypts users' important files and demands a ransom for decryption. Ransomware defense, through the use of bait files and regular backup functionalities, can effectively monitor intrusion attacks from ransomware, safeguarding users' critical data from extortion. In the event of a ransomware attack, it also enables timely recovery from backups.

Note:

This feature is currently in the grayscale testing phase. If you have a need for ransomware protection, please Contact Us to be allowlisted for usage.

Restrictions Description

This feature is only supported on the Professional or Ultimate Edition of Tencent CVM (For Linux, only operating systems with a kernel version of 3.10 or later are supported).

Each host can only be bound to one ransomware defense policy.

Billing Description

CWPP defense version: Before using the ransomware defense feature, bind the Professional or the Ultimate Edition to the host for authorization. You can purchase and bind these authorizations on the CWPP Purchase Page.

Snapshot: Backups will be executed in the form of Tencent Cloud Snapshot. Billing is conducted on a post-paid basis, with charges settled hourly. For details, see the Price Overview.

Defense Principle

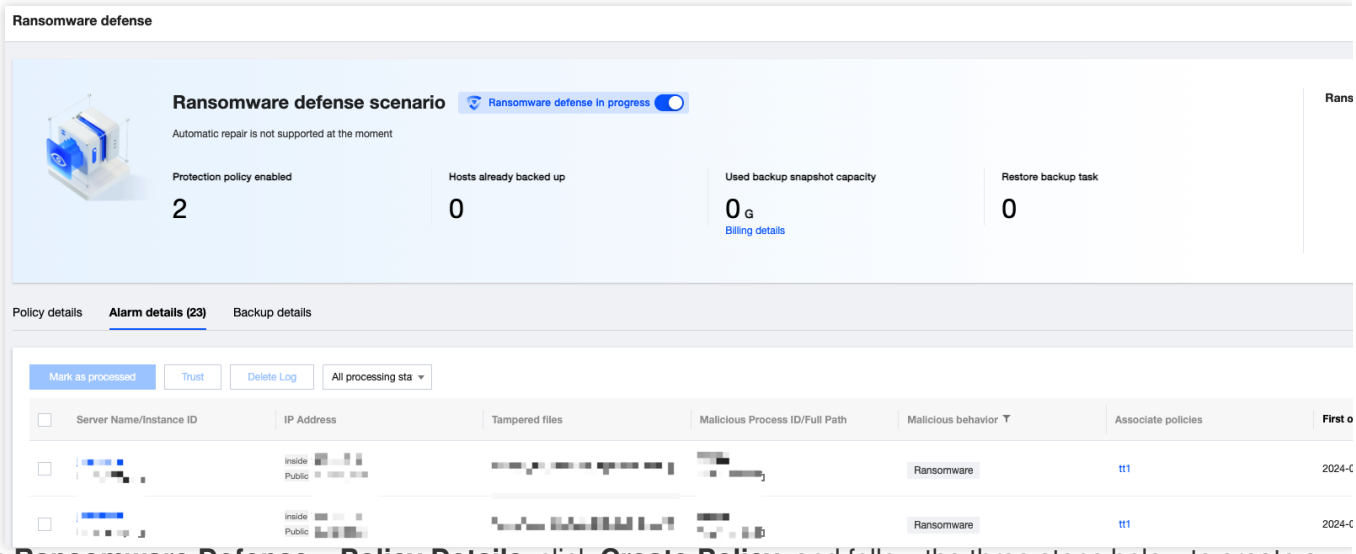
1. Monitoring bait files: Bait files are deployed in specific directories, and there is a scheduled check for alterations and encryption to the file names, hash values, and other information. If any anomalies are found, users are alerted in real-time.

2. Monitoring non-bait files: Through file detection and process detection, the system identifies any actions such as modification, deletion, or encryption of files. If any abnormalities are found, users are alerted in real-time.

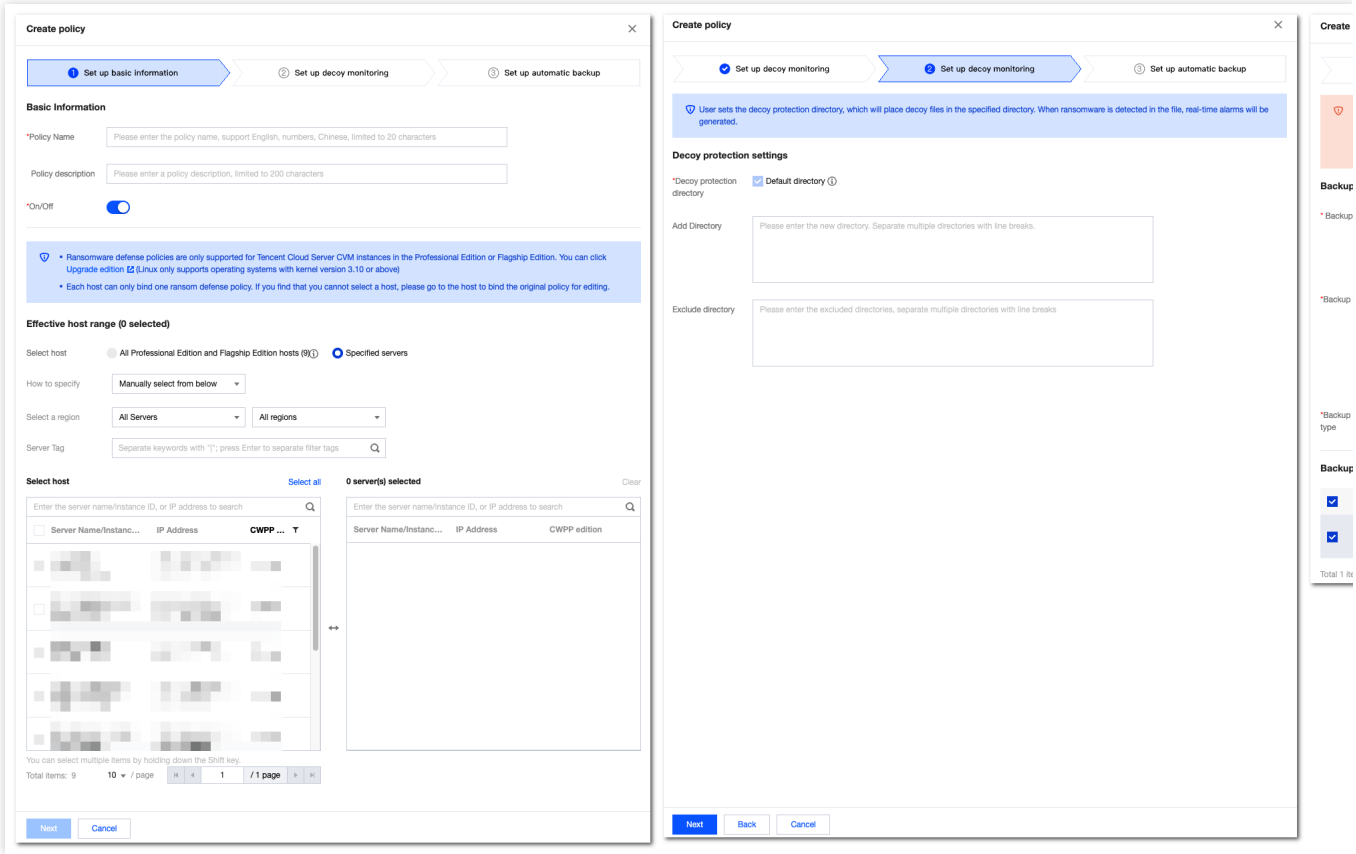
3. Regular snapshot backup: A one-click snapshot feature is provided, allowing users to configure scheduled snapshots. This ensures a fallback option for data recovery in the situation where data gets encrypted by ransomware.

Directions

1. 1. Log in to CWPP Console, select **Advanced Defense** > **Ransomware Defense** in the left sidebar.



2. 2. In **Ransomware Defense** > **Policy Details**, click **Create Policy**, and follow the three steps below to create a defense policy.



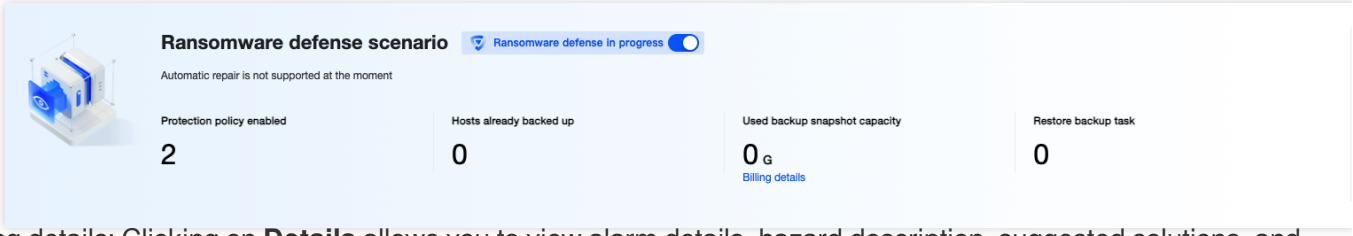
Note:

Default directory for bait files:

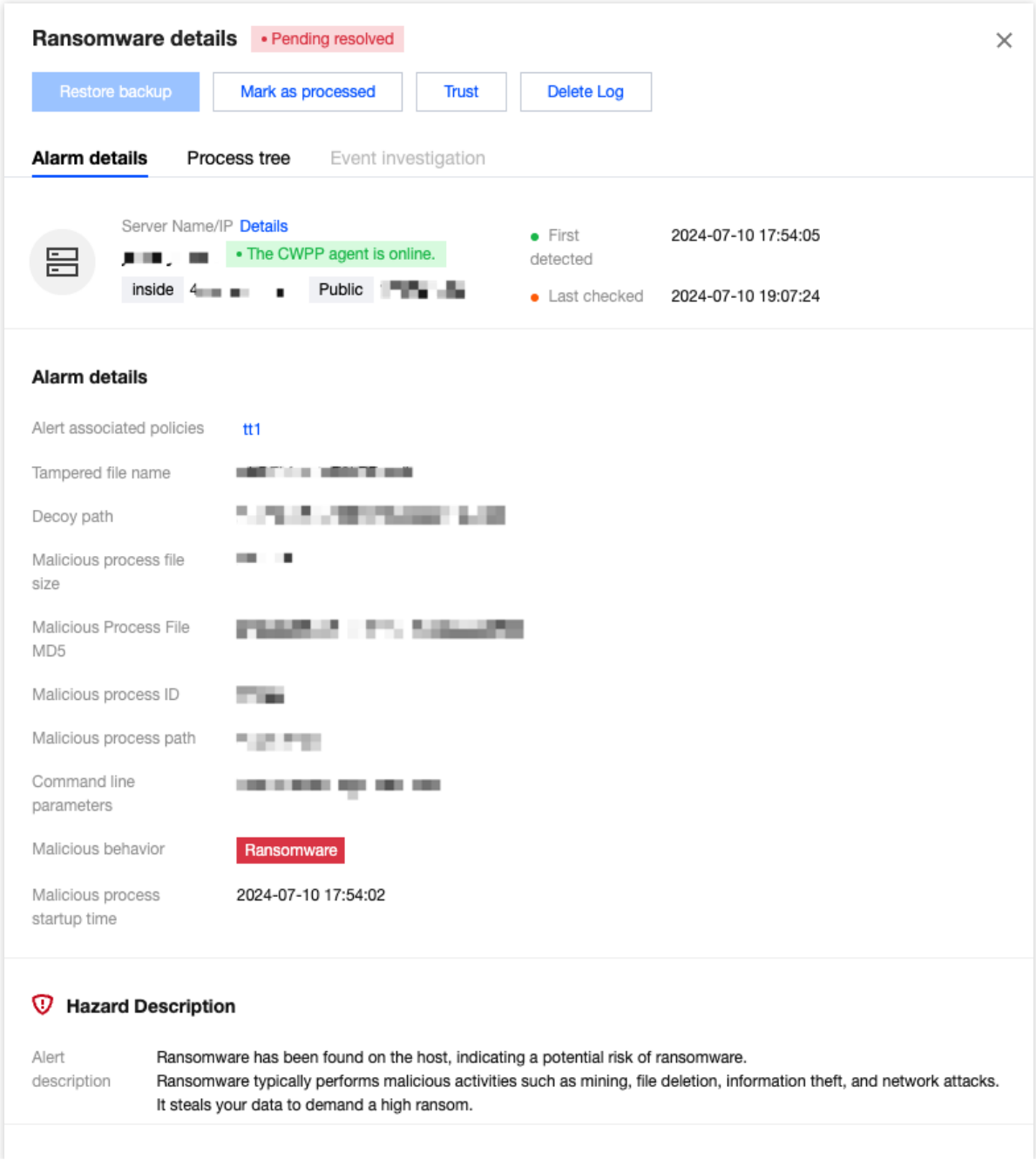
Windows operating system: C:\\ProgramData.

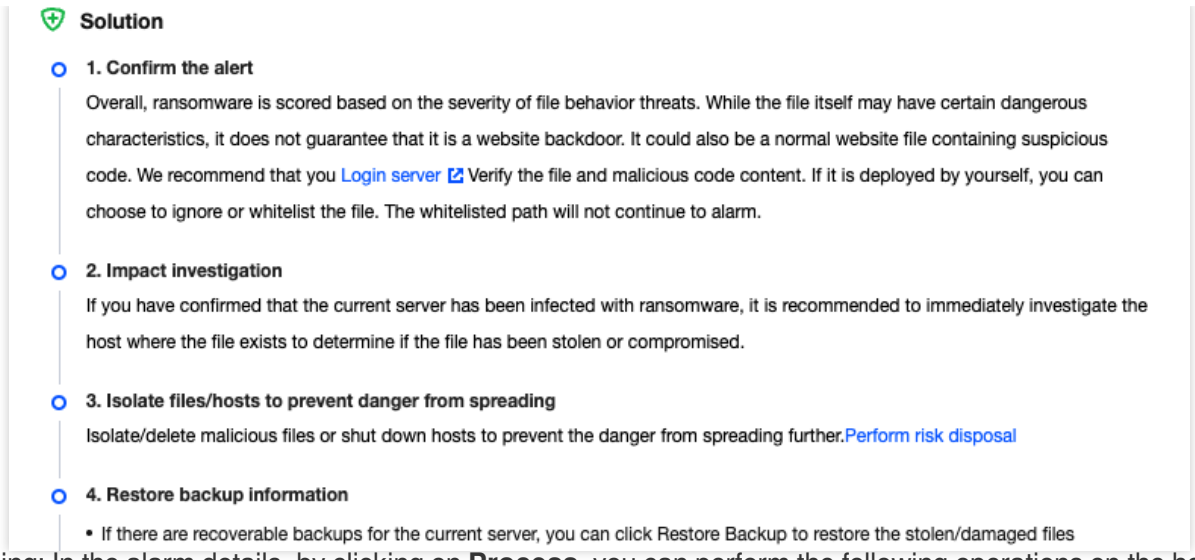
Linux operating system: YunJing.

3. 3. After creating a policy, you can view statistics on the current policy, alarms and defense rates. There is also a feature to disable all ransomware defense policies with a single click.



Viewing details: Clicking on **Details** allows you to view alarm details, hazard description, suggested solutions, and process tree information.





Handling: In the alarm details, by clicking on **Process**, you can perform the following operations on the host.

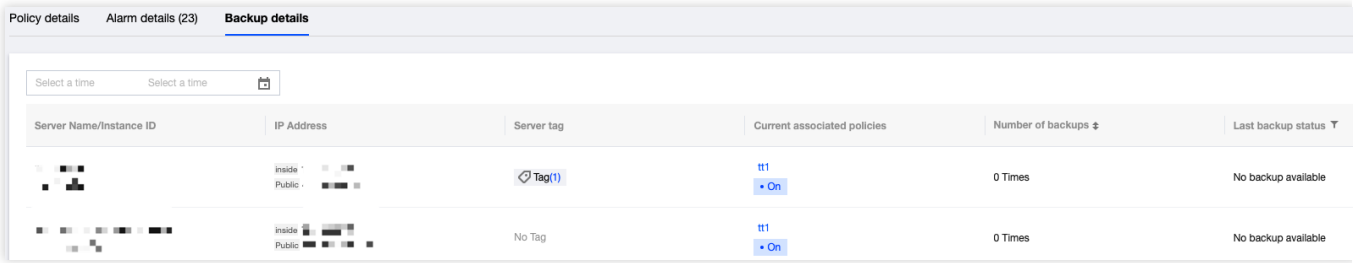
Restoring backups: If the host has been attacked by a ransomware, you can click this option to select a snapshot from the backup list for restoration.

Marking as handled: It is recommended that you follow the "Remediation Suggestions" provided in the alarm details to address the issue. Once you have resolved the alarm, you can mark it as handled.

Trust: After the trust operation is performed, only the file (MD5) or process on the current host will be allowlisted. Simultaneously, all corresponding alarms will be treated as trusted. There will be no further alarms in the future, please proceed with caution.

Deleting records: After being deleted, the alarm record will never appear in the console display again. Once deleted, the record cannot be recovered, please proceed with caution.

4. 5. In the **Backup Details**, you can view the backup status for each host, including the associated policies, the number of backups made, the status of the most recent backup, and the time it occurred. You can also view detailed records of the backups and choose one of the snapshots to restore the backup.



Log Analysis

Last updated：2024-08-13 16:29:50

Log analysis is an important part of the CWPP protection solution. It provides security event logs about the CWPP. It supports SQL retrieval and query. It offers visualized reports and statistics. This helps users quickly identify intrusions, conduct source tracing, and perform other security operation tasks. This document will introduce how to use the log analysis feature.

Restrictions

Log data can be collected. It is subjected to the following restrictions by the host protection edition.

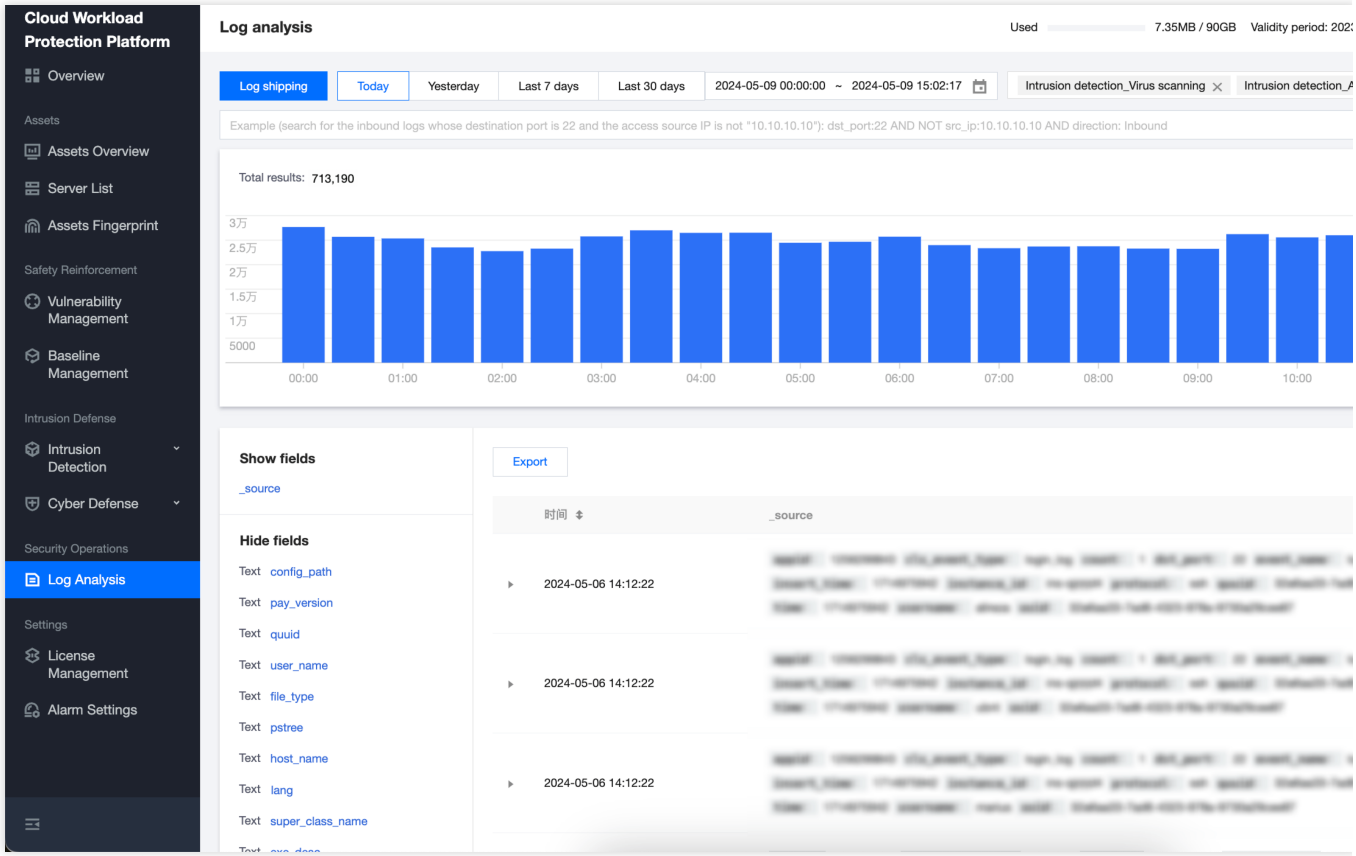
Log Category	Log Type	Log Description	Supported Versions
Host Asset Logs	Host Information	Includes host instance ID, IP, operating system, region, VPC, instance status, and whether the CWPP agent is installed. **Note:** Only the Synchronization Time of the host is changed. The rest of the information remains unchanged. It will not generate log entry.	All Hosts
	Asset Fingerprint	Includes resource monitoring, account, port, software application, process, database, web application, web service, web framework, website, Java archive file, startup service, scheduled task, environment variable, kernel module, and system installation package. **Note:** Only the Data Update Time of the asset fingerprint is changed. The rest of the information remains unchanged. It will not generate log entry.	Pro edition, and Ultimate edition
Client-Reported Logs	Client Reporting	Original host logs (including system authentication and license information, system security information, system messages, and system audit information); DNS logs, process snapshot logs, network five-tuple logs, file monitoring logs, and log-in activity logs.	Basic edition and higher
Alarm Log	Intrusion detection	Malicious file scan（malicious files）, Malicious file scan（abnormal processes）, unusual login, password cracking, malicious requests, high-risk commands, local privilege escalation, and reverse shell.	Professional edition and Flagship edition

Vulnerability Management	Emergency vulnerabilities, Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities.	Professional edition and Flagship edition
Baseline Management	Security baseline	Professional edition and Flagship edition
Advanced Defense	Corefile monitoring, Java Webshell, and network attacks	Flagship edition
Client-Related	Client offline and client uninstallation	Basic edition and later

To use the log shipping feature, you must first purchase a TDMQ for CKafka instance, and select the appropriate CKafka instance specification based on the volume of logs to be shipped.
The log shipping feature only supports using a single TDMQ for CKafka account for shipping.
According to the Cybersecurity Law, the log storage duration must be at least 6 months. It is recommended that each server be configured with a storage capacity of 20 - 40 GB to collect and retain log data.

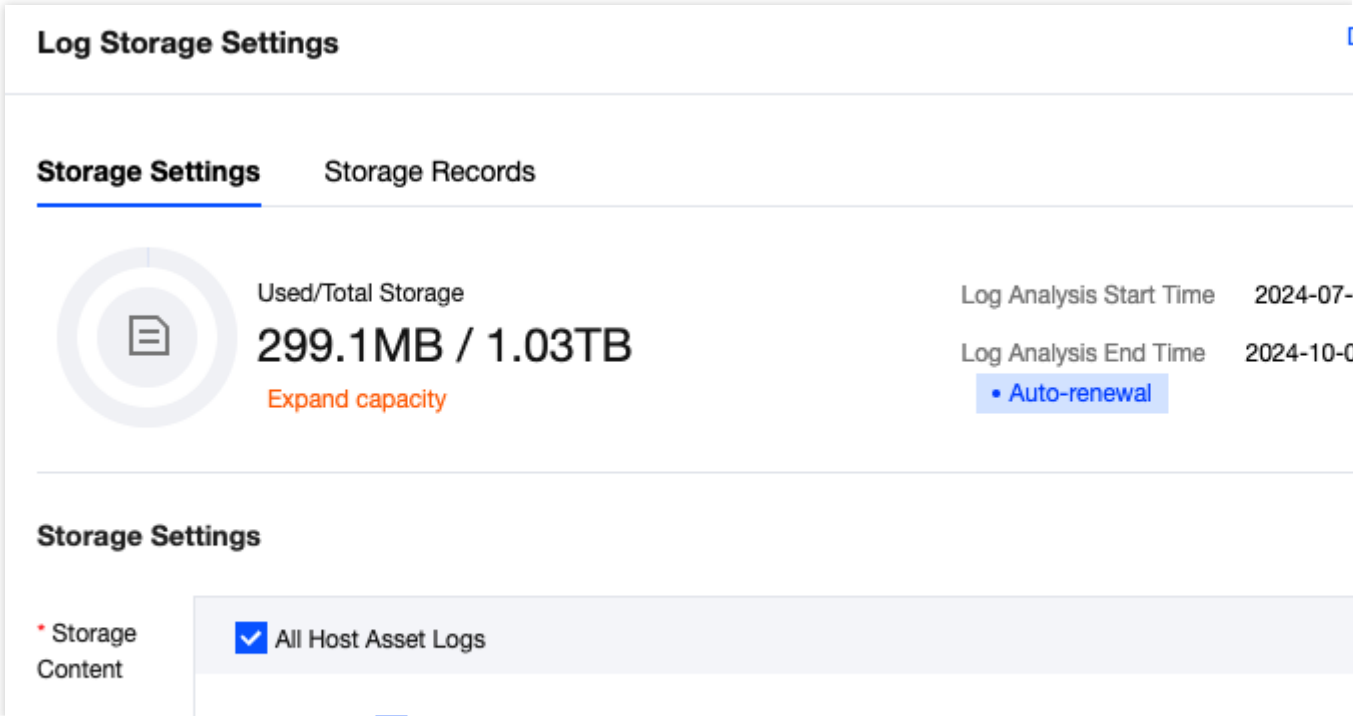
Operation Guide

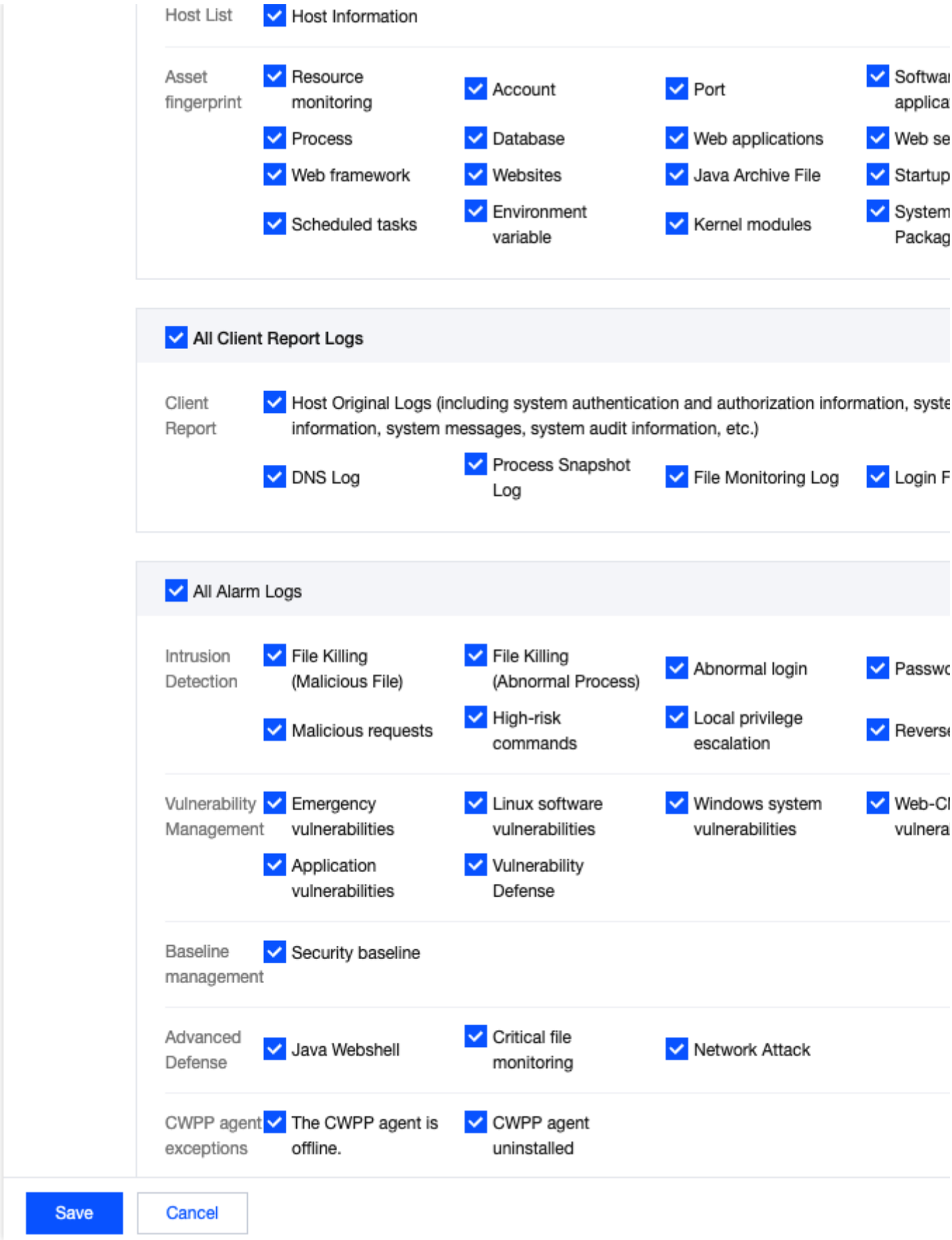
1. Log in to the Host Security console.
2. In the left sidebar, choose **Log Analysis** to perform operations such as log query and log shipping.



Log Storage Settings

Click **Log Storage Settings** , a pop-up window will appear. In the **Storage Settings** section, you can view the current log storage status and configure the storage content and storage duration. In the **Storage Records** section, you can view the log storage status at midnight on the last day of each month. By default, the display is in reverse chronological order.

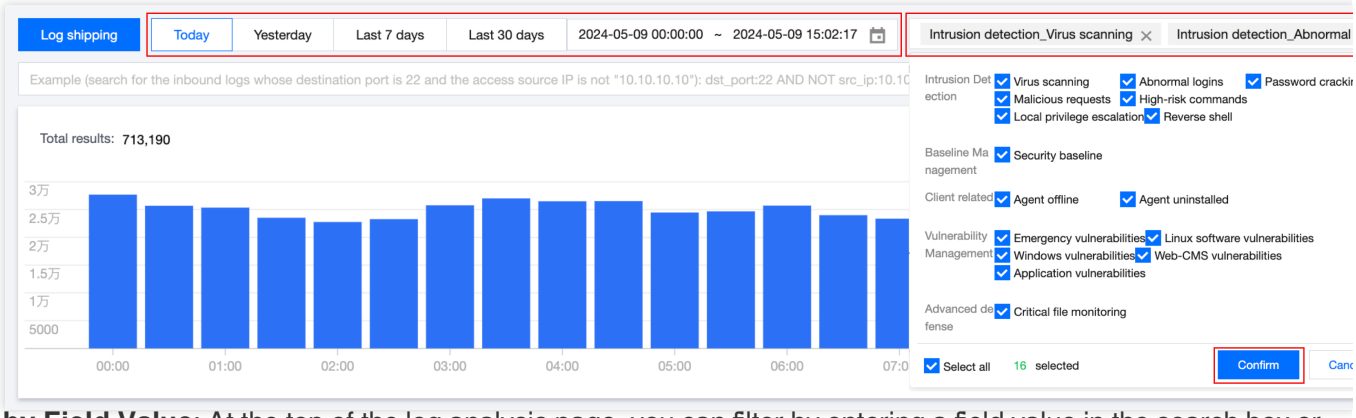




Viewing Logs

On the log analysis page, logs can be filtered based on the following methods.

Filter by Time or Type: At the top of the log analysis page, you can filter logs by time and log type. Choose the time range or log type, and click **Confirm**.



Filter by Field Value: At the top of the log analysis page, you can filter by entering a field value in the search box or by choosing a field match filter.

Filter by Search Box Input Field Value: See the following figure. Enter the desired field and field value in the search box, and click

to filter.

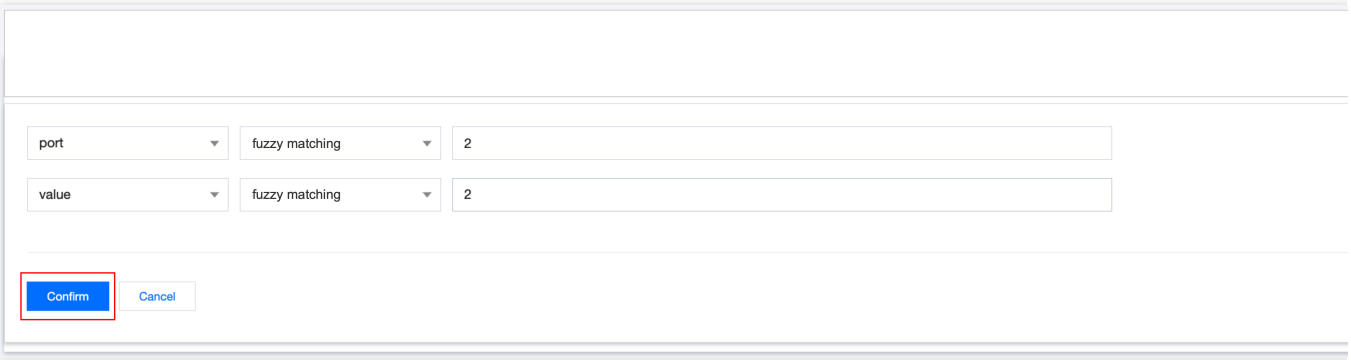
Search Syntax and Examples

grammar	semanteme	examples
key:value	Key value search, value support* Fuzzy search, support key: (value1 OR value2)	src_ip:10.0.0.1 ; src_ip:(10.0.0.1 OR 10.
A AND B	"AND" logic, returning the intersection result of A and B	src_ip:10.0.0.1 AND protocol:TCP
A OR B	"OR" logic, returning the union result of A and B "	src_ip:10.0.0.1 OR protocol:TCP
NOT B	"Not" logic, returning results that do not contain B	NOT src_ip:10.0.0.1
A NOT B	"Subtract" logic returns a result that meets A but does not meet B, i.e., A–B "	src_ip:10.0.0.1 NOT protocol:TCP
*	Fuzzy search keyword, matching zero, single, or multiple arbitrary characters, does not support the beginning *. Enter abc * to return results beginning with abc	src_ip:10.10*
?	Fuzzy search keywords, matching a specific location with a single assumption, enter abc? C *, returns a result that starts with ab and ends with c, with only one character between the two	src_ip:10.1?.0.1
> < >= <=	Greater than, less than, greater than or equal to, less than or equal to, for numeric type fields	src_ip:>=100 ; src_ip:(>=10 AND <20)
[] {}	Range query, with brackets [] indicating closed intervals and {} indicating open intervals	src_ip:[1 TO 5}
()	Boolean operations do not follow priority rules. When using multiple operators, use parentheses to specify the priority	src_ip:10.0.0.1 AND (protocol:TCP OR src

- Syntax keywords are case sensitive

Choose Field Match Filter: Click

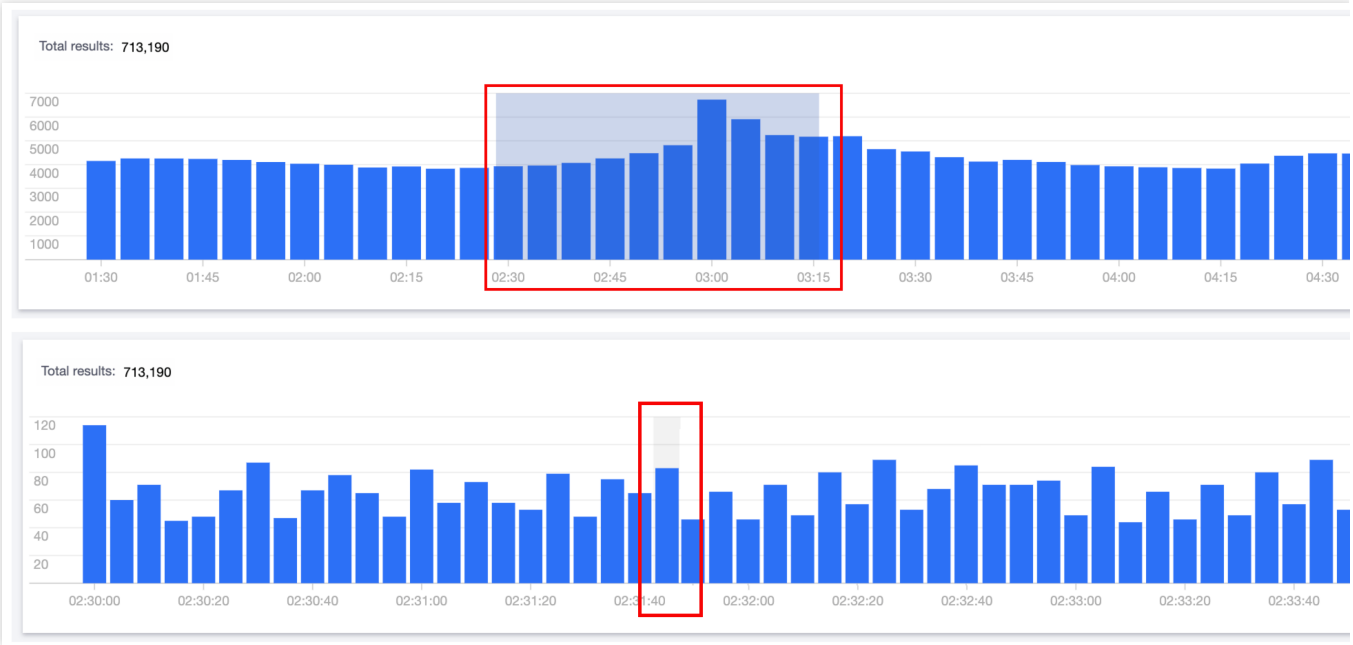
. Choose the appropriate field and operator from the drop-down list. Enter the corresponding field value, and then click **Confirm** to filter.



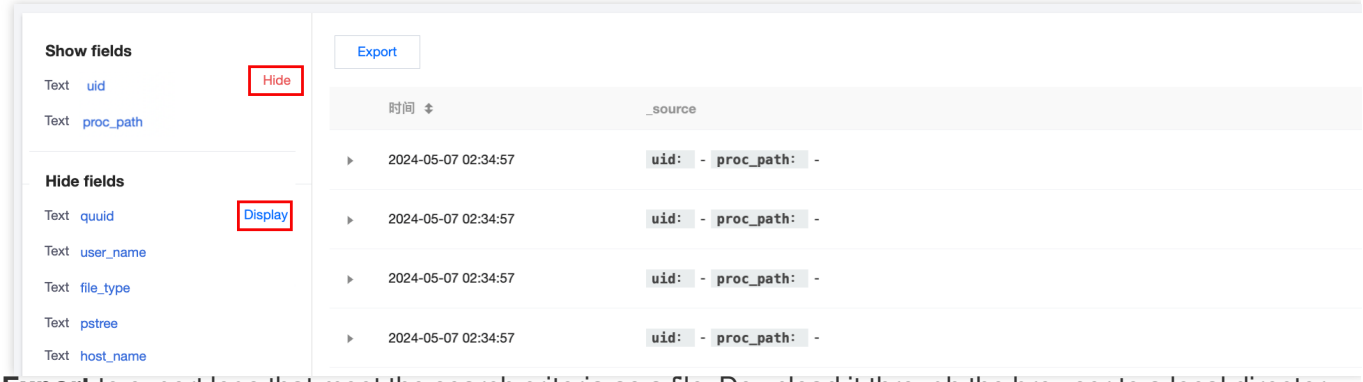
Note:

For commonly used searches, you can **Save Search**. Next time, simply click **Quick Search**, and choose the previously saved search content to filter.

On the log analysis page, click on the bar chart or click and slide to quickly select a time range for a drill-down view.



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. Download it through the browser to a local directory.

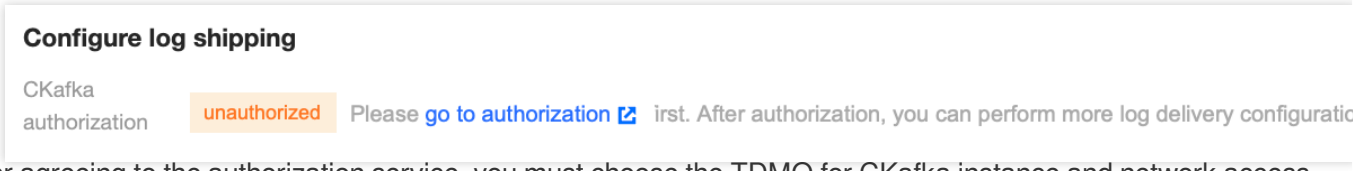
Note:

A single export supports up to 60,000 log records, with a maximum of 10,000 records per log type.

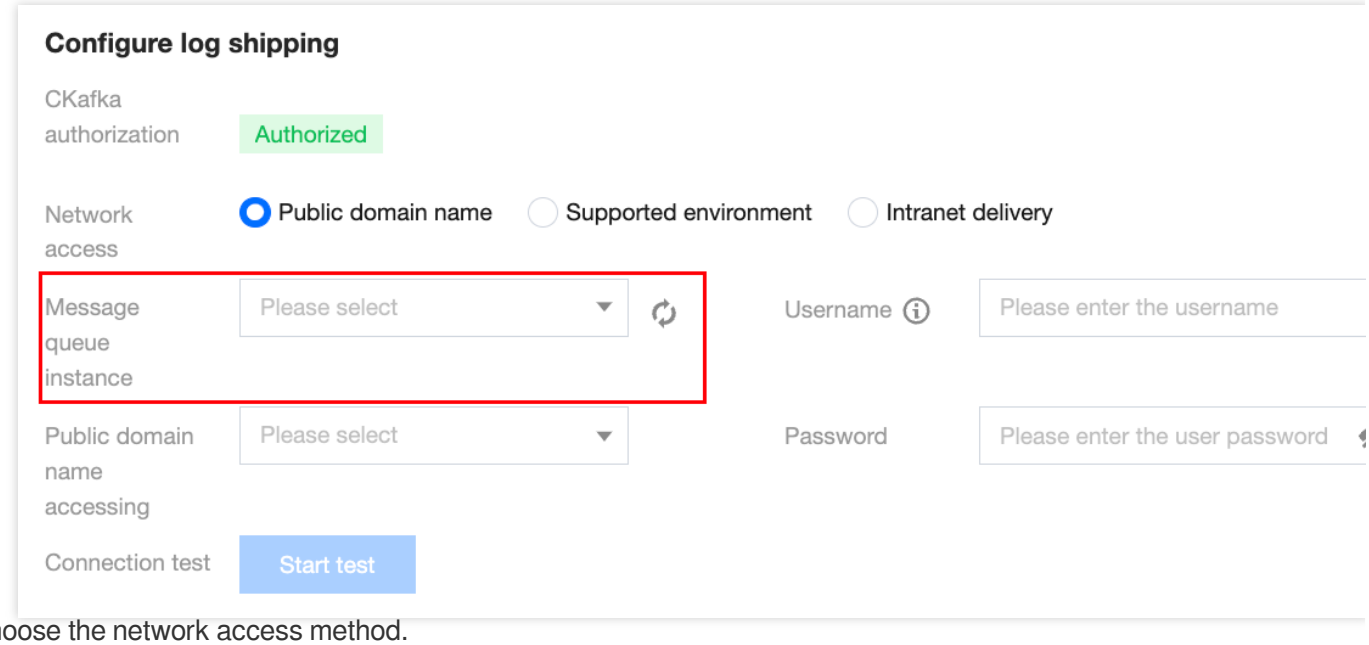
Log Shipping

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

1. Click **Log Shipping** on the top left corner to open the log shipping configuration pop-up. If the CKafka service is not authorized for the first time, click **Go to Authorize** first. After agreeing to the service authorization, you may make more log shipping configurations.



2. After agreeing to the authorization service, you must choose the TDMQ for CKafka instance and network access method. Enter the username and password for the selected TDMQ for CKafka instance, and conduct a connectivity test.

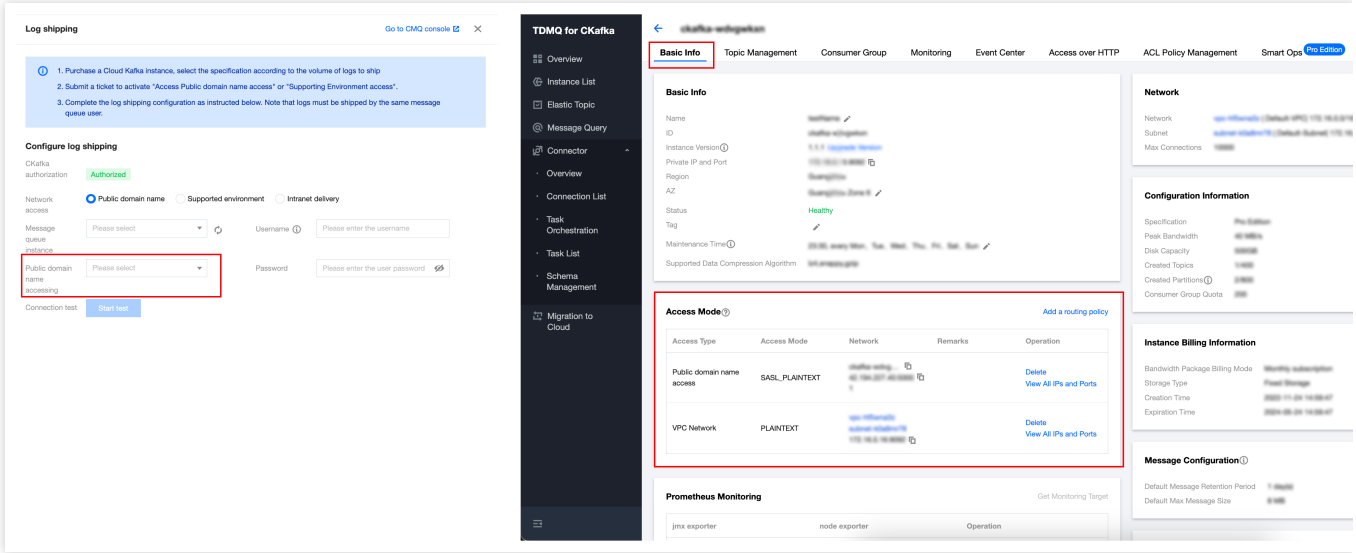


3. Choose the network access method.

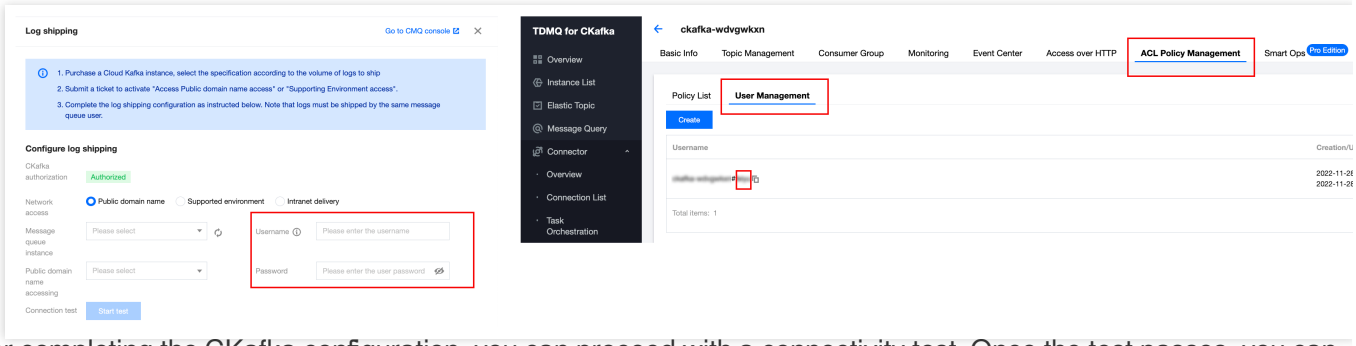
Network Access Method	Description	Optional Routing Instructions
Public domain name access.	Logs are shipped through the public network.	This is the designated access method for TDMQ for CKafka instances.
Supporting environment access.	Logs are shipped through Tencent Cloud's private network. It offers higher performance.	This is the designated access method for TDMQ for CKafka instances. But the PLAINTEXT access method is currently not supported.
Private network shipping.	Logs are shipped through Tencent Cloud's private network without the need for users to configure routing in CKafka. An invisible private network routing is automatically created to support the access.	-

Note:

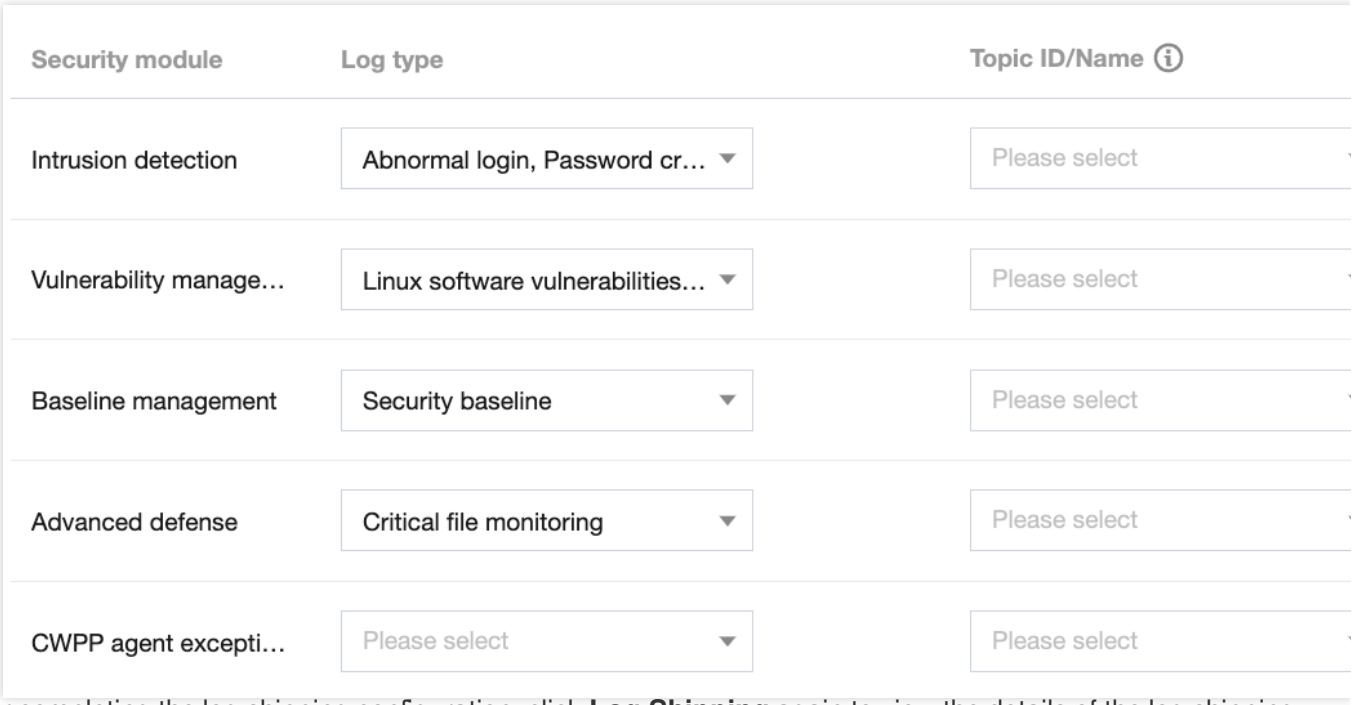
If the network access method is chosen as Public Domain Name Access or Supporting Environment Access, you also need to select an access routing. The routing policy corresponds to the access method detailed in the CKafka Instance List.



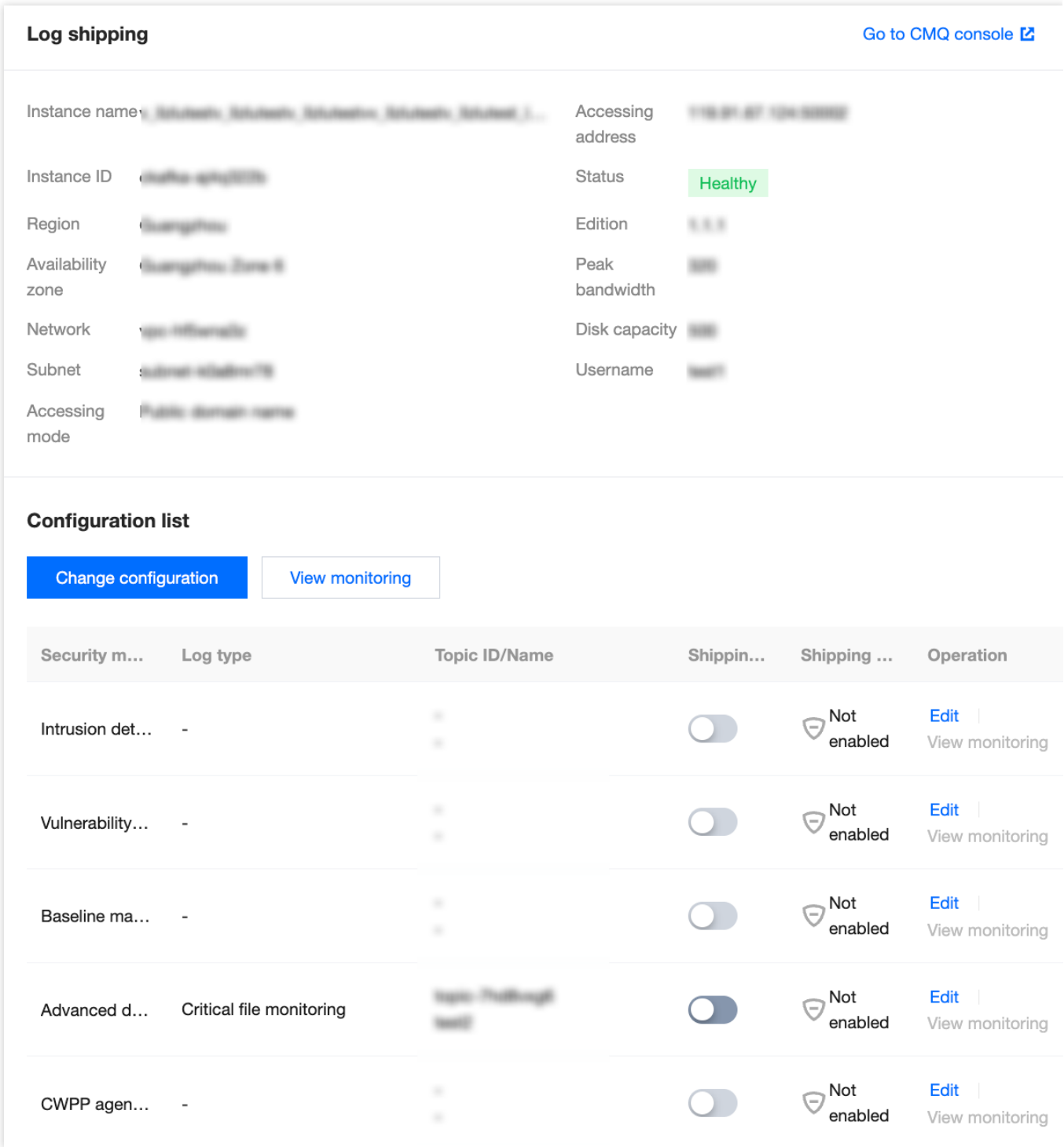
If the network access method is chosen as Public Domain Name Access or Supporting Environment Access, you also need to enter the CKafka instance's username and password. The username and password are listed under **ACL Policy Management** > **User Management** in the CKafka Instance List details. (When configuring log shipping, just enter the username after the # symbol. The CKafka instance ID before the # symbol is not required.)



4. After completing the CKafka configuration, you can proceed with a connectivity test. Once the test passes, you can configure different topics for the logs you want to ship. (for log types not being shipped, choosing a Topic ID is not required).



5. After completing the log shipping configuration, click **Log Shipping** again to view the details of the log shipping.



Basic Information: Displays the basic information of the CKafka instance.

Note:

You need to pay attention to the Status field. If it shows an alarm or abnormality, click **View Monitoring** to check if the CKafka service is abnormal, or if there is insufficient quota.

Shipping Switch: It is used to control a specified log type, and to start or stop log shipping tasks. You can control the log shipping tasks with the switch button in the **Shipping Switch** column.

Shipping Status: normal, abnormal (this status will suspend shipping), and disabled

Edit: Click **Edit** to re-edit the log type and Topic ID for shipping.

View Monitoring: Click **View Monitoring** to navigate to the monitoring page of the TDMQ for CKafka console. In the console, you can view network traffic, peak bandwidth, number of messages, disk occupancy, etc.

Reconfiguration: At the top of the log shipping list, click **Reconfiguration** to return to the state after agreeing to the CKafka authorization service. You can reconfigure the TDMQ for CKafka instance, network access method, log type, Topic ID, etc.

Note:

Reconfiguration will interrupt the current shipping process.

License Management

Last updated：2024-08-13 16:29:50

The protection license provides security protection services based on the CWPP client. You can purchase a protection license and bind it to the host where the client is installed, then the host can receive comprehensive security protection, including intrusion detection, vulnerability management, and baseline management. The protection license has flexible management mechanisms, supporting auto-renewal, auto binding, and auto purchase, thus simplifying the user's protection license management.

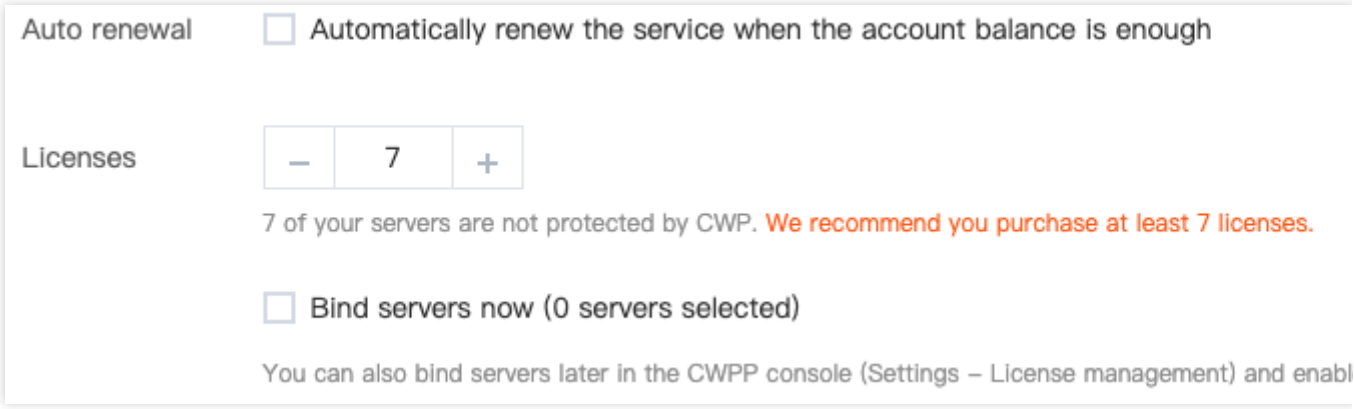
Limits

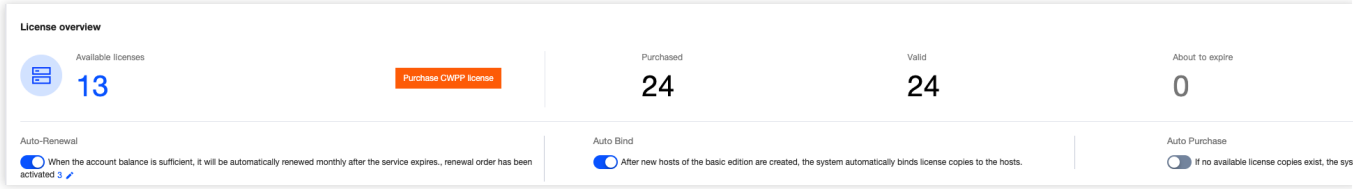
The protection license feature can only be bound to hosts where the CWPP client is installed.
The objects associated with Tencent Cloud tags and projects are security license orders, not the specific licenses or hosts.
Once the auto-backtrace switch in **Add host settings** is enabled, only Ultimate edition hosts support automatically backtracing intrusion alarm data from the past 14 days.
Only the pay-as-you-go license orders for the Pro edition are supported for scaling in and termination.
Note:
Due to the adjustment of the billing mode, CWPP discontinued the pay-as-you-go mode for the Pro edition starting from November 30, 2023. After the adjustment, the new purchase of the Pro edition under the pay-as-you-go mode should no longer be supported. Existing pay-as-you-go orders can still be used normally and allow for scale-out.

Purchasing Protection Licenses

1. Log in to the CWPP console. In the left sidebar, choose **License management**.
2. On the license management page, click **Purchase CWPP license**, go to the CWPP purchase page, and select the protection edition, duration, number of licenses, and bind the hosts. After you have completed the payment, the protection will take effect automatically.

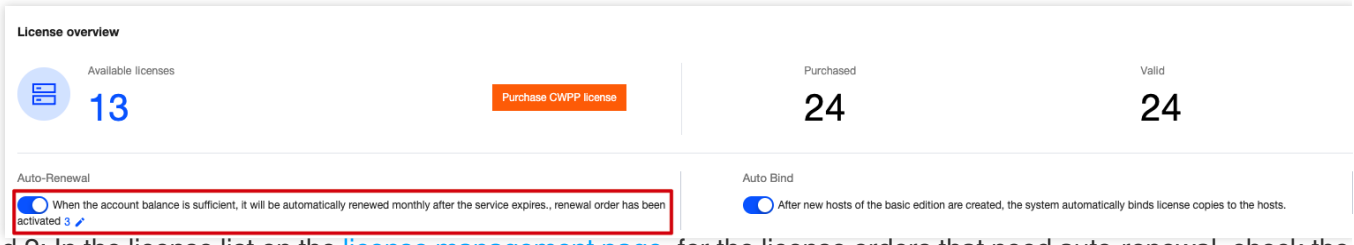
Note:
You can also purchase protection licenses first, and then go to the license management page to bind the hosts.
If you have set the number of protection licenses (as a precondition) on the CWPP purchase page, have checked the options for auto binding or auto purchase, and have successfully completed the payment, this configuration will be synchronized to the license management page.



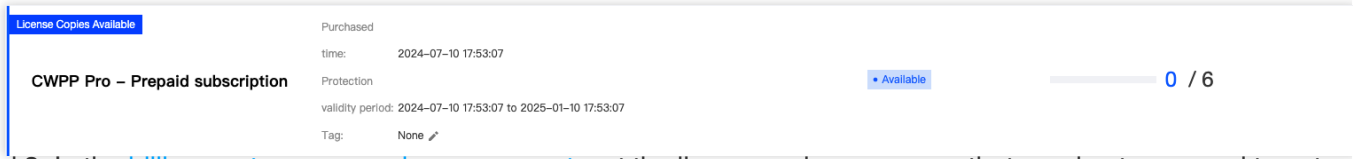


Setting Auto-Renewal

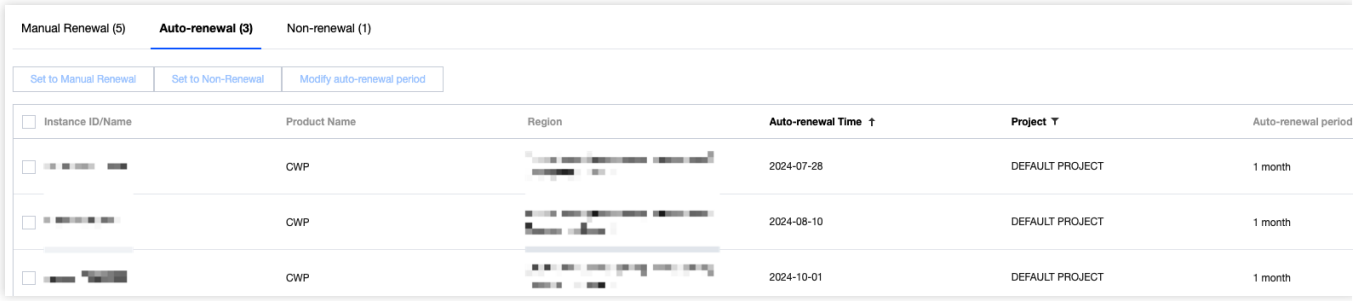
Method 1: On the license management page, check the license orders that need auto-renewal, and turn on the auto-renewal switch.



Method 2: In the license list on the license management page, for the license orders that need auto-renewal, check the auto-renewal option.



Method 3: In the billing center > renewal management, set the license order resources that need auto-renewal to auto-renewal.



Note:

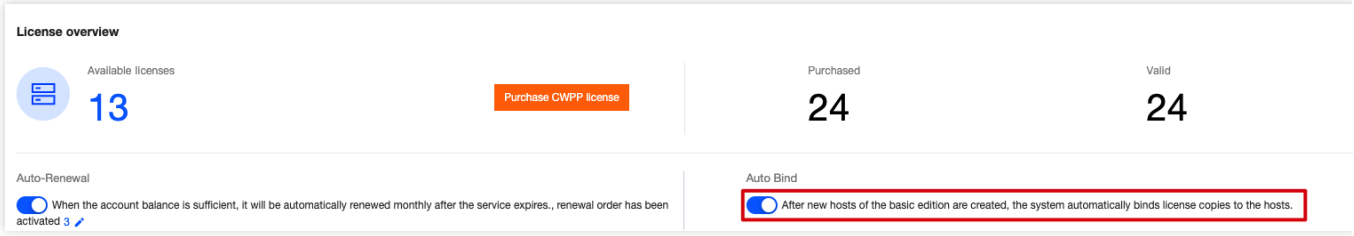
A one-month renewal is set for the three auto-renewal methods above by default. For auto-renewal, the protection edition and the number of licenses will remain consistent with the original order.

If the user modifies the auto-renewal cycle in the billing center > renewal management, the three auto-renewal methods above will follow the user's modified renewal cycle.

Some customers have the privilege of continuous service without interruption upon expiration. If the auto-renewal is disabled, the continuous service privilege for the corresponding license order will become invalid, and the auto-renewal will no longer be performed after expiration.

Setting Auto Bind

On the license management page, click the **Auto Bind** switch to enable it. This allows the system to automatically bind the remaining available licenses when new Basic edition hosts are detected.



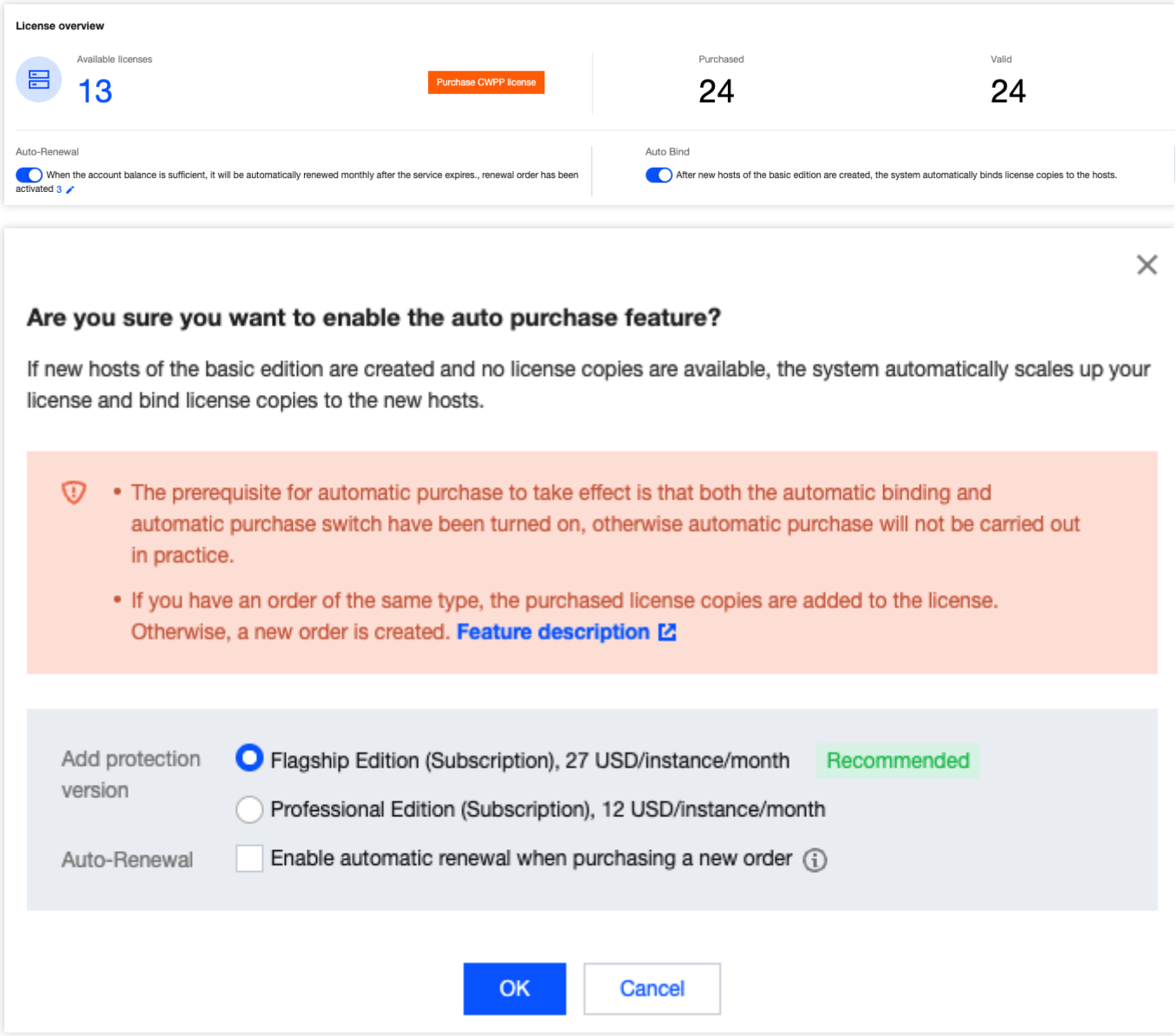
Note:

Add new Basic edition host: Refers to a Basic edition host that has never been bound to a paid edition license (excluding those hosts returned to the Basic edition due to unbinding of a paid edition license).

If there are multiple protection license orders with different editions and durations, the system will prioritize binding the higher edition and the one with the later expiration date.

Setting Auto Purchase

On the license management page, configure the exclusive protection edition. After the **Auto Bind** and **Auto Purchase** switches are enabled, the system will automatically scale out/newly-purchase licenses and bind the new Basic edition hosts when there are no remaining licenses for auto binding.



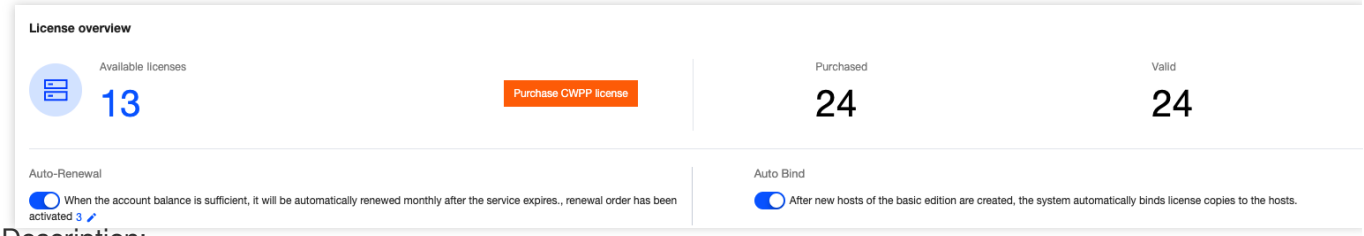
Note:

The auto-purchase will only take effect if both the auto binding and auto purchase switches are enabled. Otherwise, there will be no actual auto purchase.

If there are multiple corresponding edition orders in the license order list for the user's configured exclusive protection edition, the system will prioritize scaling out the license order with the later expiration date. Otherwise, if there are no corresponding edition orders in the license order list, a new license will be purchased, with a default purchase period of 1 month.

Protection License Overview

On the license management page, the license overview displays the number of the licenses which are available , purchased, valid, about to expire, and isolated/expired/invalidated, and provides auto-renewal, auto binding, and auto purchase switch options.



Field Description:

Available Licenses: The total number of unused licenses.

Purchased: The total number of licenses purchased, including valid licenses, those nearing expiration, and those that have expired or been invalidated (records of expired or invalidated licenses that have been deleted are excluded from this count).

Valid: The total number of unexpired licenses.

About to Expire: The total number of licenses expiring within 15 days.

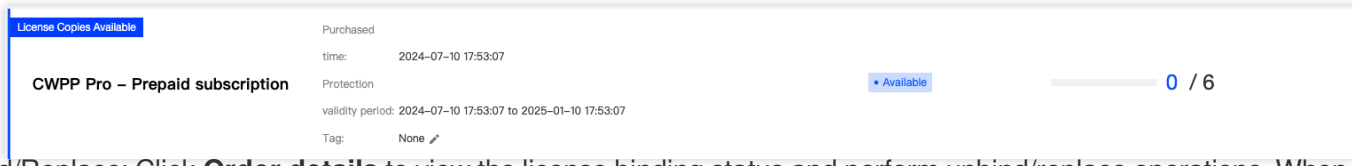
Isolated/Expired/Invalidated: The total number of licenses that have entered isolation, expiration, or invalidation due to the expiration of monthly subscriptions, or overdue payments for pay-as-you-go subscriptions.

Protection License List

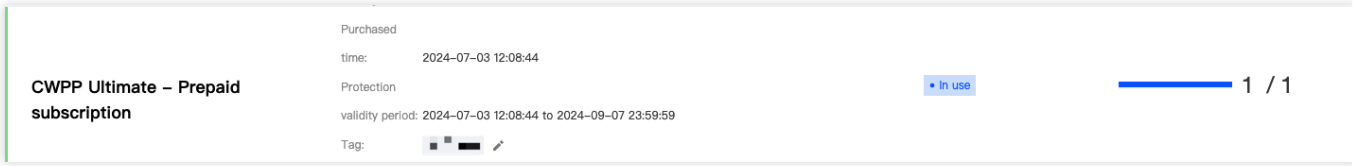
In the license list on the license management page, you can view all purchased license orders. The following operations on licenses are supported.

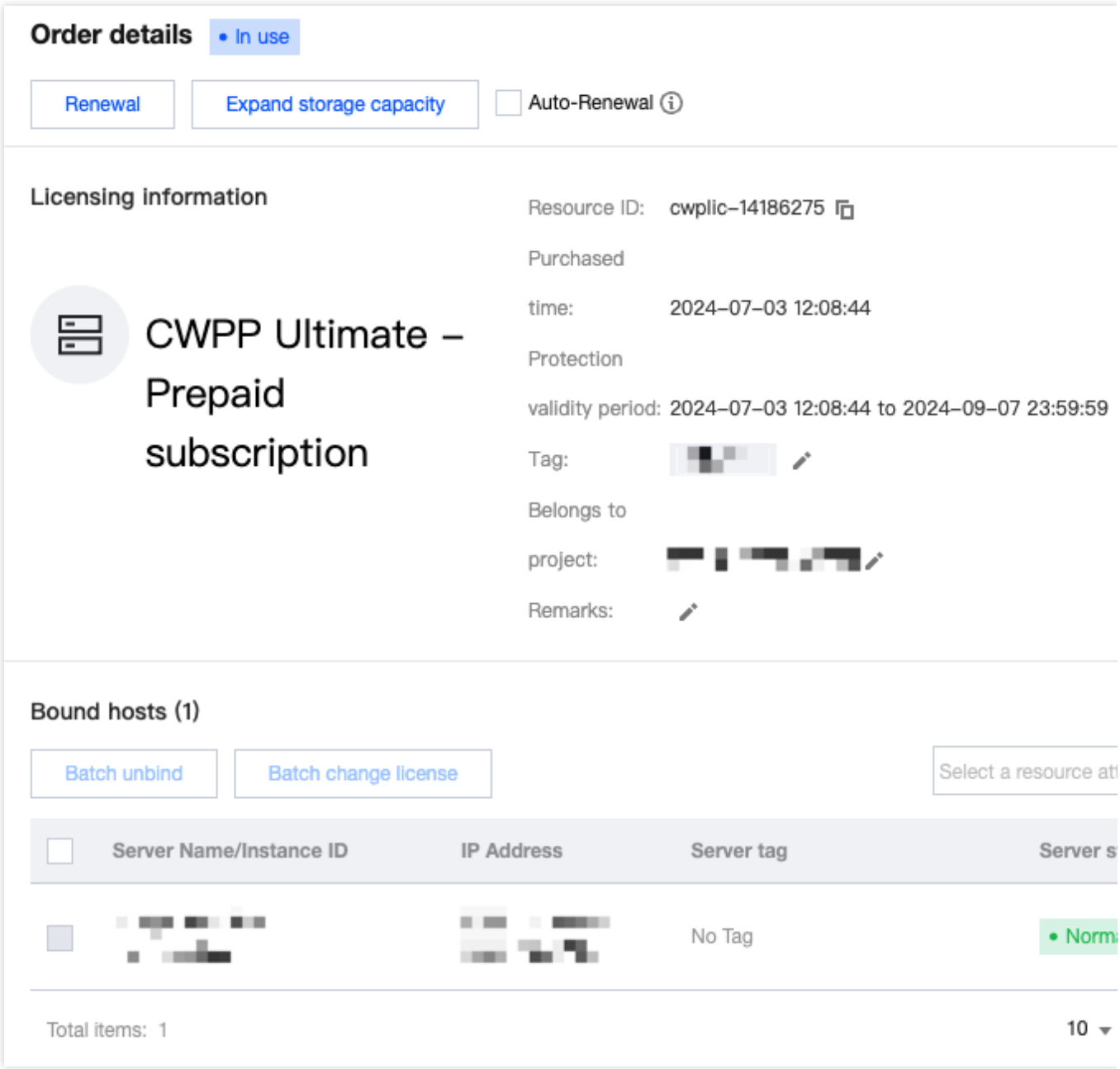
Binding/Unbinding/Replacing Licenses

Bind: Click **Bind servers** to bind the license to a host to obtain the corresponding edition of protection services.



Unbind/Replace: Click **Order details** to view the license binding status and perform unbind/replace operations. When the unbind is performed, the host will downgrade to the Basic edition. When replacing, you can only replace with the same or a higher edition license.



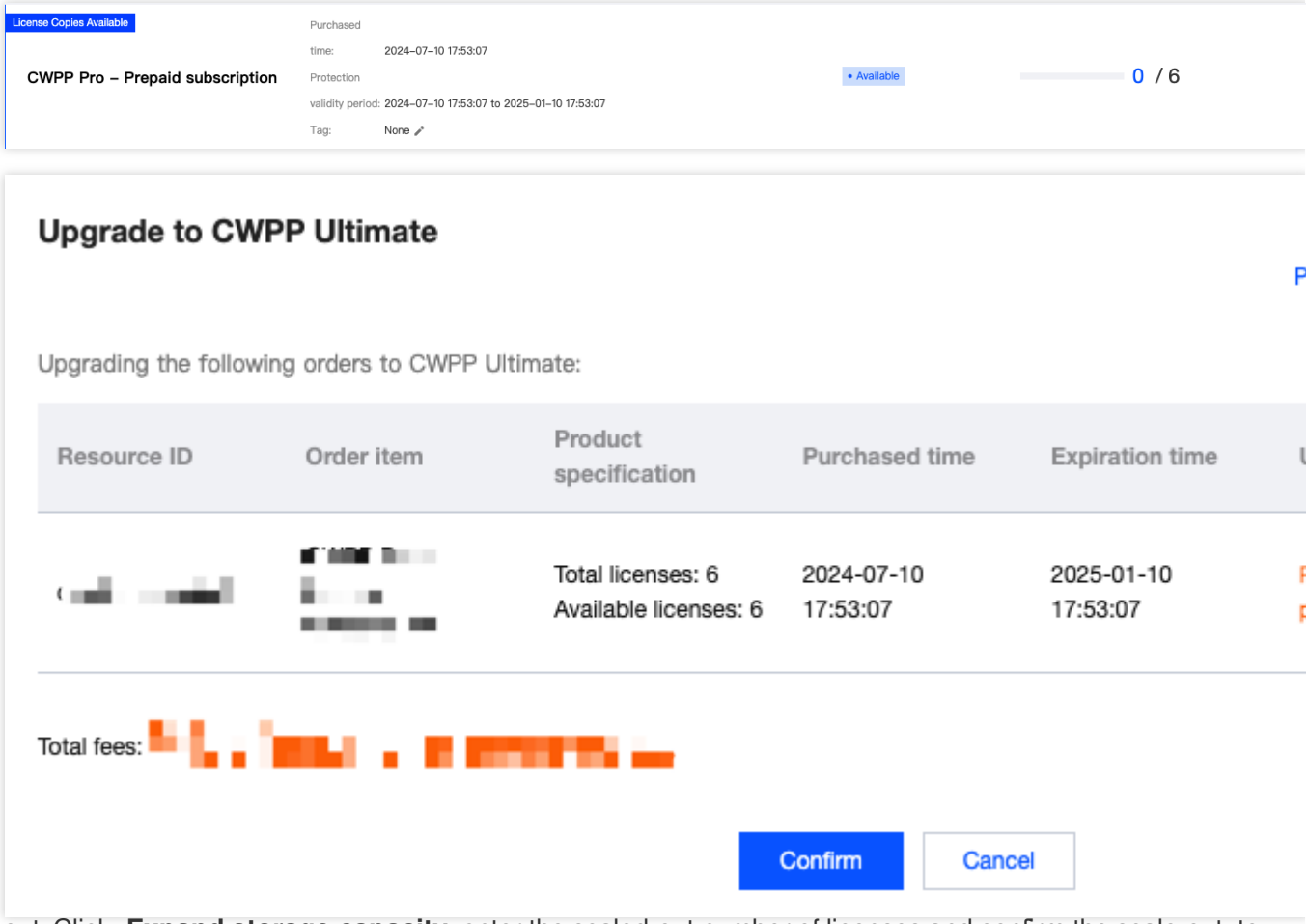


Note:

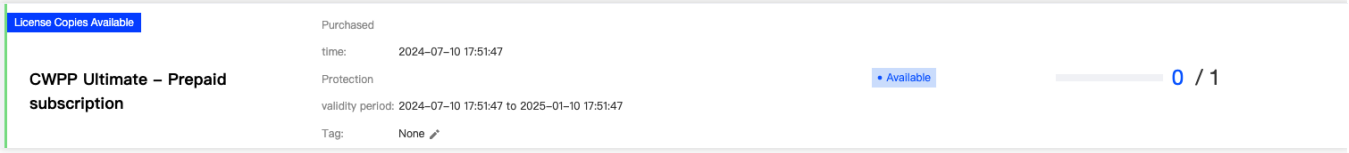
Each month, the total count of unbinds and replacements for each license order is equal to the number of licenses in that order multiplied by 2.

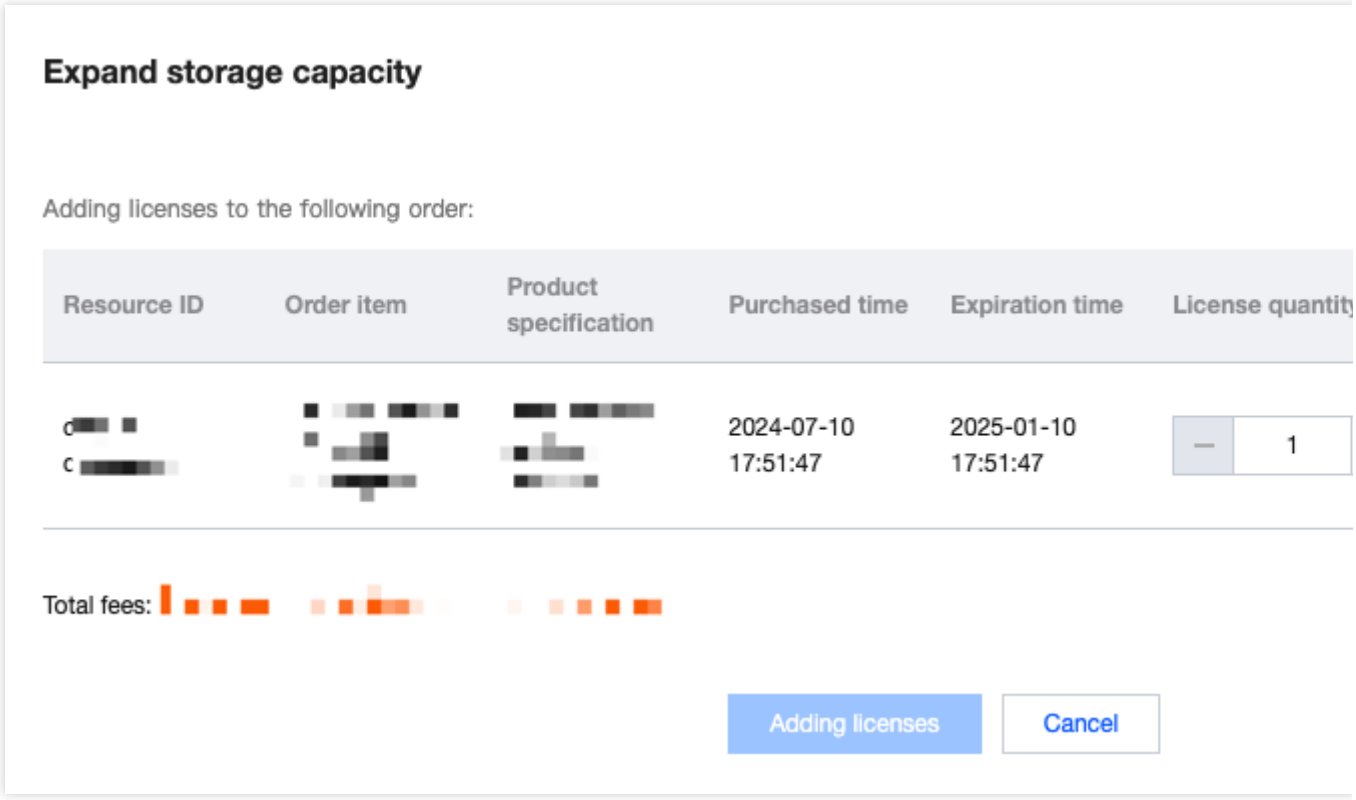
Upgrading/Scaling-out

Upgrade: For Pro edition with monthly subscription license orders, click **Upgrade to CWPP Ultimate** and confirm the upgrade, to upgrade to the Ultimate edition.



Scale-out: Click **Expand storage capacity**, enter the scaled-out number of licenses and confirm the scale-out, to scale out the license order.





Cloud Access Management

Last updated：2024-08-13 16:29:50

Overview

If you have used multiple Tencent Cloud services, which are managed by different users who share your root account key with the highest privilege, the following problems may exist:
Your key is shared by multiple users, so there are huge risks of data breaches.
Your users might introduce security risks from misoperations due to the lack of user access control.
In this case, you can create multiple users in CAM overview to take charge of different services, and give them viewing and operating privileges on different consoles by associating policies. This document provides examples of viewing and operating privileges for CWPP, guiding users on how to use access policies for CWPP.

Examples

Full Access Policy

To grant users full access to all CWPP APIs, you need to associate the policy QcloudCWPPFullAccess with them.
See license management to grant users full access with the preset policy QcloudCWPPFullAccess.

Read-only Policy

To grant users query access to CWPP, without other privileges to add, delete, or modify, you need to associate the policy QcloudCWPPReadOnlyAccess with them. The policy is implemented by granting users access privileges to APIs prefixed with Describe, Get, Check, and Export.
See license management to grant users read-only access with the preset policy QcloudCWPPReadOnlyAccess.

Custom Policies

If the preset policies cannot meet your needs, you can achieve your goal by creating custom policies.

Note:
New users will not be associated with any CWPP policies by default, indicating they do not have any privileges. For more information, see user guide for CAM.

Hybrid Cloud Installation Guide

Overview

Last updated：2024-08-13 16:29:50

Overview

With the increasing rate of cloud adoption, more and more medium and large-scale enterprises are selecting the hybrid cloud model of combining public cloud with private cloud. This model combines the benefits of public cloud, such as low costs, agility, flexibility, and ease of use, with those of private cloud, including controllability, security, and high availability for deployments. The hybrid cloud management feature supports the connection to non-Tencent Cloud machines, helping users better manage and monitor CWPP.

Feature Overview

The automatic connection of Tencent Cloud's ECM and Lighthouse to CWPP is supported.
The manual connection of non-Tencent CVMs, such as Private Cloud, Alibaba Cloud, Huawei Cloud, QingCloud, Amazon Web Services (AWS), and UCloud, to CWPP is supported.

Supported Client Version

Linux System Supported Versions

RHEL: Versions 6.1+ (64 bit)
CentOS: Versions 6.3+ (64 bit)
Ubuntu: 9.10+ (64 bit)
Debian: 6+ (64 bit)

Windows System Supported Versions

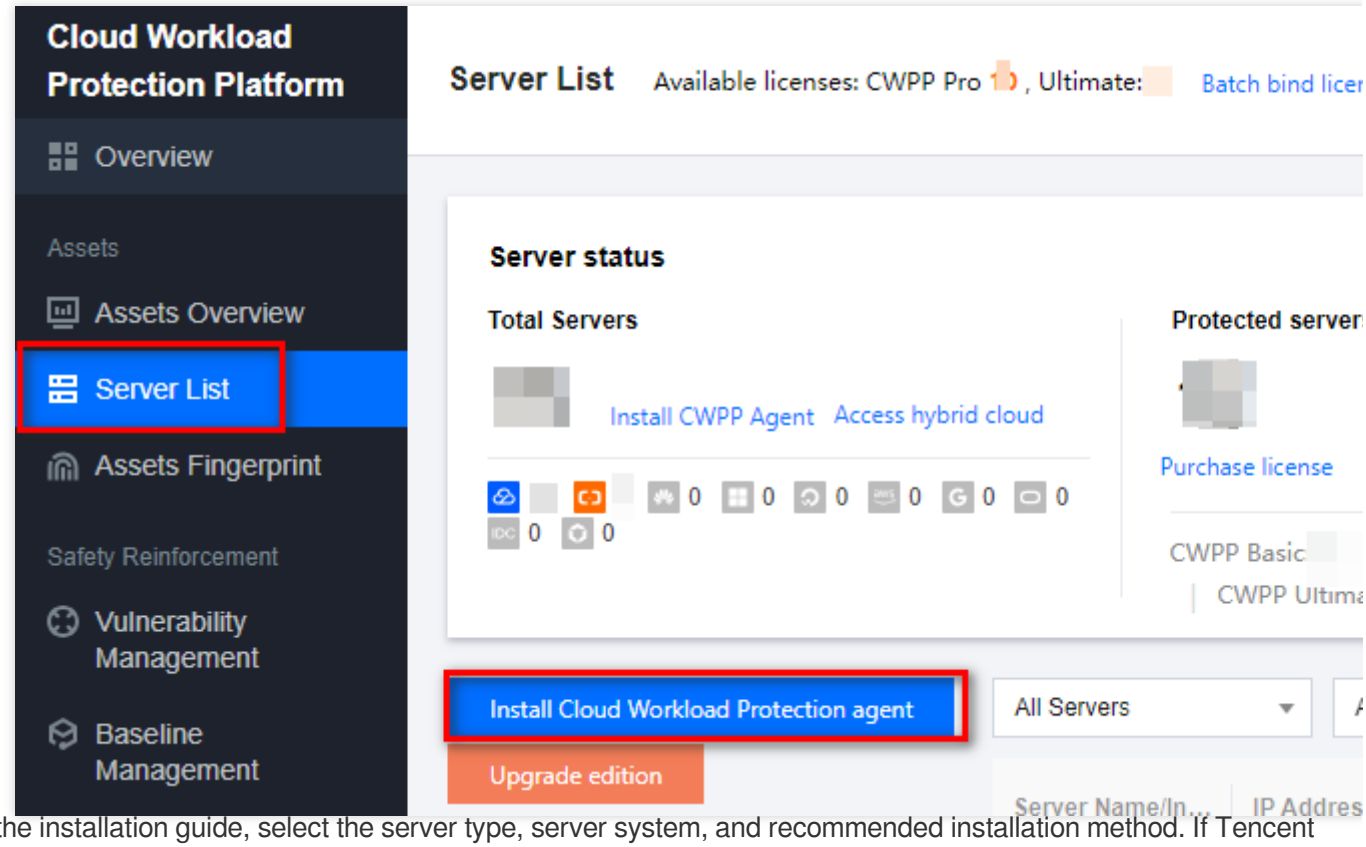
Windows server 2012, 2016, and 2019
Windows server 2008+ R2
Windows server 2003 (limited support)

Configuration of Non-Tencent Cloud Machines

Last updated：2024-08-13 16:29:50

Step 1: Installing the CWPP Agent

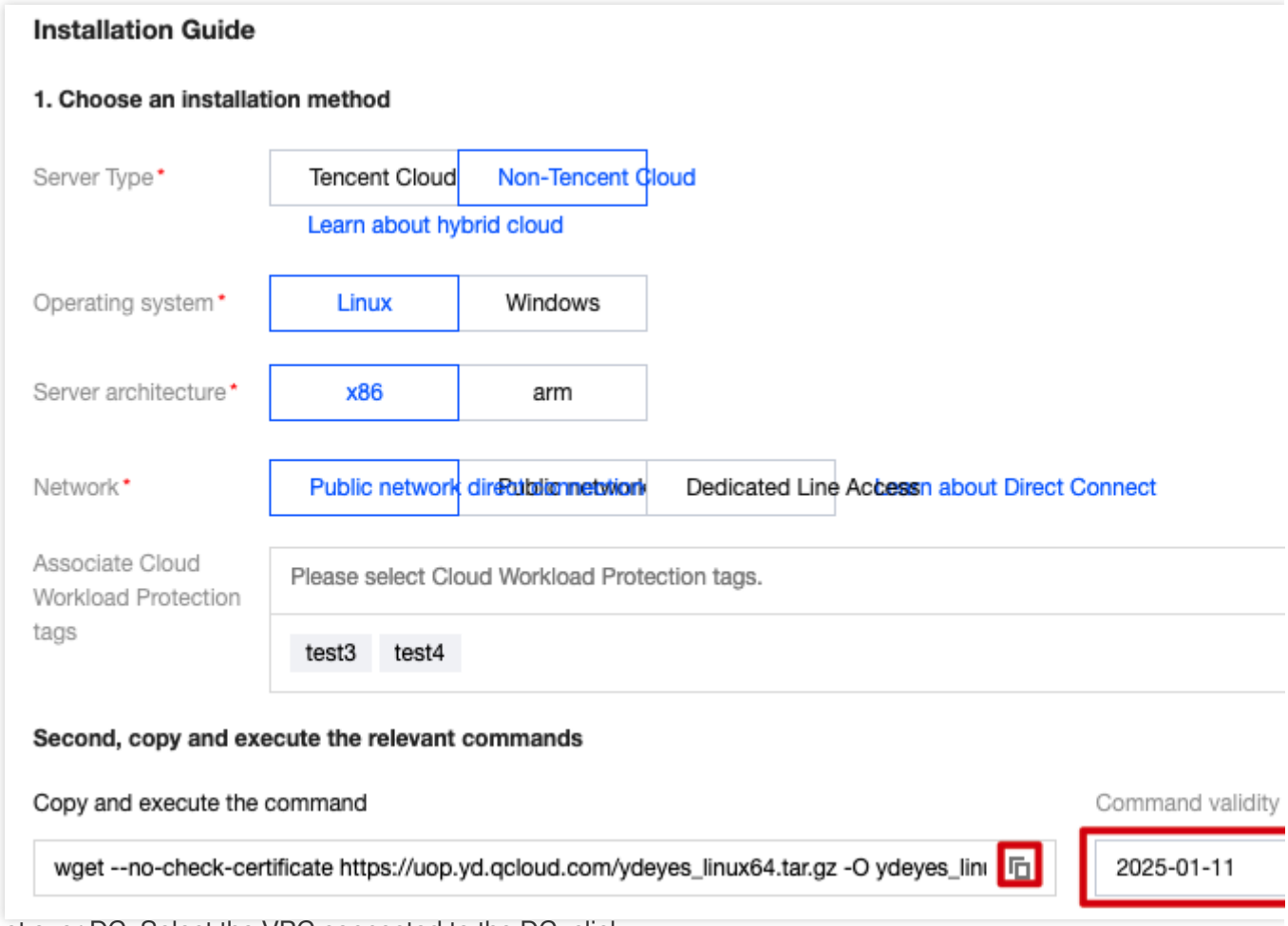
1. Log in to the CWPP console. In the left sidebar, click **Server List** > **Install Cloud Workload Protection agent**, and view the installation guide details in the pop-up window on the right.



2. In the installation guide, select the server type, server system, and recommended installation method. If Tencent Cloud and Non-Tencent Cloud are connected through DC, select the DC installation method, otherwise select the public network installation method.

Connect over the Public Network: Click

to copy and run the corresponding command to install the CWPP client. **Pay attention to the command validity**.



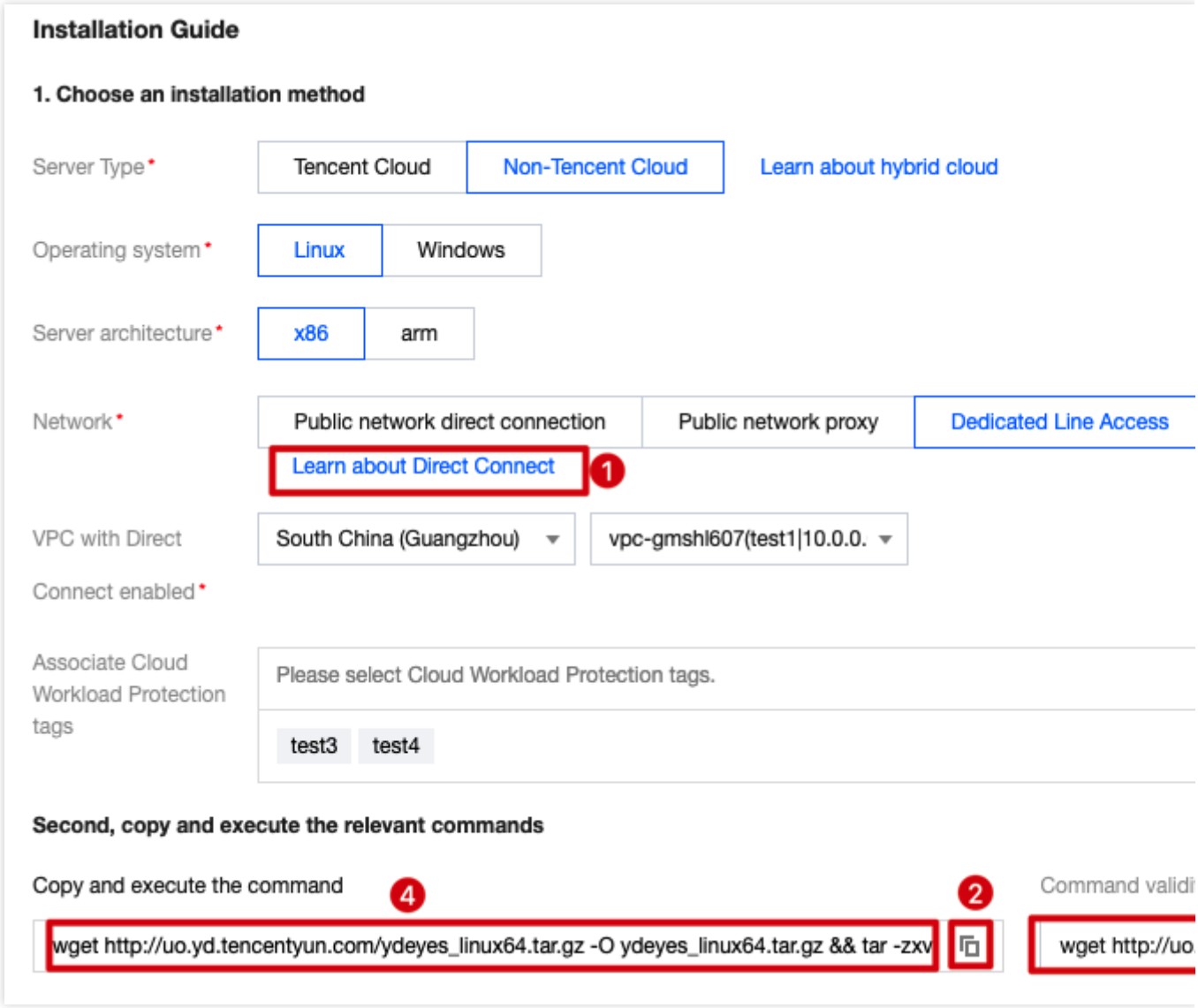
Connect over DC: Select the VPC connected to the DC, click

to copy and run the corresponding command to install the CWPP client. **Pay attention to the command validity**.

Note:

For more information on DC, click **Learn about Direct Connect** to go to the DC console.

To allow the target IP in the firewall, grant the permission as instructed by ④ in the image.



Step 2. Checking Whether the Installation Is Successful

1. Follow the installation guide to execute the command for verifying the installation success.

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 no process is 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.

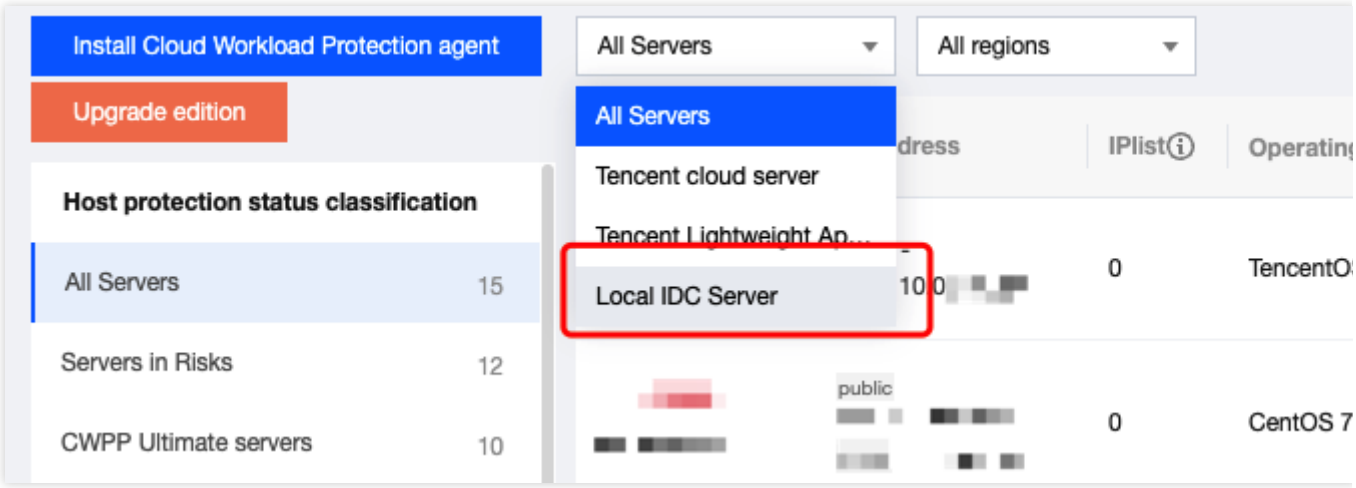
If no process is running, you can manually start the service through the task manager.

2. After successful installation, on the host list page, click **ALL Servers** > **Local IDC**** Server** to view the corresponding server.

Note:

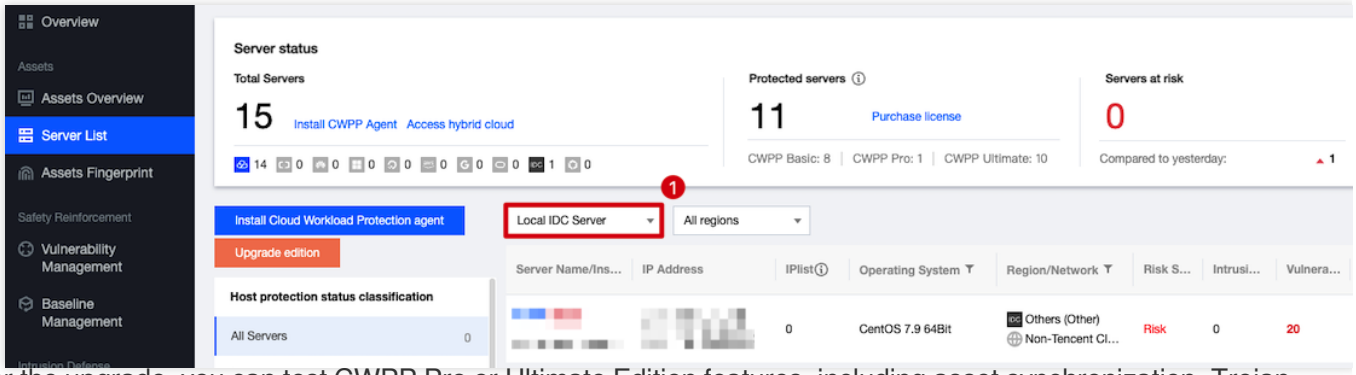
To check if the service is launched, first ensure the client is successfully installed, then verify in the host list. If the server status is Protecting, the service is launched.

If it is not launched, you can contact us for support.



Step 3: Upgrading CWPP Editions

1. Click to select **Local IDC Server** to view the corresponding server, then click **License management** to enter the license management page and upgrade to CWPP **Pro or Ultimate Edition**.



2. After the upgrade, you can test CWPP Pro or Ultimate Edition features, including asset synchronization, Trojan scan, vulnerability scan, abnormal log-ins, password cracking (interception is not supported in a non-Tencent Cloud environment), reverse shell, local privilege escalation, high risk commands, and malicious requests.

Connection to a VPC over DC

Last updated：2024-08-13 16:29:50

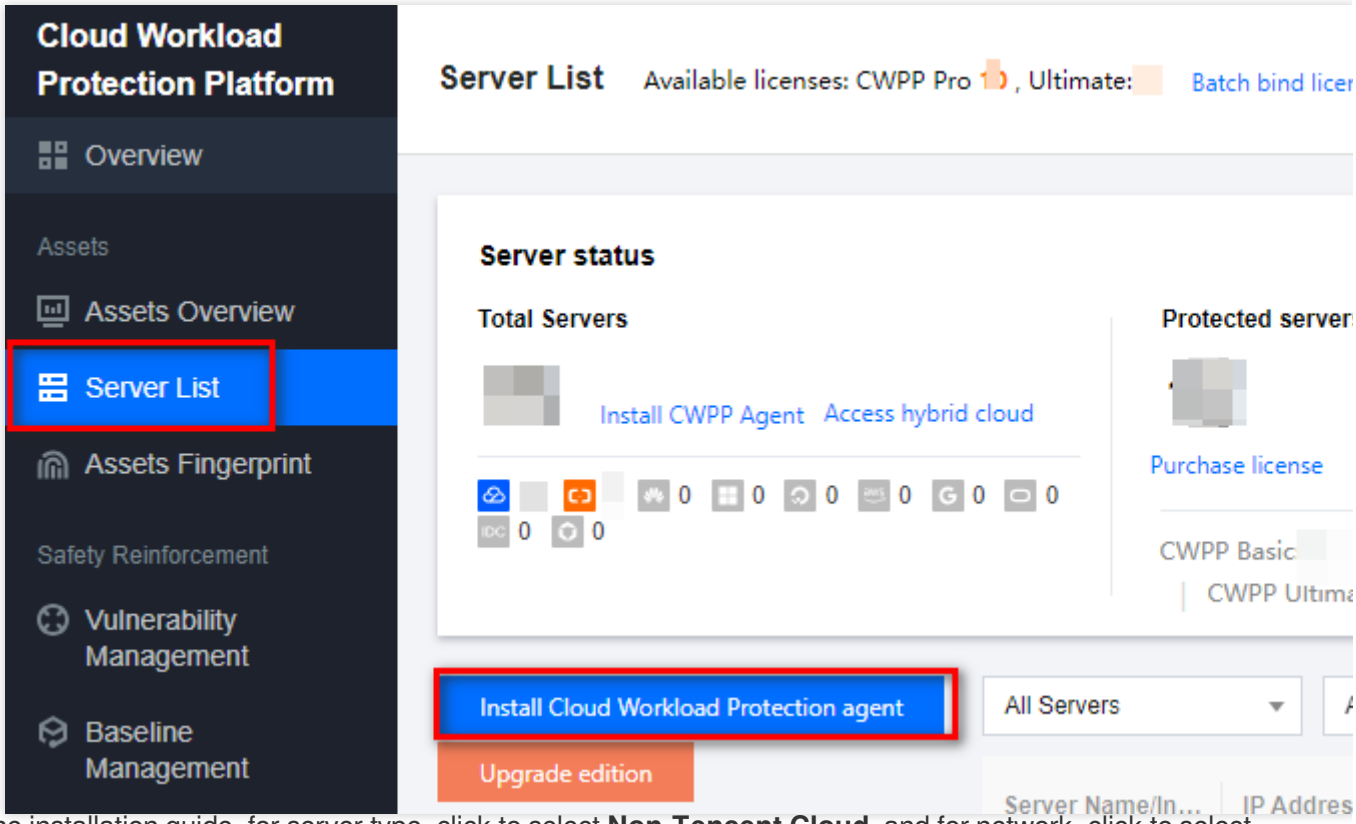
Overview

Currently, the connection to a VPC over DC is only supported in South China (Guangzhou), North China (Beijing), East China (Shanghai, Shanghai Finance, and Nanjing), and Southwest China (Chengdu). The public cloud can already communicate with the customer's data center network over a VPC, and the client can be directly installed.
If the region you need to connect is not supported by the connection to a VPC over DC, you need to use CCN to connect the DC gateway (VPN) with the VPC. You need to purchase the DC gateway and set the connection to a VPC over DC.

Operation Guide

Step 1. Checking Whether CCN Is Required for Connection

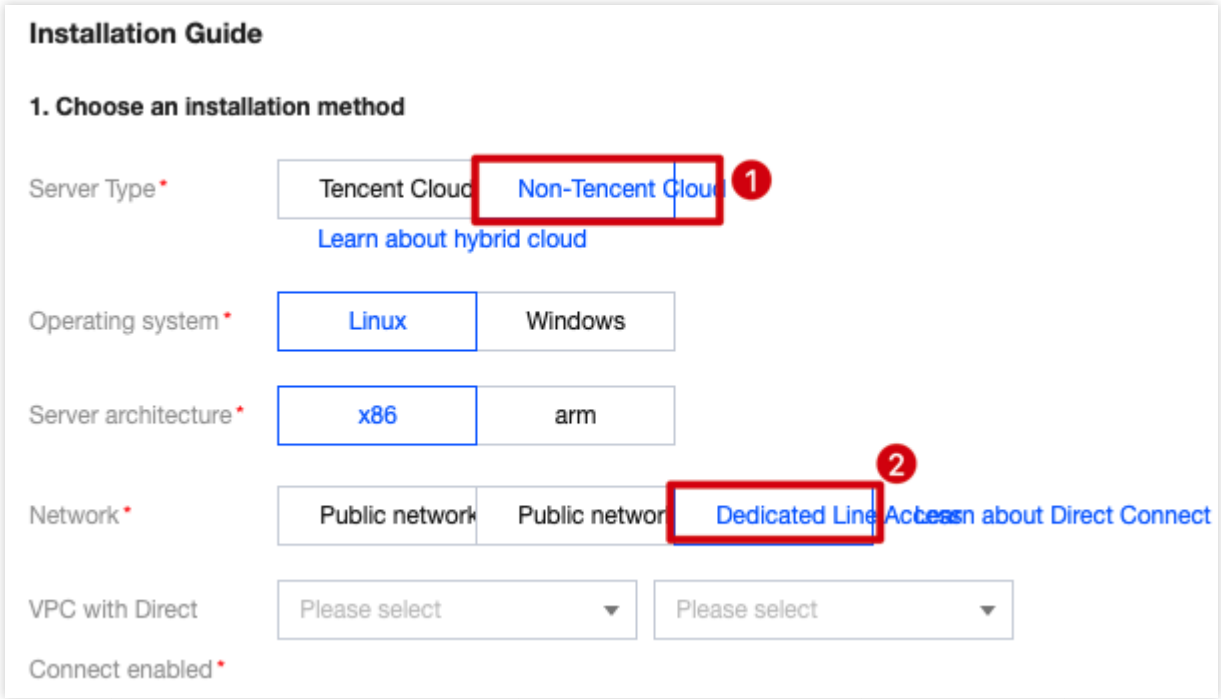
1. Log in to the CWPP console. In the left sidebar, click **Server List** > **Install Cloud Workload Protection agent**, and view the installation guide details in the pop-up window on the right.



2. In the installation guide, for server type, click to select **Non-Tencent Cloud**, and for network, click to select **Dedicated Line Access**.

Note:

Select the appropriate Linux or Windows operating system according to the user's operating system.

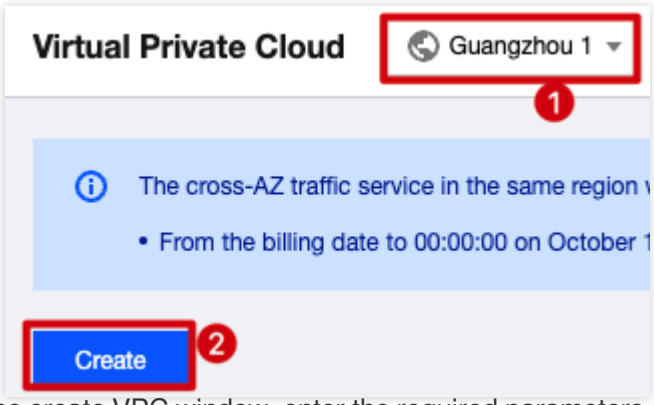


3. If you are in South China (Guangzhou), North China (Beijing), East China (Shanghai), East China (Shanghai Finance), East China (Nanjing), or Southwest China (Chengdu):

If you have a VPC connected to the non-Tencent Cloud data center network, select the VPC connected to DC and run the installation command.
If no corresponding VPC network is found to interconnect with your non-Tencent Cloud data center network, you can connect through CCN. See Step 2.

Step 2. Confirming the VPC for Connection to DC

1. If you do not have a VPC network in the 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, and click **VPC** to enter the VPC page.
2. On the VPC page, click the drop-down box to select the required region, and click **Create** to pop up the create VPC window.



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

Step 3: Using CCN to Interconnect the VPC with the Non-Tencent Cloud Data Center Network Connected by a DC

1. If a CCN that communicates with the non-Tencent Cloud data center already exists, add the VPC instance selected in Step 2 to the CCN.
a. Log in to the VPC console. In the left sidebar, click **CCN** to go to the CCN page.
b. On the CCN page, click **Manage Instances**> **Associate Instances** in the right to go to the associate instances page.
c. On the associate instances page, click **Newly Added Instances** to add the VPC instance selected in Step 2 to the CCN, and then click **Confirm** to complete the association.
2. If the CCN is not yet configured, create one.
a. Log in to the VPC console. In the left sidebar, click **CCN** to go to the CCN page.
b. On the CCN page, click **New**, and a new CCN instance pop-up window appears.
c. In the new CCN instance pop-up window, enter the required parameters and click **Confirm** to complete the creation of a new CCN instance.

Note

DC gateway: Select the DC 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 or create a new VPC instance that does not conflict.
3. Go back to the CWPP console and see Step 1 to obtain the installation command. Your non-Tencent Cloud data center needs to allow access to four ports (5574, 8080, 80, and 9080) of the IP described in Step 1.

FAQs

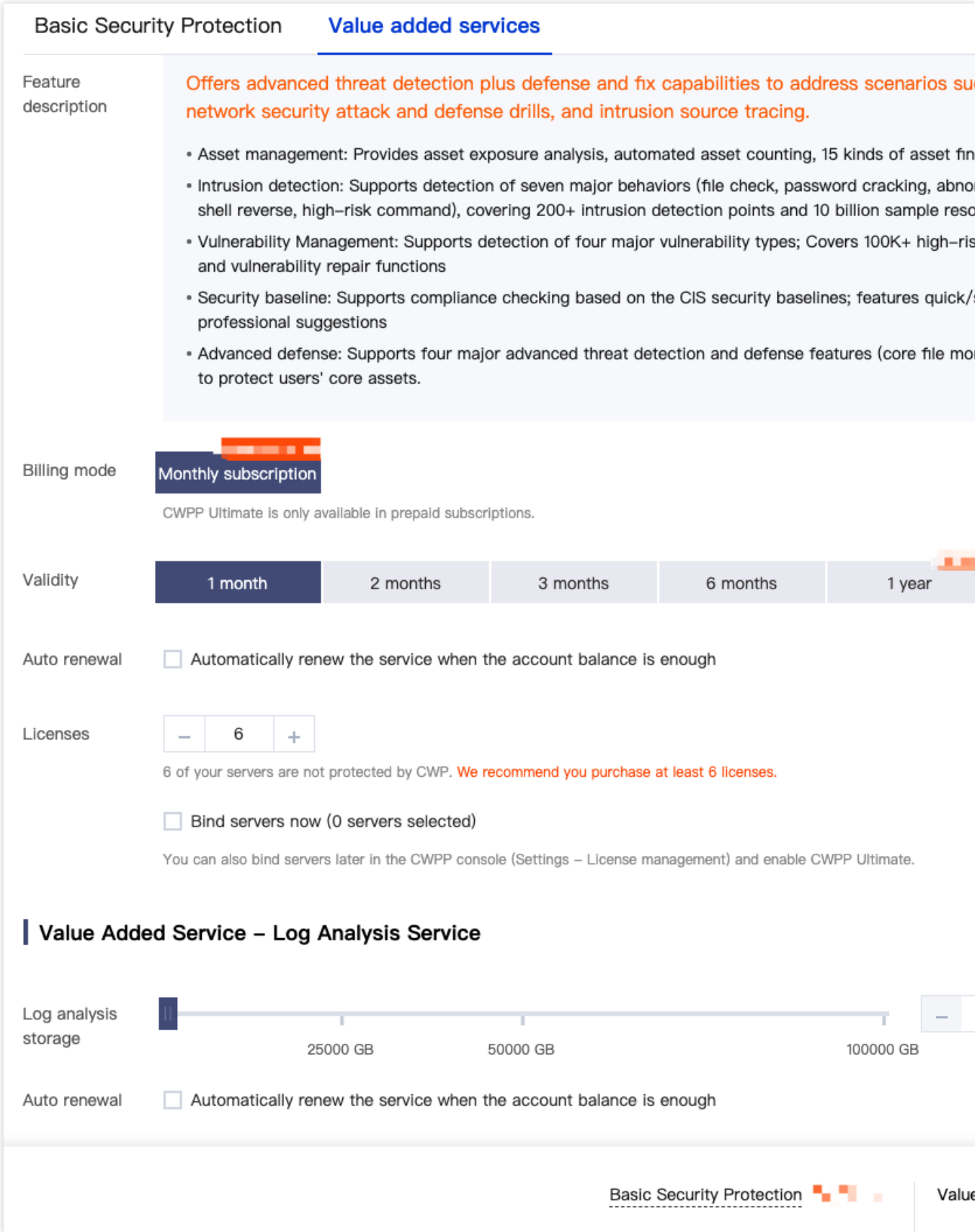
Last updated：2024-08-13 16:29:50

Does Hybrid Cloud Have Version Requirements for CWPP?

Yes, only **Pro Edition or Ultimate Edition** supports hybrid cloud features.

How to Upgrade CWPP to Pro Edition or Ultimate Edition?

1. Log in to the CWPP console. In the left sidebar, choose **License management** > **Purchase Cwpp license** to enter the purchase page.
2. On the purchase page, you can enter the number of licenses to be purchased (Pro edition or Ultimate edition). After selection according to your needs, click **Buy Now**. Once the purchase is successful, go to the license management page to bind the licenses to the servers that need protection. For details on the license operations, see license management.

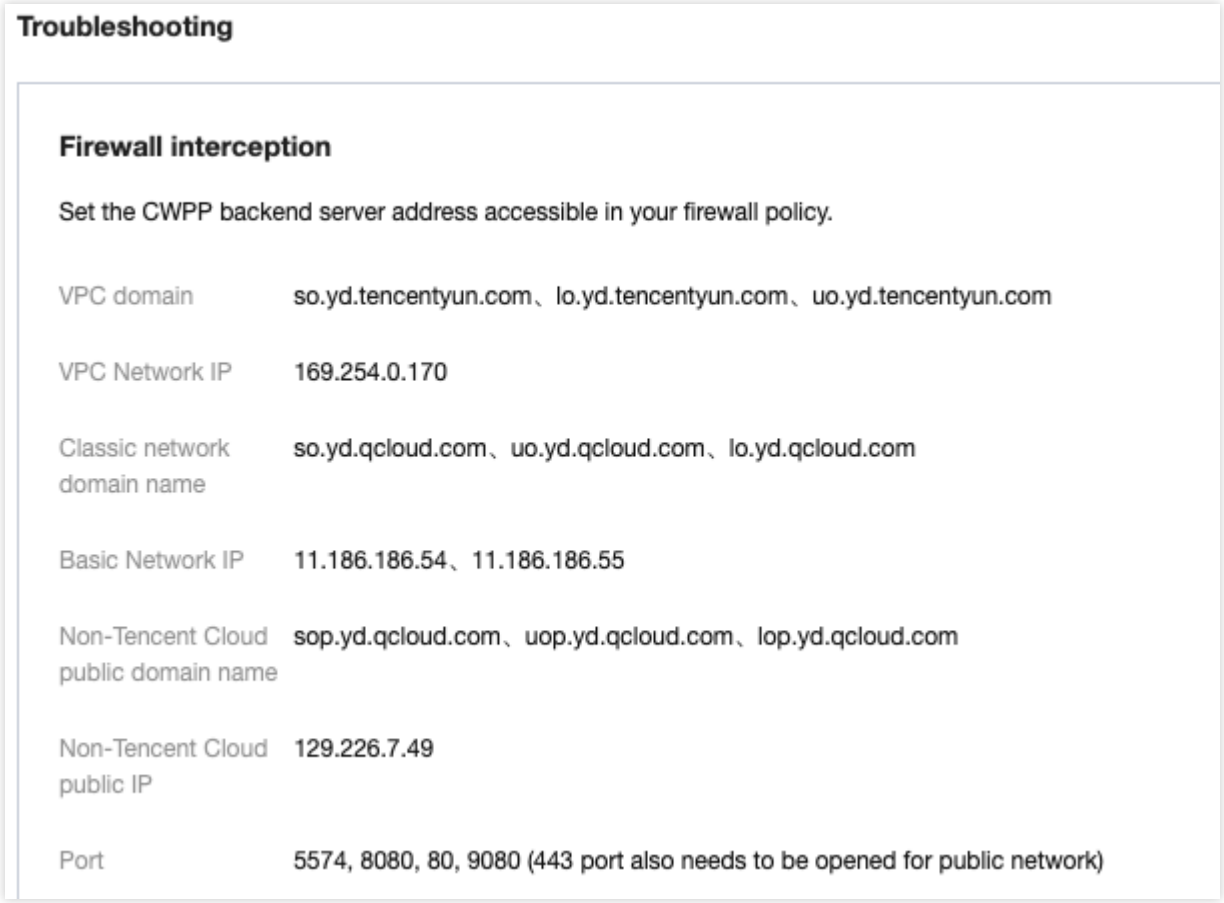


What Are the Target Address and Open Ports for the Cloud Connection over DC?

See the target address and open ports as shown below, and configure the firewall to allow traffic through.

Note:

The address and open ports do not change.



Is the Installation of Agents Supported in IDCs Outside Mainland China?

It is supported. As long as the machine can connect to the network and the system meets the requirements, you can install the CWPP agent.

When Will the Non-Tencent Cloud Instance Be Displayed in the Console After the Agent Is Installed?

Currently, it is displayed in seconds.

Do I Need to Purchase the Console if I Use a Non-Tencent Cloud Instance?

No. The management and billing take place in the public cloud console.

Network Port Access from IDC to the Cloud Is Needed to Open. What Are the Target IP and Ports?

The target IP is included in the installation command, and the ports are 5574, 80, 8080, and 9080.

Can I Use CWPP if the Private Network Machine Cannot Access the Public Network or There Is No DC?

Currently, no.

Does the Hybrid Cloud Client Conflict with the Zabbix Process?

We have not made any special configurations for Zabbix or performed injections. Check for other client installations or drivers on the instance.

FAQs for Beginners

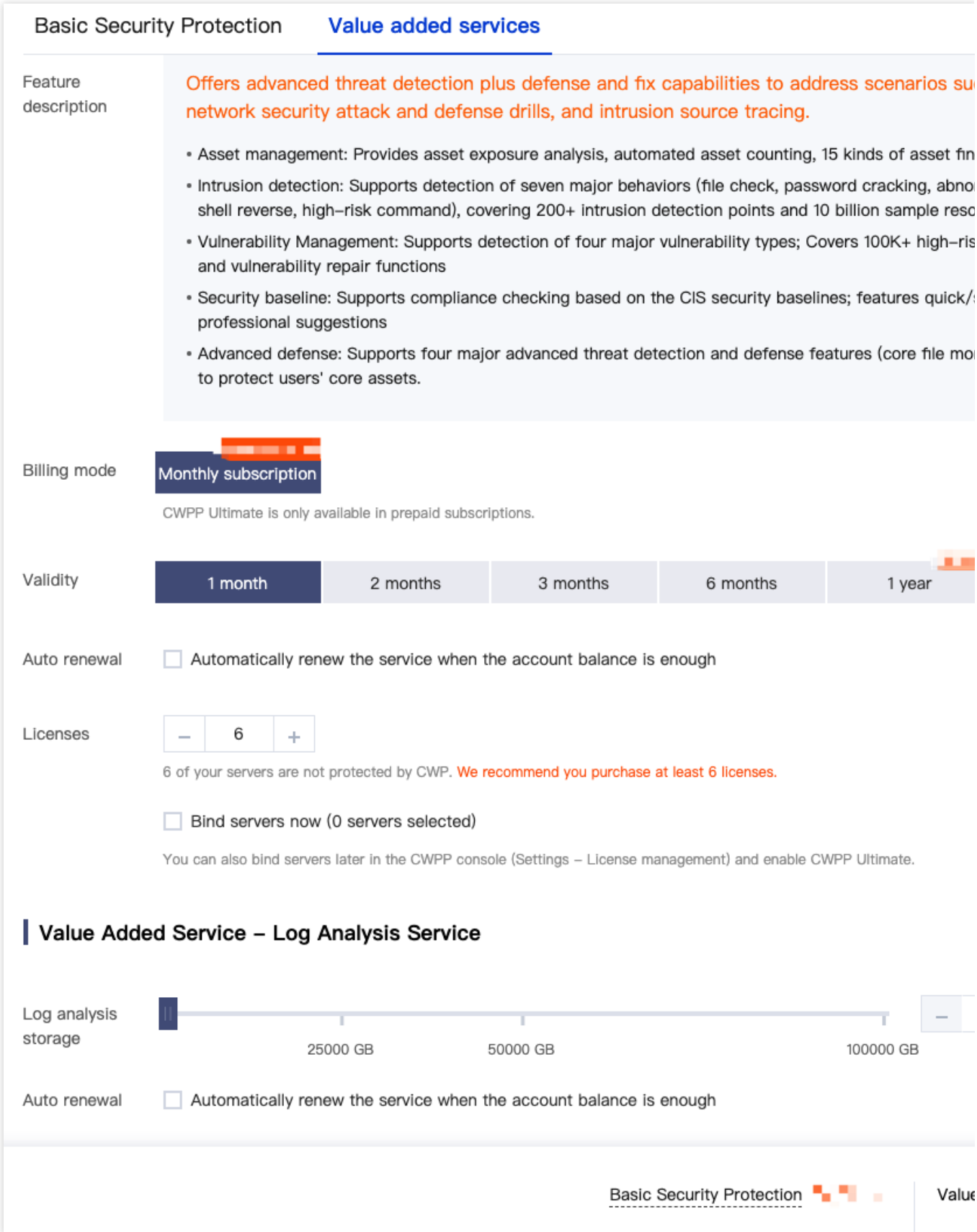
Last updated：2024-08-13 16:29:50

Does Hybrid Cloud Have Version Requirements for CWPP?

Yes, only **Pro Edition or Ultimate Edition** supports hybrid cloud features.

How to Upgrade CWPP to Pro Edition or Ultimate Edition?

1. Log in to the CWPP console. In the left sidebar, choose **License management** > **Purchase Cwpp license** to enter the purchase page.
2. On the purchase page, you can enter the number of licenses to be purchased (Pro edition or Ultimate edition). After selection according to your needs, click **Buy Now**. Once the purchase is successful, go to the license management page to bind the licenses to the servers that need protection. For details on the license operations, see license management.

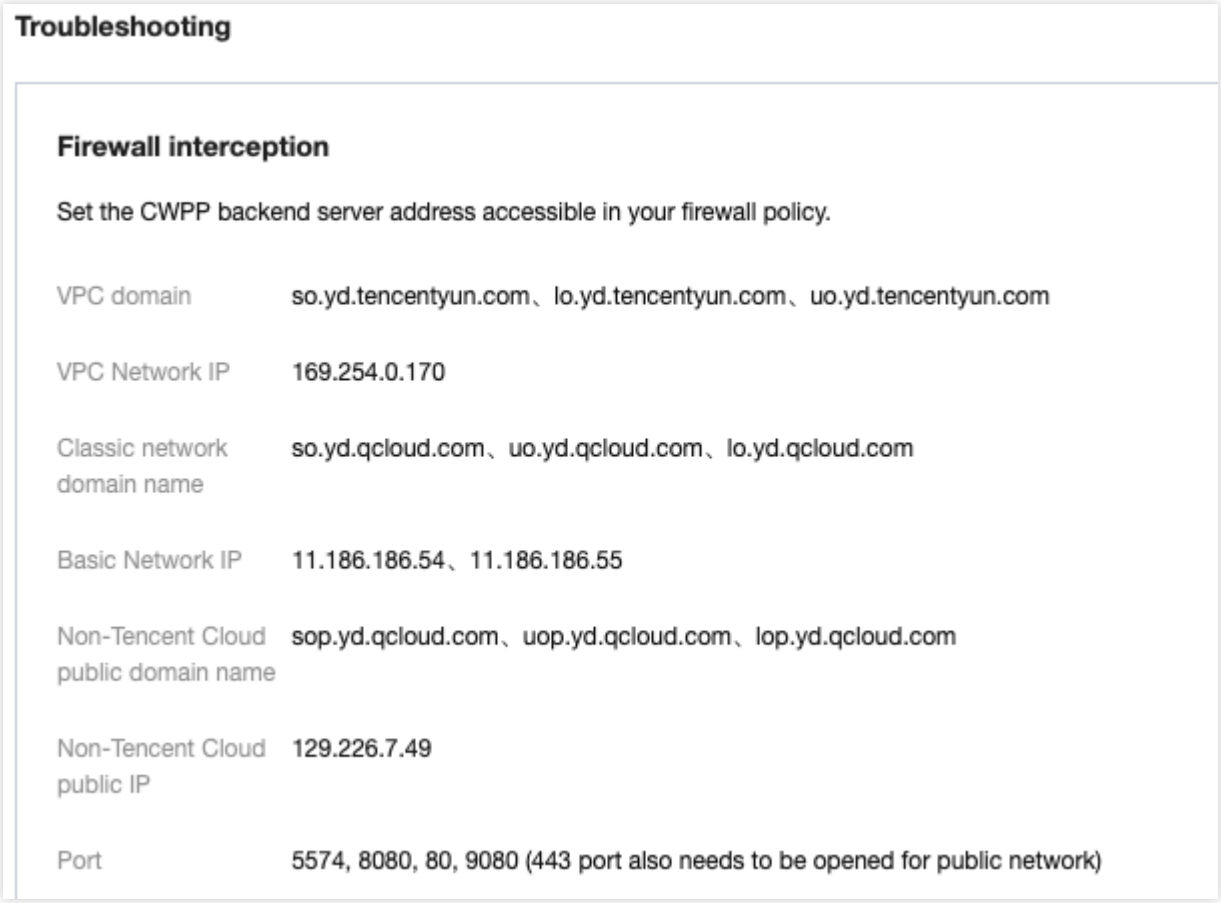


What Are the Target Address and Open Ports for the Cloud Connection over DC?

See the target address and open ports as shown below, and configure the firewall to allow traffic through.

Note:

The address and open ports do not change.



Is the Installation of Agents Supported in IDCs Outside Mainland China?

It is supported. As long as the machine can connect to the network and the system meets the requirements, you can install the CWPP agent.

When Will the Non-Tencent Cloud Instance Be Displayed in the Console After the Agent Is Installed?

Currently, it is displayed in seconds.

Do I Need to Purchase the Console if I Use a Non-Tencent Cloud Instance?

No. The management and billing take place in the public cloud console.

Network Port Access from IDC to the Cloud Is Needed to Open. What Are the Target IP and Ports?

The target IP is included in the installation command, and the ports are 5574, 80, 8080, and 9080.

Can I Use CWPP if the Private Network Machine Cannot Access the Public Network or There Is No DC?

Currently, no.

Does the Hybrid Cloud Client Conflict with the Zabbix Process?

We have not made any special configurations for Zabbix or performed injections. Check for other client installations or drivers on the instance.