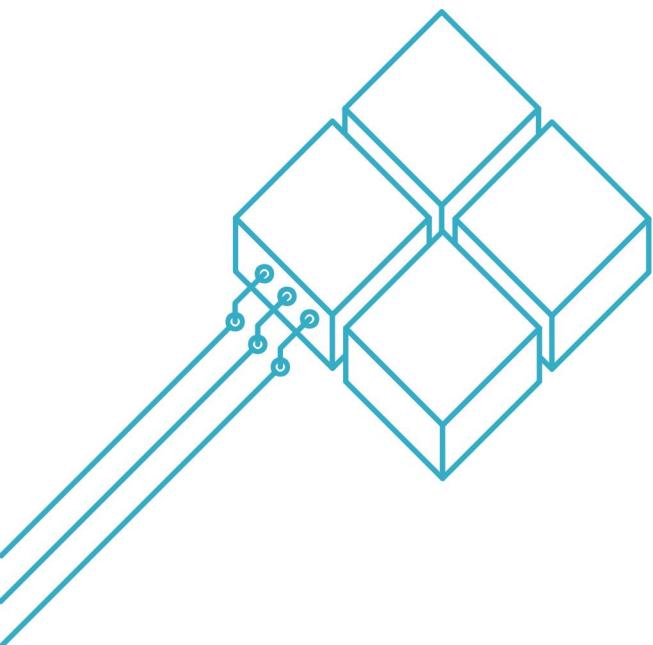


Sentry CWPP

Host Security Product

User Manual

V5.1.5



Making security more effective

2025.12

■ Copyright Notice

All text descriptions, document formats, illustrations, photographs, methods, processes, and other content appearing in this document, unless otherwise specified, are the property of **Qingteng Cloud Security** and are protected by relevant property and copyright laws. No individual or organization may reproduce or quote any part of this document in any form without the written permission of **Qingteng Cloud Security**.

■ Trademark Notice

 青藤云安全 and other **Qingteng** trademarks are the property of **Qingteng Cloud Security**. All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

■ Applicability Statement

This document provides an introduction to the product features of Beijing Shengxin Network Co., Ltd. (hereinafter referred to as "Qingteng Cloud Security") and is intended for user reference and use.

Date	Version	Note
2025.12	V5.1.5	First Release
-	-	-

Content

1 Product Overview	1
1.1 Core Features	1
1.2 Product Architecture	3
1.3 Role Description	4
2 Glossary	6
3 Asset inventory	7
3.1 Asset Collection	7
3.1.1 Asset collection boundary	7
3.1.2 Custom Assets	8
3.1.3 Asset Updates	13
3.2 Configuration	15
3.2.1 Activation/Deactivation of Assets	15
3.2.2 Asset Change Configuration	16
3.2.3 Asset Synchronization	17
3.3 Asset Inquiry	17
3.3.1 General Queries	17
3.4 Asset Comparison	27
3.5 Asset Discovery	28
3.5.1 Host node discovery	29
3.5.2 Container node discovery	31
3.5.3 Cluster node discovery	33
3.6 Appendix: Custom Asset Fingerprints - Field Descriptions	34
3.6.1 Running Application	34
3.6.2 Web Application	41
3.6.3 Web Framework	46
4 Intrusion Detection	57
4.1 Intrusion Detection Configuration and Response	58

4.1.1 Monitoring Configuration	58
4.1.2 Detection Notification	66
4.1.3 Detections Viewing	67
4.1.4 Detection Response	71
4.2 Memory Backdoor	82
4.2.1 Feature Authorization	84
4.2.2 Detection Configuration	86
4.2.3 Alarm Viewing	90
4.2.4 Alarm Response	94
4.2.5 Repair Verification	100
4.3 Network Monitoring	100
4.3.1 Functional Authorization	101
4.3.2 Preconditions	103
4.3.3 Detection Configuration	106
4.3.4 Custom Rules	107
4.3.5 Alarm Viewing	107
4.3.6 Alarm Response	109
4.4 Container Behavior Model	114
4.4.1 Function Authorization	115
4.4.2 Precondition	117
4.4.3 Detection Configuration	118
4.4.4 Model Viewing and Adjustment	120
4.4.5 Alarm Viewing	123
4.4.6 Alert Response	124
4.5 Antivirus	128
4.5.1 Functional Authorization	129
4.5.2 Install Local Engine	132
4.5.3 Detection Configuration	134
4.5.4 Alarm Viewing	139
4.5.5 Alarm Response	142
4.6 Honeypot	147
4.6.1 Feature Authorization	148
4.6.2 Honeypot Management	149
4.6.3 Honeypot Alerts	158
4.6.4 Alarm Response	159

5 Ransom protection	165
5.1 Detection Configuration	168
5.1.1 Enable the tenant driver master switch	168
5.1.2 Turn on the host driver switch	170
5.1.3 Activate ransomware protection authorization	170
5.1.4 Enable ransomware protection	172
5.1.5 Install the local engine	174
5.2 Alarm viewing	175
5.3 Ransom Whitelist	176
5.3.1 Alarm whitening	177
5.3.2 Manual whitening	177
5.3.3 Whitelist List	179
5.4 Alarm Response	179
5.4.1 Automatic Response	179
5.4.2 Manual response	180
5.4.3 Response Logs	181
6 Risk discovery	182
6.1 Risk Analysis	182
6.1.1 Host risk	182
6.1.2 Container risk	207
6.1.3 Cluster Risk	220
6.1.4 Node Image risk	226
6.2 Remediation History	248
6.2.1 Host Remediation History	248
6.2.2 Container Remediation History	250
6.2.3 Cluster Remediation History	251
6.3 Risk Detection	252
6.3.1 Task List	252
6.3.2 Policies	260
6.3.3 Execution Records	263
6.4 Library Query	265
7 Compliance	267

7.1 Baseline Check	267
7.2 Baseline Management	272
7.2.1 Baseline Template Configuration	272
7.2.2 Check Item Configuration	282
8 Event Collection	298
8.1 Introduction to Event Collection	298
8.2 Use of event collection	298
8.3 Event collection function	298
8.3.1 Asset perspective allocation	299
8.3.2 Host event configuration	302
8.3.3 Container Event Configuration	303
8.3.4 EDR event configuration	305
8.4 Purchasing and Enabling Event Collection	307
8.4.1 Event Collection Specifications	307
8.4.2 Event Collection Authorization	307
8.5 How to Enable Event Collection	310
8.5.1 How to Enable Agent Authorization	310
8.5.2 How to Enable Plugins	311
8.5.3 How to Configure Collection Parameters	313
8.6 How to Configure Collection/Filtering Policies	316
8.6.1 Filtering Policies	317
8.6.2 Collection Policies	319
8.7 How to Configure Data Export	321
8.8 How to Automatically Enable Event Collection for Newly Authorized Hosts	322
8.9 How to Disable Event Collection	323
8.9.1 Disabling Event Collection by Host/PC or Container	323
8.9.2 Disable event collection by event category	326
9 Security Control	328
9.1 Control Event	328
9.2 Peripheral Control	329
9.2.1 Peripheral Policies	329
9.2.2 Peripheral Logs	333

9.2.3 Peripheral Alarm Notifications	333
9.3 File Control	334
9.3.1 File Control Strategy	334
9.3.2 Alarm list	344
9.3.3 File White List	346
9.4 Process Control	349
9.4.1 Process Control Strategy	349
10 Web Application Firewall	356
10.1 Feature Authorization	356
10.2 Attack Alerts	357
10.3 Monitoring Configuration	359
10.3.1 Rule Configuration	359
10.3.2 Custom Rules	360
10.3.3 Whitelist	362
10.3.4 Blacklist	365
10.4 Alert Notification	367
11 Probes Installation	368
11.1 Introduction to the Agent	368
11.1.1 Installation	368
11.2 Integration Management	403
11.2.1 Plugins	403
11.2.2 Event Sources	406
11.2.3 Anti-Virus Engines	409
11.2.4 Network Concurrent Monitoring	411
11.2.5 Dante Proxy Management	415
11.2.6 CDN Management	420
11.3 Local Client	425
11.3.1 Product Installation	425
11.3.2 Exit and Uninstallation	427
11.3.3 Update and Upgrade	427
11.3.4 Scanning Task	429
11.3.5 Risk Handling	432

11.3.6 Security Item Management	432
11.3.7 Real - time Detection	434
11.3.8 Settings Center	435
11.3.9 Log Center	436
11.3.10 Tray Menu	436
11.4 Agent - APP Grayscale Upgrade	437
11.4.1 Update packages	438
11.4.2 The system generates or creates an agent version	438
11.4.3 Creating an Agent Upgrade Task (Grayscale Upgrade)	440
11.4.4 Promote batch upgrades	440
11.4.5 View the status of the upgrade task	440
11.4.6 Check the distribution of agent versions	440
11.4.7 Check the version upgrade and configuration	441
12 General Features	442
12.1 Probes	442
12.1.1 Running Monitor	442
12.1.2 Task Management	462
12.1.3 Security Tools	464
12.2 Groups Management	468
12.2.1 Overview	468
12.2.2 Business Groups	469
12.2.3 Tags	477
12.2.4 IP Display Management	480
12.2.5 IP Group Management	484
12.2.6 CMDB Mamagement	487
12.3 Report Center	489
12.3.1 Widget Management	490
12.3.2 Dashboard Management	509
12.3.3 Report Management	513
12.3.4 Screen Management	520
12.4 Permission Management	523
12.4.1 Account	524
12.4.2 User Groups	526
12.4.3 Roles	527

12.4.4 Permission Policies	528
12.4.5 Data Templates	529
12.5 SystemManagement	529
12.5.1 Deployment Management	529
12.5.2 Brand Configuration	547
12.5.3 API Configuration Management	549
12.5.4 Outgoing	552
12.5.5 SMS and Email Configuration	569
12.5.6 Audit Logs	575
12.5.7 System Monitor	576
12.6 Tenant Management	578
12.6.1 Tenant Overview	579
12.6.2 Probe Management	586
12.6.3 Outgoing	593
13 Tools	594
13.1 Download Center	594
13.2 Feedback Tool	594
13.2.1 Screenshot Feedback	595
13.2.2 Screen Recording Feedback	595
13.2.3 After-sales customer service	596
13.3 Ticket Tool	597
14 Message Center	601
14.1 Message Notification	601
14.1.1 Message List	601
14.1.2 Message Search	601
14.2 Message Configuration	602
14.2.1 Receiving Configuration	602
14.2.2 Recipient Configuration	607
14.2.3 Group Bot Configuration	607
15 Personal Center	608
15.1 Authorization Information	608

15.2 Language Switch	609
15.3 Account Information	609
15.4 Version information	610

1. Product Overview

1.1. Core Features

Sentry CWPP - Host Security Product focuses on server security protection, providing continuous capabilities of security monitoring, analysis, and rapid response. It enables unified security policy management and quick intrusion response across various environments, including public clouds, private clouds, hybrid clouds, physical servers, and virtual machines. The product adopts the Adaptive Security architecture proposed by Gartner, which is designed to effectively defend against advanced attacks in complex and changeable environments. This architecture represents the future direction of the whole security industry. The innovation lies in two aspects:

1. Shifting the security perspective to inside the business systems behind firewalls, emphasizing a business-centric, inside-out approach to building a security system.
2. Transforming security from traditional event-based protection to a continuous security response and management process, providing multi-dimensional, ongoing protection for enterprise security.

Sentry CWPP - Host Security Product can be easily integrated with various cloud platforms and traditional servers, allowing global deployment with minimal effort. The product requires no hardware purchase, complex configuration or extensive learning, yet offers high precision. Sentry CWPP empowers IT and security personnel to manage the security of massive server fleets, significantly enhancing enterprise security protection even with limited resources and expertise. Security is an ongoing process, and Sentry CWPP is fast, flexible, and scalable. It combines existing security technologies with a continuous operational security model, providing users with a dynamic,

ongoing security solution.

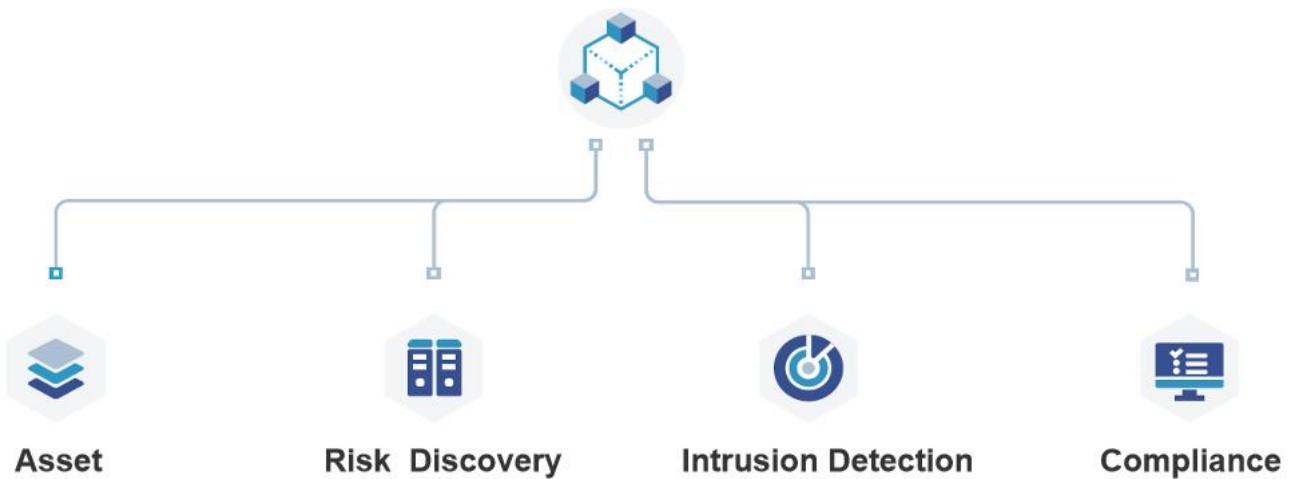


Figure 1.1: Sentry CWPP Host Adaptive Security Platform Product System

The Sentry CWPP - Host Security Product consists of four main components:

- Asset Inventory:

Automates the construction of granular asset information from a security perspective, supporting precise identification and dynamic awareness of business-layer assets. Using an Agent-Server architecture, it provides over 10 types of host asset inventories and automatic recognition of more than 200 types of business applications, with excellent scalability.

- Risk Discovery:

Helps users accurately identify internal risks, enabling security teams to quickly locate and resolve security issues. It provides detailed asset and risk information for analysis and response.

- Intrusion Detection:

Offers multi-anchor detection capabilities, enabling real-time and accurate perception of intrusion events and identification of compromised hosts. It also provides response measures for intrusion incidents.

- Compliance Baseline:

Establishes baseline requirements based on China's Information Security Level Protection and CIS (Center for Internet Security) standards, covering multiple versions of mainstream operating systems, web applications, and databases. Users can quickly conduct internal risk assessments, identify issues, and make timely repairs to meet regulatory requirements. Additionally, enterprises can define their own baseline standards for internal security management.

1.2. Product Architecture

The Qingteng Cloud Security Host Monitoring and Management System consists of three parts: Server, Web Presentation Layer, and Agent Probe.

- Server:

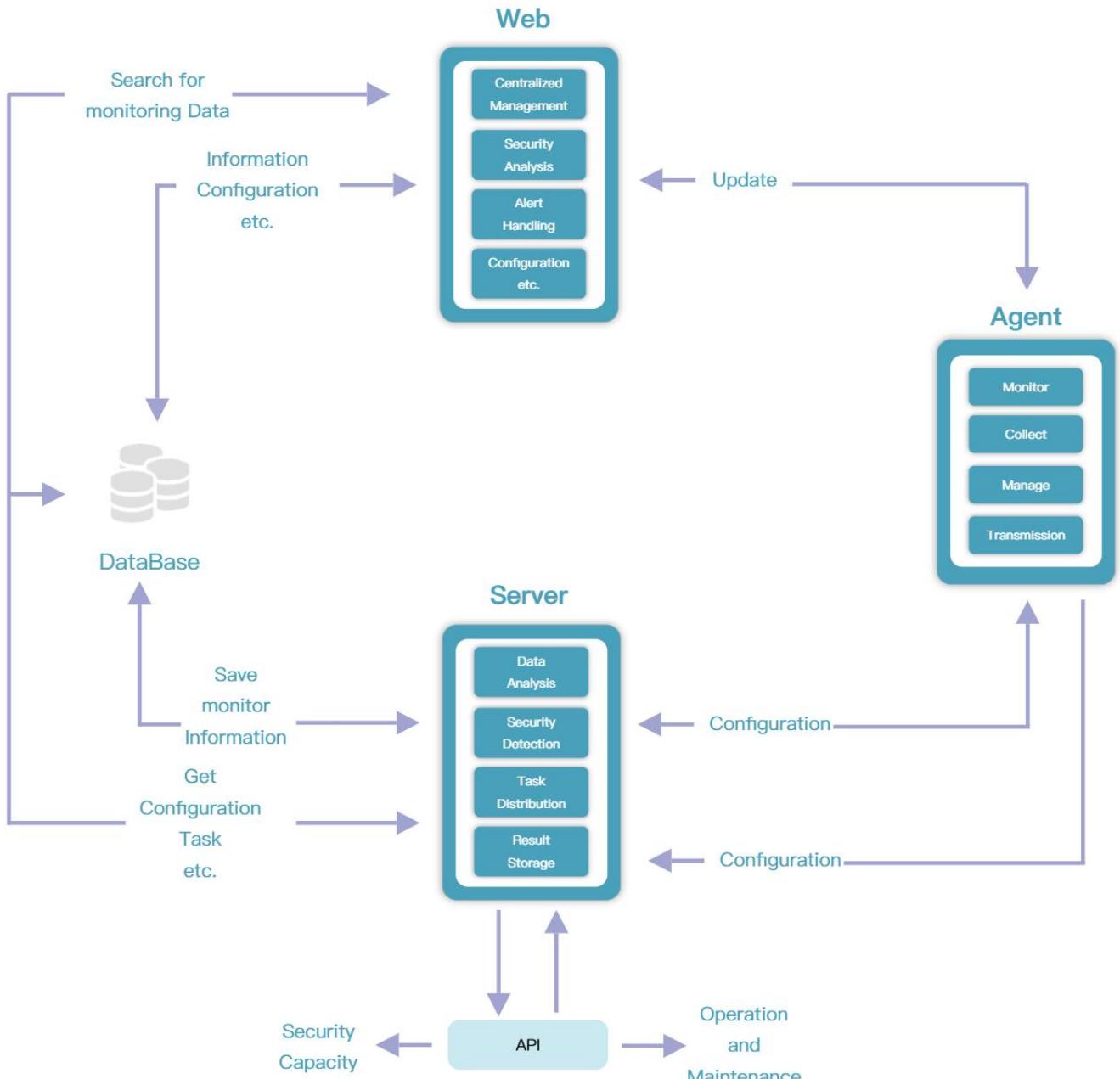
Hosts the majority of the system's operational programs, responsible for unified data collection, analysis, and control.

- Web Presentation Layer:

Displays processed data results on the interface for user review.

- Agent Probe:

Installed on managed hosts, responsible for security inspections and real-time intrusion monitoring.



1.3. Role Description

The product includes two predefined administrator roles:

- DeployAdmin: Deployment Administrator Role, Only features under the following modules are visible/accessible:
 - General → Tenant Management
 - General → System Management → Deployment

- o General → System Management → System Monitor

Admin: Tenant Administrator Role, which has access to all features except those exclusive to the DeployAdmin role.

Status	Role Name	Description	Associate Perm...	Assign User Co...	Assign User Gr...	Creator	Last Update Ti...	Operation
Active	Administrator	Default Admin Role	39	26	0	[system]	2021-07-01 08:00:00	Details
Active	Asset Analyst	The related functions of asset inquiry and analysis, including asset inquiry and asset comparison.	1	3	0	[system]	2021-07-01 08:00:00	Details
Active	Asset Manager	Full Permissions of the Asset APP	1	1	0	[system]	2021-07-01 08:00:00	Details
Active	Audit	For console auditing, it includes auditing of various functional modules and accessing system audit logs.	2	4	0	[system]	2021-07-01 08:00:00	Details
Active	Compliance Analyst	You can only view compliance baseline results data and baseline configuration data.	2	1	0	[system]	2021-07-01 08:00:00	Details
Active	Compliance Officer	Possessing the highest permission of a compliant baseline APP	2	1	0	[system]	2021-07-01 08:00:00	Details
Active	Data Outgoing Ad...	Full Permissions of the Data Outgoing	1	2	0	[system]	2021-07-01 08:00:00	Details
Active	DeployAdmin	Default DeployAdmin Role	18	6	0	[system]	2021-07-01 08:00:00	Details
Active	Event-Collect Man...	Possessing full permissions for Event-Collect	1	2	0	[system]	2021-07-01 08:00:00	Details

2. Glossary

- Asset: Any entity within an enterprise that holds security data value. In this system, it refers to base tables collected by sensors or advanced views formed through operational configurations.
- Managed Object: Nodes that provide runtime environments for practical business applications from a user perspective, including: hosts, containers, pods, clusters, and images.
- Query Scenario: Specific contexts where users execute queries to retrieve required information or data.
- Asset Change: Events defined for collected asset data (creation, deletion, modification) with monitoring capabilities.
- Asset Comparison: Statistical analysis of asset state changes by comparing snapshots from two distinct time points.
- Baseline Configuration: A benchmark consisting of multiple inspection items. A single baseline may define multiple configurations, each selecting different inspection criteria.
- Baseline Check: User-created inspection tasks where each task evaluates a group of hosts against multiple baseline rules.
- Inspection Environment: Execution environments for baseline checks, including Linux, Windows, containers, and orchestration platforms.
- Inspection Targets: Objects assessed during baseline checks, covering: Systems, applications, containers, images, Docker, K8s Master, K8s Node, Openshift Master, Openshift Worker, CRI-O hosts, CRI-O containers, Containerd hosts, Containerd containers, YAML files

3. Asset inventory

Asset inventory, committed to helping users automatically build fine-grained asset information from a security perspective, uses the Agent-Server architecture, provides host key asset inventory, automatic identification of more than 200 types of business applications, and has good scalability. Comprehensive and timely asset data support greatly shortens the investigation time in the event of a security incident, and asset information is synergistically linked with patches, risks, baselines and other functions, which can quickly locate the problematic host and view the application details in a timely manner, helping users quickly deal with existing risks and reduce unnecessary losses.

3.1. Asset Collection

3.1.1. Asset collection boundary

Currently, the system supports the collection of various asset data such as process ports, account assets, hardware assets, registries, web services, databases, and cloud-native assets. For specific details of supported assets, you can enter "Asset Management" to view or check the asset boundary list.

Steps:

- Click the "All Resources" button on the top right corner of the asset query page to view all asset categories.

Asset > Asset Inquiry

Asset Inquiry

Please specify the target value for the query.

Quick Query System Assets Application Assets Last Updated At : 2025-12-27 03:00:00 C Total 13 items

Managed Objects		Common Assets		Account Management	
Host	35	Process	6304	The account with a UID of 0	309
Container	299	Port	3067	The account with a UID of 0	1081
Pod	197	System Account	7287	Accounts with login shell privileges	374
Cluster	5	Java Archive (JAR) file	3912	Enabled account	249
Image	1218	Website	158	Expired Password Account	0

Web Server		Run Application		Web Application	
Apache	6	system	22	Jenkins	1
Tomcat	7	TitanAgent	22	Confluence	1
Nginx	25	SSH	19		

For assets with identification rules such as running applications, web applications, PHP frameworks, Python frameworks, Java frameworks, sensitive registries, and application startup information, you can enter the "Configuration - Identify Boundaries" page of the asset through "Configuration" to view the detailed supported boundaries of the asset. One-click export is supported.

Application Launch Information

Asset Definition Data Collection Policy Identify Boundaries Change Field Configuration

Please select filter content

4 items

name	Innovation	Applicable ...	Description
Startup item 1	Non-Innovation		Startup item 1
Startup item 2	Non-Innovation		Startup item 2
Startup item 3	Non-Innovation		Startup item 3
Startup item 4	Non-Innovation		Startup item 4

4 items 1 50 Item/Page

3.1.2. Custom Assets

In addition to collecting the above assets, you can also enrich the assets according to your needs and add custom assets.

3.1.2.1. Custom Asset Fingerprints

Based on built-in asset scripts, users can enable the identification of new assets by adding custom

asset fingerprints.

Currently, assets that support custom fingerprints include: running applications, web applications, Python frameworks, PHP frameworks, and Java frameworks.

Fingerprint rules for each type of asset must be created separately based on the operating system type.

Steps:

1. Select a specific asset category from the left sidebar, choose the corresponding operating system tab, and click "New Asset" to enter the fingerprint configuration interface.
2. Fill in the basic information and rule parameters for the fingerprint rule, then save to complete the rule creation.
3. Supported operations for custom fingerprint rules include: adding, deleting, editing, enabling, and disabling.
4. Asset synchronization: Supports synchronization by host or full synchronization. After creating an asset rule, users can first select non-critical hosts for custom synchronization verification. Once the data collection meets requirements, global synchronization can be performed.

For detailed parameter descriptions, refer to the appendix in the last section: "Custom Asset Fingerprints - Field Descriptions."

Note:

After performing operations such as adding, deleting, editing, enabling, or disabling asset rules, manual synchronization is required for the changes to take effect globally.

Asset > Configuration

Configuration

Built-in Assets Custom Asset Fingerprint Custom Asset Script

Last Sync Time: 2025-09-10 16:17:46 Sync Assets

Custom Asset Fingerprint

After creating an asset rule, you can first select a subset of non-critical hosts for custom synchronization verification. Once data collection is confirmed to meet requirements, proceed with global synchronization. Any changes to asset rules—including additions, deletions, edits, enabling, or disabling—require manual synchronization to take effect globally.

Status	Rule Name	Description	Last modified time	Operation
<input type="checkbox"/> Disable	dxh	-	2025-09-04 16:47:26	Edit Delete
<input type="checkbox"/> Disable	dxhSSH	dxhSSH自定义资产	2025-09-04 16:47:26	Edit Delete
<input type="checkbox"/> Disable	dxh1	test	2025-09-04 16:47:26	Edit Delete
<input type="checkbox"/> Disable	dxhNginx	200字符测试,有多个进程名, ...	2025-09-04 16:47:26	Edit Delete
<input type="checkbox"/> Disable	dxhClickHouse	dxhClickHouse自定义规则	2025-09-04 16:47:26	Edit Delete

3.1.2.2. Custom Asset Script

Support for adding asset identification by uploading custom asset scripts, allowing configuration of various display attributes for assets.

Note: Before uploading a custom script, it must be signed by our company; otherwise, it will fail the verification process and the script upload will be unsuccessful.

Asset > Configuration

Configuration

Built-in Assets Custom Asset Fingerprint Custom Asset Script

Sync Assets

Custom Asset Script

Changes such as adding, removing, enabling, disabling, or modifying asset configurations require manual synchronization to take effect.

Query Asset Categories

All Categories +

应用脚本 (0)

Asset Classi... Asset Name Applicable ... Max Cache Time Script Executi... Description Operation

No Data

Steps:

1. First, create an asset category in the left sidebar. Hover over the category and click the corresponding icon to modify or delete the category name.
2. Click on a specific category, then click "New Asset" to enter the configuration page for that asset.

Parameter Descriptions:

- **Asset Category:** Select an existing asset category or create a custom one.
- **Storage Table Name:** This field is parsed from the script and cannot be modified on the interface.
- **Maximum Cache Time:** Determines the cache validity period for data collected by the agent. Beyond this period, the system will re-execute the script to recalculate the data. For asset types with frequently changing return values, such as running processes, a shorter cache validity period can be set. To disable caching, set this value to 0.
- **Script Execution Cycle:** Set a periodic update cycle for the asset. Each update will re-execute the script to retrieve the latest data.

Asset Collection Script:

- Currently, only scripts for Linux, Windows, and AIX systems are supported.
- Asset scripts must be signed and verified by Qingteng.
- Supports simultaneous upload of scripts for the same asset across different operating systems, allowing unified configuration.

Result View:

- The column fields in the result view are defined and parsed by the script. This view determines the default display style of the asset data.
- Supports configuration of field titles, display order, visibility, and whether the field participates in homepage searches.
- Click the settings button next to a field to configure enumeration conversion for that field.

After configuration, click "Save" to complete. Custom assets support editing, deletion, and management configuration operations. For details, refer to the introduction below.

Synchronize Assets:

- After performing operations such as adding, deleting, enabling, disabling, or managing configuration for an asset, manual synchronization is required for the changes to take effect.
- This operation is executed asynchronously. After the synchronization command is issued to the Agent, it may take some time to complete.

Note:

- Before uploading a script, ensure it has undergone logical verification and security checks to guarantee the accuracy and safety of data collection.

The screenshot shows the 'Create Custom Asset' page under 'Asset > Configuration > Create Custom Asset'. The page is titled 'Create Custom Asset' with 'Cancel' and 'Save' buttons. It has three main sections: 'Basic Information', 'Collection Configuration', and 'Asset Collection Script'.

- Basic Information:** Includes fields for 'Asset Classification' (dropdown), 'Asset Name' (text input), 'Description' (text area), and 'Storage Table Name' (dropdown).
- Collection Configuration:** Includes 'Max Cache Time' (0 minutes), 'Script Execution' (Daily selected), 'Start Time' (00:00), and a 'Collection Configuration' button.
- Asset Collection Script:** A note stating 'Currently supports Linux, Windows, and AIX scripts only.' with an 'Add Script' button.

Parameter description:

- **Asset Classification:** You can select an existing asset classification or create a custom asset classification.
- **Max Cache Time:** Determines the cache time of the collected data, after which the system will re-execute the script for calculation. For asset types whose return values change frequently, such as running processes, you can set a shorter cache time. If you don't want to cache, you can set the value to 0.
- **Script execution cycle:** You can set a regular update cycle for an asset, and the script will be

re-executed every time it is updated to obtain the latest data.

- Asset Collection Script:
 - Currently, only Linux, Windows, and AIX scripts are supported
 - Asset scripts need to be signed and verified by Qingteng
 - You can upload scripts from different operating systems of the same asset at the same time for unified configuration

After the custom asset is created, you can edit, delete, and manage the configuration of the custom asset, as described below.

3.1.3. Asset Updates

The data collected by the asset is updated regularly, and you can customize the update policy when you need to change the periodic update cycle of the asset.

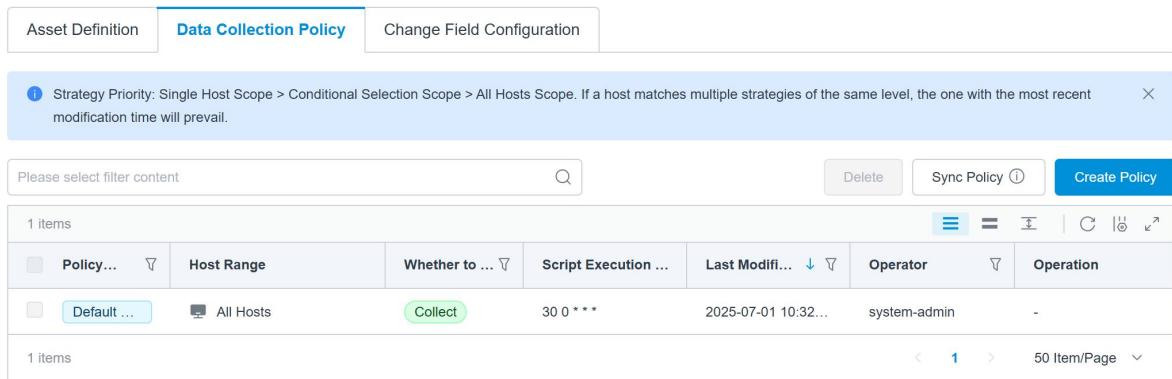
Scheduled asset updates:

Steps:

- Each preset asset has a default scheduled update cycle, and you can customize the collection policy and specify the update period.
- You can use the Configuration - Operation- Configuration button to enter the asset collection policy tab page, click the Create Policy button on the page, and fill in the relevant information.
- You can edit, delete, or delete a new policy.

Asset > Configuration > Management Configuration

VastBase



Policy...	Host Range	Whether to ...	Script Execution ...	Last Modifi...	Operator	Operation
Default ...	All Hosts	Collect	30 0 * * *	2025-07-01 10:32...	system-admin	-

Illustrate:

- The final collection policy executed by each agent is calculated based on the priority:
 - For host or container assets, the scope of a single host > the scope of the conditional selection > the scope of all hosts. If a host matches multiple policies of the same level, the last modification time is the most relevant.
 - For clusters, a single cluster scope > the entire cluster scope. If a cluster matches multiple policies of the same level, the last modified time is the most recent.
- You can configure collection policies for assets in batches, and after you create them, you can add a collection policy for the selected assets according to the execution scope. The final effective policy of the machine is calculated by the priority of all the policies of the asset.

Immediate asset updates:

In addition to updating by asset class, an update can be triggered immediately based on the host scope. Updates can be performed by host, business group, and cluster.

Steps:

- Click the button on the right side of "Update All" in the upper right corner of the asset query page to select the updated dimension and manually update the asset.

▼

- You can also go to the list page and click the "Update" button to update a single managed object or a single asset.

Note: To avoid asset update timeouts, we recommend that you select a small number of images at a time and complete the update in multiple installments. Images that are in the Updating state are not added to the queue repeatedly.

3.2. Configuration

3.2.1. Activation/Deactivation of Assets

The "Enabled" parameter determines whether to collect data from such assets. Enabling means that the policy will be updated on a regular basis or immediately after each occurrence, and disabled means that the asset data will no longer be collected and updated, but the collected historical data will still be retained.

Steps:

- Go to the configuration list and click the button in the "Enable" column to switch the asset collection status.



The screenshot shows the 'Asset > Configuration' section. On the left, there's a sidebar with categories like '集群资产 (13)', '系统软件 (12)', etc. The main area has tabs for 'Built-in Assets' and 'Custom Assets'. A search bar says 'Please select filter content'. Below it is a table with columns: 'Max Cache Time', 'Script Executi...', 'Description', 'Enable/Disable' (which is highlighted with a red box), 'Monitor Changes', and 'Operation'. There are 198 items listed.

3.2.2. Asset Change Configuration

If you want to monitor the changes of certain key assets over a period of time, you can enable the asset change monitoring configuration.

Steps:

- First of all, you need to turn on the "Whether to monitor changes" button in the asset management list, which means to monitor the new or deleted events of this type of asset.
- If you want to monitor the change of the value of a specific field of a certain type of asset, you can go to the Change Configuration page through the Manage Configuration button and select the change field to be monitored. If you do not fill in this field, the modification event of the asset is not monitored.
- You can query the specific changes of assets through the asset comparison function, and for more information, see the "Asset Comparison" section of this document.

Asset > Configuration > Management Configuration

VastBase ⚠

The screenshot shows a user interface for managing asset configurations. At the top, there are three tabs: 'Asset Definition', 'Data Collection Policy', and 'Change Field Configuration'. The 'Change Field Configuration' tab is selected and highlighted in blue. Below the tabs, a blue banner contains the text: 'This function allows you to configure monitoring fields for asset change events.' with a close button 'X'. Under the banner, there is a section titled 'Unique Identifier' with a help icon. It says: 'Identify asset additions and deletions based on this identifier.' A text input field contains the value 'pid'. Below this, another section titled 'Change Field Monitoring Configuration' with a help icon says: 'If not filled in, it means not monitoring changes to asset modification events.' A 'Configure' button is located at the bottom of this section.

3.2.3. Asset Synchronization

After you add, delete, enable, disable, or manage configurations, you need to manually synchronize assets before they can take effect.

Steps:

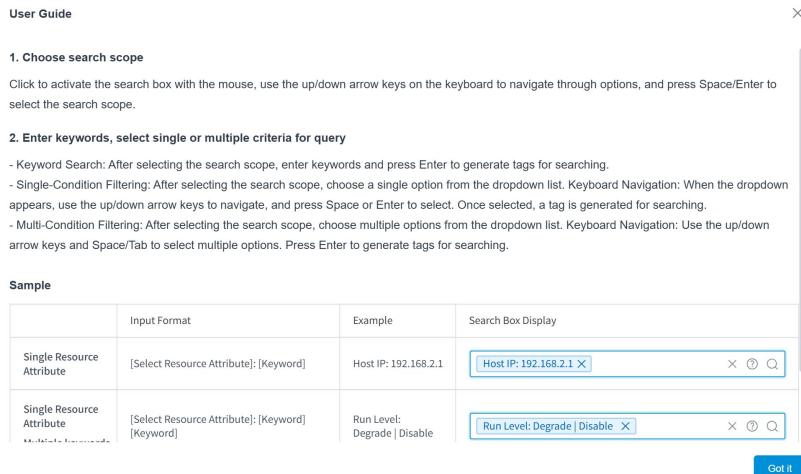
- You can click the "Synchronize Assets" button on the asset management page to manually synchronize the configuration.

3.3. Asset Inquiry

3.3.1. General Queries

The system provides instructions for how to enter the search box, and you can click the button to view.





3.3.1.1. Unified query

When searching for assets, you can use the unified query box to find a management object, the key assets on the management object, and a specific type of asset.

Scenario 1: Search for a management object

based on the IP, name, ID, and other information to find a machine, pod, or container. You can view the key assets on this object, including processes, ports, system accounts, running applications, and jar packages.

Steps:

- For example, select the search attributes of the host, such as the IP address and name of the host. Complete the query by entering the value of the retrieved property.
- Go to Assets Page corresponds to a single-class asset page and matches the search attributes you entered. The Details after a single piece of data corresponds to the page of a single type of asset, and matches and locates the data.

The screenshot shows the 'Asset Inquiry' interface. At the top, there's a search bar with 'Host IP: 10.42.2.60'. Below it is a table with one item. The table columns are 'Host', 'Business Group', 'Operating System', 'Tags', and 'Operation'. The first row contains '10.42.2.60 | cdplugin-0', 'dxh', 'Alpine Linux v3.13', an empty 'Tags' field, and an 'Operation' button. Red arrows point from the text 'highlighted host IP value' to the host IP in the search bar and to the 'Details' link in the table row.

Host	Business Group	Operating System	Tags	Operation
10.42.2.60 cdplugin-0	dxh	Alpine Linux v3.13		Details

- Click on the highlighted host IP value to pop up the corresponding host details page; It contains the basic information and management information of the host, as well as the associated business risks and device alarms.
- If you want to view the changes in the asset data of the host, you can click the "Asset Comparison" button in the upper right corner to view it.
- If you want to update the asset data of a single host, you can click the "Update Data" button in the upper right corner.

The screenshot shows the '10.42.2.60 Details' page. It has two main sections: 'Basic Information' and 'Management Information'. In 'Basic Information', fields include Hostname (cdplugin-0), Host IP (10.42.2.60), Host Type (server), and various system stats like CPU (0 Cores) and Memory (0KB). In 'Management Information', fields include Business Group (dxh), Tags, Cluster, and management contacts like Owner and Machine Room. A central 'Update Data' button is visible.

Scenario 2: Search for a certain type of asset

and search for process ports, accounts, applications, or packages based on key information such as

names and paths.

Steps:

- Taking a process as an example, complete the query by entering the value of the corresponding search attribute.

The screenshot shows the 'Asset Inquiry' page under 'Asset > Asset Inquiry'. At the top right are buttons for 'All Resources' and 'Update All'. Below is a search bar with a dropdown menu set to 'Process'. The search bar has placeholder text: 'Multiple filter tags are separated by the Enter key.' To the right of the search bar are a help icon and a magnifying glass icon. On the left, there's a sidebar with 'Search Results' and filters for 'Process Name', 'PID', and 'Startup Parameters'. A note says 'Please select filter'. At the bottom right is a link 'Go to Assets Page' with a magnifying glass icon.

Illustrate:

- On the query results page, you can update, analyze, and export the data. You can also switch the simple search in the input box to an advanced search statement, and see the "List Query" section of this document for details.

3.3.1.2. Hierarchical view query

The asset query page includes a unified query box, preset dashboards, and asset navigation views.

- The asset navigation view is hierarchical at two levels, and the asset classification is displayed at the first level; The name of the asset is displayed at the second level. By clicking the name of the secondary asset in the asset navigation view, you can directly enter the asset list page.
- The number after each type of asset represents the total data volume of the asset, which is updated regularly at 03:00 every day, and the latest statistical update time is displayed in the upper right corner of the dashboard, or you can click to trigger an update immediately.



Preset dashboards: The system presets three dashboards: Quick Query, System Assets, and

Application Assets, which you can manage and add custom dashboards.

- Quick query: From a security perspective, commonly used assets and query scenarios are preset to facilitate quick query. Thereinto:
 - Query scenarios help you troubleshoot the security of assets, such as viewing high-privileged running sites and special accounts. You can directly click on the corresponding query scenario to enter the result page.
- System assets: From a security perspective, focus on system asset data of hosts, containers, and clusters.
- Application assets: From a security perspective, focus on application assets, such as software applications, databases, web services, and software packages.

The screenshot shows the 'Asset Inquiry' page with the following data:

Managed Objects		Common Assets		Account Management		Database	
Host	74	Process	8944	The account with a UID of 0	254	MySQL	5
Container	230	Port	4537	The account with a GID of 0	817		
Pod	108	System Account	5728	Accounts with login shell privileges	255		
Cluster	3	Run Application	604	Enabled account	192		
Image	1390	Java Archive (JAR) file	6530	Expired Password Account	0		
		Website	180	Users (groups) bound to a Role	68		
		Web Application	1				
		Java framework	483				
		Python framework	0				

Set up boards: As asset classes continue to grow, the system also provides you with more flexible navigation and querying methods. You can customize the content of the dashboard according to your needs and display it on the asset query page.

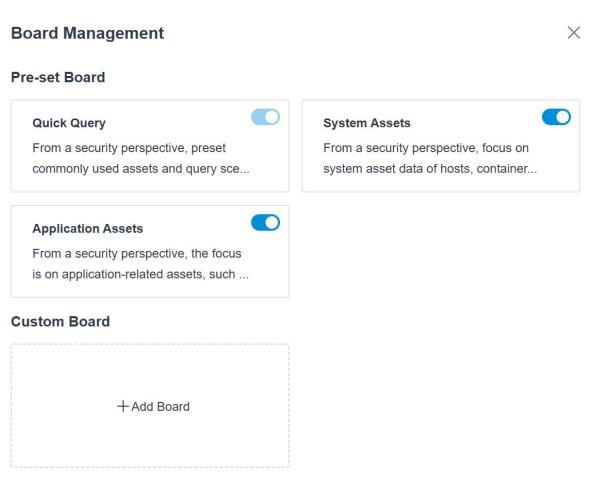
Steps:

- Click the button



behind the assets application, and the "Board Management" drawer will pop up to manage the board.

- Click the  button, you can choose to preset the board and customize the board to show or hide.
- Custom boards: You can click "Add Board" to customize and configure personalized dashboards, including new, editing, deleting, and showing/hiding dashboards.



After saving, a blank board tab will be added to the asset query page. The system supports the configuration of Kanban content, including adding modules, editing modules, deleting modules, sorting, and collapsing/expanding modules.

Steps:

- You can click the button to make the card edit and add the content to the module.

- When the mouse hovers over a piece of data in the module, press the left mouse button to drag the content up and down to sort.

The screenshot shows the 'Asset Inquiry' page with a search bar and filter options. The main content area displays two sections: 'New modules' and 'All assets', both of which show 'No Data'.

3.3.1.3. List Query

You can click on the secondary assets on the asset query page or through the unified query to enter the asset list page, which supports simple search and advanced search.

Simple Search:

Steps:

- Move the cursor into the search box and click to display the conditions that support filtering, including management objects (types), management objects (such as hosts, containers, and pods), and assets.

The screenshot shows the 'Asset Inquiry > Host' page with a table of host assets. The table includes columns for Host IP, Hostname, Host Type, Agent ID, Communication Status, Business Group, Operating System, Tags, and Owner. Several rows are listed, each with a highlighted asset name.

- Click the highlighted asset name to view the details of the app, including basic information and associated asset information.

- Click on the highlighted management object to pop up the details of the corresponding management object.
- If you want to update, analyze, and export the data for this asset, you can do so by clicking the corresponding button in the upper right corner.
- The system also supports switching the simple search you entered to an advanced search statement, see "Advanced Search" in 1.2.1.3 of this document for details.

Advanced search: To support more complex query scenarios, the system provides an advanced search method that you can search by entering QSL statements.

Steps:

- Click button to view the QSL syntax description.

- In the Advanced Search input box, you can display the last 10 historical query statements and display the fields that can be used for query.
- If you select the historical query statement, press enter, or click Search, the query will be executed.
- If you select a common field, you can enter the corresponding value, build a query statement based on the syntax instructions, and directly execute the query.

Illustrate:

- Toggle between simple and advanced queries:
 - After a simple query is executed, you can click the highlighted "Advanced Search" button to convert it into an advanced query statement.
 - In advanced query mode, if your query statement is updated and the query is executed, you cannot directly switch to a simple query.

Scene saving: Advanced retrieval builds can be saved as common queries. Later, you can view the list of saved queries, select a query, quickly reproduce the saved query statements, and display the query results.

Steps:

- After performing a query, you can click the button to save the query scene. Thereinto:



- Select Category to select an existing category or create a new category.



The screenshot shows a 'Save Query' dialog box. It has a title bar 'Save Query' with a close button 'X'. Below the title are four input fields: 1) 'Select ...:' with a dropdown menu labeled 'Select Module'. 2) 'Query ...:' with a placeholder 'Please enter the query name (within 20 characters)'. 3) 'Query ...:' with a placeholder 'Please enter the query statement'. 4) 'Descript...:' with a placeholder 'Please enter a description (up to 50 characters)'.

- If you want to see a list of saved queries, you can click the button to the left of the advanced filter box. You can also go to the All Resources - Saved Queries page to query and manage.



- If you select one of the queries, you can quickly reproduce the query statement, and the system will jump to a new tab to display the query results.
- If you want to modify the query statement, you can also modify it directly in the search box on the query results page.
- When you hover over a query, you can click the button to delete it.



Data analysis: The system supports the analysis of the query results, and you can visualize the asset data by clicking the "Analyze" button on the asset list page.

For detailed instructions, see the Data Center module documentation.

3.4. Asset Comparison

After a hacker compromises a host, it may start a new process, add a scheduled task, or modify the registry. By monitoring the changes in these assets and analyzing and comparing them to asset change events, you can better understand and manage your assets.

This product provides the "Asset Comparison" function to realize the change comparison and analysis of key assets.

Steps:

- If you want to view the asset comparison results, you need to open the "Monitor Changes" button in the management configuration module one day in advance, and select the monitoring change fields.
- Then specify the query host on the asset comparison page, and the system will jump to the comparison result page.
- By default, the system displays the changes in asset data in the last 30 days, and you can click to switch to the last 60 days and the last 90 days.
- You can also toggle the date you want to compare by clicking on a point on the timeline. The highlighted dots on the timeline represent the date you are currently selected; The orange dot indicates that the date has changed from the previous asset data.

Asset Comparison Results

Host 172.16.21.122 Asset Comparison Results

Select asset change time

30 Days 60 Days 90 Days

Host 172.16.21.122 Asset Comparison Results

Ascending Order Descending Order

graphics card
2
↑ 1 ↓ 1 ▷ 0

If you click on an asset, the card is highlighted to show the comparison of the data snapshots of the asset before and after the selected two dates.

- The results display includes the deletion, creation, and modification of assets, and you can cancel or display the comparison results of some events by selecting Cancel or Display.
- The red indicates the deletion event, the green indicates the new event, and the yellow indicates the modification event.
- Click the triangle icon in front of the data to view the specific details of a data.

Asset Comparison Results

Select asset change time

30 Days 60 Days 90 Days

Host 172.16.21.122 Asset Comparison Results

Ascending Order Descending Order

graphics card
2
↑ 1 ↓ 1 ▷ 0

Name	Date
1	2025-06-19
2	Device 1234:1111

3.5. Asset Discovery

This function is mainly used to discover unprotected hosts, containers, and cluster nodes in the

customer's intranet environment, expose business risks, and promote agent installation coverage and risk protection.

3.5.1. Host node discovery

Host node discovery supports ARP cache scanning, ping scanning, Nmap scanning, and other scanning technologies to help you detect and identify active hosts in the intranet environment that are not included in the control scope of the platform. Click "Install Agent" to jump to the agent installation page.

Host IP	IP Version	Equipment Type	Operating System	MAC Address	Discovery Method	Initiating Host	First discovered	Recently Discovered	Operation
172.17.0.3	IPv4	-	-	02:42:ac:11:00:03	ARP Cache Scan	192.168.21.1...	2025-05-15 15:2...	2025-05-15 15:24...	Ignore
102.168.21...	IPv4	VMware	-	00:50:56:ee:82:0f	ARP Cache Scan	192.168.21.1...	2025-05-15 15:2...	2025-05-15 15:24...	Ignore
102.168.21.1	IPv4	VMware	-	00:50:56:e0:00:08	ARP Cache Scan	192.168.21.1...	2025-05-15 15:2...	2025-05-15 15:24...	Ignore
102.168.21.2	IPv4	VMware	-	00:50:56:e9:21:85	ARP Cache Scan	192.168.21.1...	2025-05-15 15:2...	2025-05-15 15:24...	Ignore
172.17.0.2	IPv4	-	-	02:42:ac:11:00:02	Ping Scan	192.168.21.1...	2025-05-15 15:2...	2025-05-15 15:24...	Ignore
10.244.36....	IPv4	-	-	32:78:28:ee:80:d0	ARP Cache Scan	172.16.12.17...	2025-05-15 15:2...	2025-05-15 15:26...	Ignore
172.16.12.90	IPv4	-	-	be:b7:65:aa:c3:a4	ARP Cache Scan	172.16.12.17...	2025-05-15 15:2...	2025-05-15 15:26...	Ignore
172.16.12.10	IPv4	-	-	da:f5:44:73:df:6a	ARP Cache Scan	172.16.12.17...	2025-05-15 15:2...	2025-05-15 15:25...	Ignore
172.16.12.18	IPv4	-	-	9a:83:7b:c2:ba:64	ARP Cache Scan	172.16.12.17...	2025-05-15 15:2...	2025-05-15 15:25...	Ignore
172.16.12.12	IPv4	-	-	7e:7d:32:0e:ce:fe	ARP Cache Scan	172.16.12.17...	2025-05-15 15:2...	2025-05-15 15:25...	Ignore
172.16.12....	IPv4	-	-	8a:84:4a:sf:db:62	ARP Cache Scan	172.16.12.17...	2025-05-15 15:2...	2025-05-15 15:25...	Ignore
172.16.12.1	IPv4	-	-	10:c3:ab:fc:d4:2e	ARP Cache Scan	172.16.12.17...	2025-05-15 15:2...	2025-05-15 15:25...	Ignore

Steps:

- Create a scan task: Click Create Scan Task, fill in the basic settings, select a scan method, select the target host IP protocol, configure scan settings, and complete the task creation.
- View task list: Click "Scan Task List" to view the created tasks, including task status and execution time, and support editing, deleting, and immediate operation.
- View the list of discovered hosts: After the task is executed, the newly discovered hosts are displayed in the host discovery list, which can be filtered based on the relevant fields.
 - Export: You can export list data
 - Ignore hosts: You can add discovered hosts to ignore, after which the host will be

removed from the list, and subsequent scans will also ignore the host. It can be recovered in Ignore Host Management.

- **Ignore Hosts:** This list displays the information of all hosts that have been added to the ignore and supports removing and ignoring hosts. Once removed, the host will reappear in the host node discovery list.

CMDB Comparison Findings: The system automatically compares host data between local hosts and CMDB-synchronized hosts, quickly identifying hosts without the Agent installed. It is recommended to install the Agent promptly to reduce security risks. Click "Go to Install" to jump to the Agent installation page for operation. If you need to adjust CMDB synchronization configurations, click "CMDB Connection Configuration" to navigate to the CMDB connection configuration page.

Steps:

- **View Discovered Host List:** Newly discovered hosts are displayed in the Host Discovery List, and you can filter them based on relevant fields.
- **Export:** Supports exporting list data.
- **Ignore:** Allows adding discovered hosts to the ignore list. After being ignored, hosts will be removed from this list and skipped in subsequent scans. They can be restored in the "Ignored Host List".
- **Ignored Host List:** This list displays information of all hosts added to the ignore list and supports removing hosts from the ignore status. After removal, the hosts will reappear in the Host Node Discovery List.

The screenshot shows a user interface for 'CMDB Comparison Findings'. At the top, there are tabs for 'Internal Network Scan Discovery' and 'CMDB Comparison Findings', with the latter being active. Below the tabs, there are two informational messages: one about automatically comparing system hosts with CMDB-synchronized host data, and another about adjusting CMDB synchronization settings. A search bar and a filter button ('Please select filter content') are also present. The main area is a table titled 'Ignored Host List' containing 134 items. The columns include Host IP, Hostname, Business Group, Owner, Email, Host Location, Tags, Sync Time, and Operation. Each row lists a host entry with its details. At the bottom of the table, there are navigation links for page numbers (1, 2, 3, >) and an item per page dropdown set to 50.

Host IP	Hostname	Business Group	Owner	Email	Host Location	Tags	Sync Time	Operation
192.168.1.124	host_124	数据组	赵六	赵六@company.com	深圳机房	proxy,test	2025-10-24 19:00:00	Ignore
192.168.1.125	host_125	网络组	钱七	钱七@company.com	杭州机房	monitor,backup	2025-10-24 19:00:00	Ignore
192.168.1.126	host_126	安全组	孙八	孙八@company.com	成都机房	storage,standby	2025-10-24 19:00:00	Ignore
192.168.1.127	host_127	系统组	周九	周九@company.com	武汉机房	compute,active	2025-10-24 19:00:00	Ignore
192.168.1.128	host_128	监控组	吴十	吴十@company.com	西安机房	network,passive	2025-10-24 19:00:00	Ignore
192.168.1.129	host_129	运维组	张三	张三@company.com	北京机房	web,production	2025-10-24 19:00:00	Ignore
192.168.1.130	host_130	开发组	李四	李四@company.com	上海机房	database,staging	2025-10-24 19:00:00	Ignore
192.168.1.131	host_131	测试组	王五	王五@company.com	广州机房	cache,development	2025-10-24 19:00:00	Ignore

3.5.2. Container node discovery

Container Node Discovery is used to identify all hosts without container security authorization. On this page, you can inventory the container environments contained in the hosts and grant container security capabilities to such nodes for protection, thereby reducing security risks.

1. Statistics Area

You can view statistics on node environments, nodes with container environments, and nodes with unknown container environments. The definitions are as follows:

- **Node Environment Statistics:**
 - With container environment: Hosts in the current list where the value of "whether containing a container environment" is "Yes".
 - Without container environment: Hosts in the current list where the value of "whether containing a container environment" is "No".
 - Unknown container environment: Hosts in the current list where the value of "whether containing a container environment" is "Unknown".
- **Nodes with Container Environment:**
 - Total: Hosts in the current list where the value of "whether containing a container

environment" is "Yes".

- Pure container nodes: Nodes of type docker_node.
- Cluster nodes: Nodes of type k3s_node or k8s_node.
- Unknown Container Environment:
 - Total: Hosts in the current list where the value of "whether containing a container environment" is "Unknown".
 - Nodes with inventory failure: Hosts where the latest scan result is "Failed".
 - Uninventoried nodes: Hosts with no latest scan result.

2. Container Node Discovery List

The list displays all hosts without container security authorization. You can initiate scans on the hosts in the list to detect whether a container environment exists on the host.

- With container environment: Hosts with container runtime processes.
- Without container environment: Hosts with no detected container runtime processes.
- Unknown container environment: Hosts that have not been scanned or have failed scans.

3. Operation Instructions

- Container Node Discovery Scan: Multiple scanning methods are supported.
 - Scheduled scan: Click "Scan Configuration" to enable scheduled scanning, where you can configure the scan cycle and scan scope. This configuration is disabled by default.
 - Manual scan:
 - Click "Custom Scan" to select scanning all hosts, scanning by host, or scanning by business group, and trigger an immediate scan.
 - Alternatively, select specific hosts in the list or use the "Select All" button to select all hosts, then click "Batch Scan" to trigger an immediate scan.

- Configure Container Authorization:
 - Individual authorization: Click "Configure Container Authorization" in the operation column of the list to jump to the authorization configuration page for operation.
 - Batch authorization: Select specific hosts in the list or use the "Select All" button to select all hosts, then click "Batch Configuration" to jump to the "Create Authorization Task" on the authorization configuration page for operation.

The screenshot shows the 'Container Discovery' section of the Sentry CWPP interface. At the top, there are three summary boxes: 'Node Environment Statistics' (Includes Container Environment: 3, Non-Container Environment: 1, Unknown Container Environment: 14), 'Nodes with Container Environment' (3 Total, showing 2 Pure Container Nodes and 1 Cluster Node), and 'Unknown Container Environment' (14 Total, showing 0 Cleanup Failed Nodes and 14 Undeleted Nodes). Below these is a search bar and a table header with columns: Host, Business Group, Whether Includes C..., Number..., Container Runtime..., Node Type, Cluster Version, Sock File Path, Last Scan Time, Scanning R..., Operation. The table lists 18 items, each with a host IP, business group, whether it includes containers, number of containers, runtime version, node type, cluster version, sock file path, last scan time, scanning result (all successful), and an 'Operation' button labeled 'Configure Contain...'. The table has a 'Select All' button at the top right and a 'Custom Scan' button at the bottom right.

3.5.3. Cluster node discovery

Cluster nodes are found to monitor the cluster environment in real time through cluster components, identify resource nodes in the existing cluster that are not protected for security, and recommend that you install the agent in time to reduce security risks. Click Install Agent to jump to the agent installation page.

The screenshot shows the 'Cluster Discovery' section of the Sentry CWPP interface. It features a search bar and a table header with columns: Cluster, Node IP, Node Name, Node Type, First discovery time, Recently Discover.... The table currently shows 0 items. The table has a 'Search for Cluster Name' input at the top left and a 'Custom Scan' button at the bottom right.

Steps:

- This function relies on the security authorization of the cluster and the data collection

capabilities of the cluster components, and needs to be configured and installed first.

- You can count and display the information of nodes that do not have the agent installed in the cluster according to different clusters, and can filter them based on relevant conditions.
- List data can be exported.

3.6. Appendix: Custom Asset Fingerprints - Field Descriptions

 **Preparation:** Most of the rule content involves regular expressions. It is recommended to learn them in advance. Reference: <https://www.runoob.com/regexp/regexp-syntax.html>

3.6.1. Running Application

3.6.1.1. Rule Parameter Description

3.6.1.1.1. Basic Information

1. **Application Name:** Identifies the application name matched by the fingerprint. This application name must be unique, must strictly match the official application name and letter case from the official website, and cannot be modified after saving. Required field.
2. **Xinchuang (信创):** Whether the application to be identified is a Xinchuang application.
3. **Description:** Briefly introduce the running application. Optional field.

3.6.1.1.2. Rule Content

1. **Process Fingerprint:** Refers to the process information corresponding to the

application. If the application has multiple process names, multiple process fingerprints can be added. Multiple process fingerprints have an "OR" relationship.

- **Process Name:** Fill in the name in the corresponding process after the application starts, requiring exact matching. Required field.
 - Example 1: Bind application corresponds to the process name named
 - Example 2: Tomcat corresponds to the process name java
 - Example 3: Chrome [Windows] corresponds to the process name chrome.exe
- **Secondary Process Name:** When application process names are the same, the secondary process name is needed for further identification, generally used for Java applications. Java application process names are all java, the secondary process name is the content in parentheses of the Java process name, requiring exact matching. Non-Java processes do not need to fill in this field.
 - Example 1: Tomcat secondary process name is org.apache.catalina.startup.Bootstrap
 - Example 2: Jboss secondary process name is org.jboss.Main
- **Match Process Startup Parameters:** Match keywords in the process startup parameters to identify if it is this application, requires regex matching. Generally, it is the characteristic string in the startup parameters. Only some processed Java applications, Python applications, and Oracle need to fill this. Java applications include: weblogic, jenkins, activemq, tomcat, glassfish, jetty, resin, jboss, wildfly, websphere, kafka, flink, openfire.
 - Example 1: tomcat process startup parameter is ^tomcat\\$\
 - Example 2: django process startup parameter

is ^/.^python.*manage.py.^runserver

- Example 3: Apache process startup parameter does not need to be filled.

2. **Version Acquisition:** Parameters used to obtain the application version information [Only applicable to Linux OS]. After the application is installed, check if the correct version information is displayed in the process. If correctly identified, this parameter content may not need to be filled, and the version information is obtained directly from the process; if the version is not identified or is incorrectly identified, this parameter content needs to be filled.

Provides the following three version acquisition methods, which can be flexibly selected based on application characteristics:

- **Main Jar Package Version Matching:** Determine the application version number through the version of the main jar package. Main jar package path composition: home field name / supplementary directory name / jar package name. Multiple main jar package paths can be filled, multiple main jar package paths have an "OR" relationship. Note: If the main jar package is reflected in the command line parameters, the home field may not need to be configured. If the home name is not found in both the process environment variables and the command line parameters, and the main jar package is also not reflected in the command line parameters, the version cannot be obtained.

- **Home Field Name:** There are two acquisition methods, choose one, requires exact matching. Optional field.
 - Obtain from process environment variables: The home field name set in the process's environment variables, obtained from the result of executing cat /proc/\$pid/environ.

- Obtain from command line startup parameters: The home field name set in the command line startup parameters, find the application's home field name from the process's startup parameters.
- **Supplementary Directory Name:** The path that supplements the home directory. The jar package exists in a subdirectory of the home directory; use this field for concatenation, requires exact matching. Optional field.
- **Jar Package Name:** Match the main jar package name under this path using a regular expression. Required field.
- **Parameter Filling Method:**
 - Step 1: Determine the main jar package name.
 - In the process command line startup parameters after the application starts, find the Java main class (i.e., the secondary process name). Use the jar xvf command to see which classes are in the jar package. If this main class is found, it means this jar package is the main jar package.

```
root      31002      1  8 05:28 pts/0    00:00:26 /opt/jdk-11.0.11/bin/java -cp /opt/neo4j-enterprise-4.3.2/plugins/*:/opt/neo4j-enterprise-4.3.2/conf/*:/opt/neo4j-enterprise-4.3.2/lib/* -XX:+UseG1GC -XX:-OmitStackTraceInFastThrow -XX:+AlwaysPreTouch -XX:+UnlockExperimentalVMOptions -XX:+TrustFinalNonStaticFields -XX:+DisableExplicitGC -XX:MaxInlineLevel=15 -XX:-UseBiasedLocking -Djdk.nio.maxCachedBufferSize=262144 -Dio.netty.tryReflectionSetAccessible=true -Djdk.tls.ephemeralDHKeySize=2048 -Djdk.tls.rejectClientInitiatedRenegotiation=true -XX:FlightRecorderOptions=stackdepth=256 -XX:+UnlockDiagnosticVMOptions -XX:+DebugNonSafepoints -Dlog/j2-disable.jmx=true -Dfile.encoding=UTF-8 com.neo4j.server.enterprise.EnterpriseEntryPoint --home-dir=/opt/neo4j-enterprise-4.3.2
```

```
[root@localhost lib]# jar xvf neo4j-enterprise-4.3.2.jar | grep EnterpriseEntryPoint  
[已解压: com/neo4j/server/enterprise/EnterpriseEntryPoint.class]
```

○

■

- Step 2: Determine the location of the main jar package, i.e., its location relative to the home directory, find the home name of the environment variable that can locate the home directory.
 - Example 1: Find the home name from the process environment variables. After executing cat /proc/\$pid/environ, find the home name for the Sqoop application

is **SQOOP_HOME**.

```
...../bin:/opt/apache-zookeeper-3.6.2-bin/bin:/opt/spark-2.4.5-bin-hadoop2.7/bin:/opt/apache-kylin-3.1.1-bin-hbase1x//bin:/opt/hbase-1.4.13/bin:/opt/apache-hive-1.2.2-bin:/opt/hadoop-2.7.5/bin:/opt/hadoop-2.7.5/sbin:/opt/jdk1.8.0_261/bin:/opt/sqoop-1.4.7//bin:/opt/apache-zookeeper-3.6.2-bin/bin:/opt/spark-2.4.5-bin-hadoop2.7/bin:/opt/apache-kylin-3.1.1-bin-hbase1x//bin:/opt/hbase-1.4.13/bin:/opt/apache-hive-1.2.2-bin:/opt/hadoop-2.7.5/bin:/opt/hadoop-2.7.5/sbin:/opt/jdk1.8.0_261/bin:/usr/local/bin:/usr/sbin:/usr/bin:/root/binHISTSIZE=1000SQOOP_HOME=/opt/sqoop-1.99.7/KYLIN_HOME=/opt/apache-kylin-3.1.1-bin-hbase1x/LESSOPEN=||/usr/bin/lesspipe.sh:s_=:/opt/jdk1.8.0_261/bin/java[root@localhost ~]#
```

○

■

●

- Example 2: Obtain from command line startup parameters: Find the home name from the process's command line startup parameters. After executing ps -ef | grep xxx, find the home name for the Neo4j application is home-dir.

●

```

root      31002      1 99 05:28 pts/0    00:00:09 /opt/jdk-11.0.11/bin/java -cp /opt/neo4j-enterprise-4.3.2/plugins/*:/opt/neo4j-enterprise-4.3.2/conf/*:/opt/neo4j-enterprise-4.3.2/lib/* -XX:+UseG1GC -XX:-OmitStackTraceInFastThrow -XX:+AlwaysPreTouch -XX:+UnlockExperimentalVMOptions -XX:+TrustFinalNonStaticFields -XX:+DisableExplicitGC -XX:MaxInlineLevel=15 -XX:-UseBiasedLocking -Djdk.nio.maxCachedBufferSize=262144 -Dio.netty.tryReflectionSetAccessible=true -Djdk.tls.ephemeralDHKeySize=2048 -Djdk.tls.rejectClientInitiatedRenegotiation=true -XX:FlightRecorderOptions=stackdepth=256 -XX:+UnlockDiagnosticVMOptions -XX:+DebugNonSafepoints -Dlog4j2.disable.jmx=true -Dfile.encoding=UTF-8 com.neo4j.server.enterprise.EnterpriseEntryPoint --home-dir=/opt/neo4j-enterprise-4.3.2 --config-dir=/opt/neo4j-enterprise-4.3.2/conf

```

- The jar package is under home/lib of this application, so the value of the supplementary directory name is lib.

- Example

path: /opt/neo4j-enterprise-4.3.2/lib

```
[root@localhost lib]# pwd neo4j-enterprise-4.3.2.jar
/opt/neo4j-enterprise-4.3.2/lib
```

- Specific filling example description: Fill in the home field name (or obtain method), supplementary directory name, and jar package name regex.

Main JAR Package Version Matching
Determine the application version by locating the main JAR package. The main JAR path format: home field name / additional directory name / JAR file name

Home Field Name	Additional Directory Name	* JAR File Name ①
Extract from Command Line	home\lib	neo4j\enterprise-[1d\ S]*\jar
+ Add Delete		

- **Command Line Result Matching:** Execute a version query command in the command line and perform regex matching on the returned result for version information. Multiple command line matching results can be filled; multiple command line matching results have an "OR" relationship.
 - **Version Query Command:** Fill in the command line parameter to get the application version number, e.g., -v, --version parameter fields. Required field.
 - **Command Result:** Fill in the regular expression to obtain the version

number from the result returned after executing the command line parameter.

Required field.

- Specific filling example: After executing smbd -V, the return result is Version 4.10.16.

Command Output Matching

Execute a version query command in the command line and use a regular expression to extract version information from the output

* Version Query Command	* Command Output
-V	Version% <u>s*</u> ([.%d]+)% <u>s*</u>
+ Add	

•

○

- Note: After the application starts, if the process name is not itself (e.g., Python applications start with process name python), executing parameters like -v gets the Python version, not the correct application version.

- **File Content Matching:** For a small number of applications whose version cannot be obtained through the main jar package, find configuration files containing version number information and perform regex matching on the file content for version information. Multiple file content matching information has an "OR" relationship.

- **Home Field Name:** There are two acquisition methods. Optional field.
 - Obtain from process environment variables: The home field name set in the process's environment variables, fill in the corresponding home field name obtained from the result of executing cat /proc/\$pid/environ.

- Obtain from command line startup parameters: The home field name set in the command line startup parameters, fill in the application's home field name found from the process's startup parameters.
- **Supplementary Directory Name:** The path that supplements the home directory. The file exists in a subdirectory of the home directory; use this field for concatenation. Optional field.
- **File Name:** Fill in the name of the file containing the version number. Required field.
- **Version:** Match the version information in the content of the file under this path using a regular expression. Fill in the regex expression that can obtain the version based on characteristics in the version number file. Required field.
- Specific example description: (Mathematical formula in original text seems misplaced and is omitted here as it doesn't relate directly to the example).

File Content Matching
Match version information by searching configuration files containing version details using regular expressions

Home Field Name	Additional Directory Name	* file name	* Version ⓘ
Extract from Command Line	LOGSTASH_HOME	logstash-core	versions-gem-copy.yml
logstash%::%s*([%d]+)%s*			
+ Add			

3.6.2. Web Application

3.6.2.1. Rule Parameter Description

3.6.2.1.1. Basic Information

1. **Application Name:** Fill in the name of the web application. Required field. The web application name must be consistent with the naming and case on the corresponding official website, e.g., phpMyAdmin.

2. **Xinchuang (信创):** Whether the web application to be identified is a Xinchuang application.
3. **Description:** Fill in some basic information about the web application. Optional field.

3.6.2.1.2. Rule Content

1. **Identification Fingerprint:** Match the application name from the fingerprint file content. The web application is considered to exist if more than 3 fingerprint files are matched. To be compatible with different versions of the application, it is recommended to fill in about 10 fingerprint data entries; multiple fingerprint data entries have an "AND" relationship. Required field. The meanings of each field are as follows:

- **Fingerprint File Path:** The relative path of the fingerprint file under the web directory. Try to select files from multiple different directories.
- **Application Name:** Match the application name information in the fingerprint file content using a regular expression. Fill in the regex for the characteristic string of this web application in the corresponding fingerprint file content.
- **Parameter Filling Method:**
 - Prerequisite: Need to install ack on the machine where the web application is installed (Learn installation method:
<https://blog.csdn.net/zjw0411/article/details/79158342>). Use ack to execute commands (learn ack syntax by yourself) to obtain path information.
 - Take phpMyAdmin as an example:
 - Enter the directory of the web application "phpMyAdmin": cd /var/www/html/phpMyAdmin/

- Use ack to search for file directories containing "phpMyAdmin". Here, "phpMyAdmin" is the characteristic information for the phpMyAdmin application: ack 'phpMyAdmin'
- The list of files containing "phpMyAdmin" and specific information will be printed.

```
[root@bogon ~]# cd /var/www/html/phpMyAdmin-4.3.0/
```

```
[root@bogon phpMyAdmin-4.3.0]# ack -l 'phpMyAdmin'
```

ChangeLog

ack 检索到包含 phpMyAdmin 的文件列表

DCO

-l 参数表示不打印详情，

README

可不加参数显示出全部信息进行筛选加入规则中

changelog.php

chk_rel.php

composer.json

config.sample.inc.php

db_designer.php

db_operations.php

doc/Makefile

doc/conf.py

doc/config.rst

import.php

1.

○

■

- Based on the characteristic string "phpMyAdmin" and the file list retrieved by the characteristic string, fill in the identification fingerprint list.
- Note: The file path is a relative path. A '/' symbol needs to be added before the file path. When the web application performs identification fingerprint comparison, it will search for fingerprint files in the website root directory and its first-level subdirectories for matching.
- Specific example description shown in table format .

*Identif... : Match application name from fingerprint file content. The web application is considered present when more than three fingerprint files match. To support different application versions, it is recommended to provide about 10 fingerprint entries.

The screenshot shows a configuration page for identifying a web application. At the top, there are two required fields: "Fingerprint file path" and "application Name". Below these, a table lists several entries, each consisting of a path and an application name. Each entry has a delete icon to its right. A "Add" button is located at the bottom left of the list area.

Fingerprint file path	application Name
/ChangeLog	phpMyAdmin
/Libraries/common.inc.php	phpMyAdmin
/Changelog.php	phpMyAdmin
/config.sample.inc.php	phpMyAdmin
/index.php	phpMyAdmin
/README	phpMyAdmin

+ Add

2. Version Acquisition: After determining the existence of the corresponding web application by matching identification fingerprints, the version number of the web application needs to be obtained based on the path and regex in the version acquisition. Generally, the version number of a web application exists in some characteristic files under the web application directory. This item should have at least one rule filled in to obtain the web application version number. If multiple characteristic files exist, fill in multiple version acquisition rules. If the first rule fails to get the version number, it will try to match the second rule, and so on. Optional field. If not filled, the version cannot be obtained. The meanings of each field are as follows:

-

- **Version File Path:** Fill in the path of the file containing the version number. It is the relative path of the file under the site directory. Required field.
- **Version Number:** Match the version number information in the file content using a regular expression. Fill in the regex used to match the version. Required field.
- **Parameter Filling Method:**
 - Take phpMyAdmin as an example:
 - Enter the directory of the web application "phpMyAdmin": cd /var/www/html/phpMyAdmin/
 - Use ack to search for files where the application's version number exists.

If the downloaded version is known (e.g., 4.3.0), use the command: ack '4.3.0' to search for the file path containing this version number. If the downloaded version is unknown, use ack 'version' to manually determine possible files containing the version number, and open the corresponding file to check if the content describes the application's version information.

```
[root@bogon ~]# cd /var/www/html/phpMyAdmin-4.3.0/  
[root@bogon phpMyAdmin-4.3.0]# ack 'Version 4.3.0'  
README  
4:Version 4.3.0  
[root@bogon phpMyAdmin-4.3.0]#
```

应直接搜索实际版本号，这里为了显示版本号前后字符串定位信息能打印出来故而为之

- - Based on the obtained characteristic information of the version number, the surrounding strings, and the file where the version number exists, create the version acquisition list.
 - The version number regex is the regex containing the characteristic string of the version number. Since the version number needs to be written as a regex to capture the version, and the version number usually follows (or precedes) a string, the regex needs to first check if the string before the version number indicates its location, then the regex returns the version number following the string.

- The regex is generally: $(?<=Version\s)((\d)+(\.(\d)+)+.*),$ where Version\s is the regex for the string before the version number and can be replaced.
- The version file path is the directory of the file containing the version number.
- Note: The file path is a relative path. A '/' symbol needs to be added before the file path. When the web application performs identification fingerprint comparison, it will search for fingerprint files in the website root directory and its first-level subdirectories for matching.
- Specific example description shown in table format:

Version ...: Version Detection

Enter file paths containing version numbers and corresponding regular expressions for version matching. Multiple entries are allowed to support different application versions.

* Version file path	* Version Number ⓘ
/README	(?<=Version\s)((\d)+(\.(\d)+)+.*)

[+ Add](#)

3.6.3. Web Framework

3.6.3.1. PHP Framework

3.6.3.1.1. Rule Parameter Description

3.6.3.1.1.1. Basic Information

1. **Application Name:** Fill in the framework name. Must strictly match the official application name and letter case from the official website. Required field. Example: ThinkPHP
2. **Xinchuang (信创):** Whether the PHP framework to be identified is a Xinchuang

application.

3. **Description:** Fill in a brief introduction of the framework, which can be obtained from the official website. Optional field.

3.1.1.2 Rule Content

1. **Identification Fingerprint:** Locate the file name and path containing the module fingerprint, and fill in the module fingerprint string in the file to identify the PHP framework. To be compatible with different versions of the framework, it is recommended to enter about 10 fingerprint information entries; multiple fingerprint data entries have an "AND" relationship. Required field. The meanings of each field are as follows:

- **Fingerprint File Path:** Fill in the path information of the identification fingerprint. This is a relative path. Try to select files from multiple different directories.
- **Framework Name:** Match the framework name information in the fingerprint file content using a regular expression. Fill in the characteristic regex of the framework name.
- **Parameter Filling Method:**
 - Prerequisite: Need to install ack on the machine where the PHP framework is installed (Learn installation method: <https://blog.csdn.net/zjw0411/article/details/79158342>). Use ack to execute commands (learn ack syntax by yourself) to obtain path information.
 - Take ThinkPHP as an example:
 - Enter the directory of the PHP framework ThinkPHP: cd /var/www/html/ThinkPHP/
 - Use ack to search for file directories containing "ThinkPHP". Here,

"ThinkPHP" is the characteristic information for the ThinkPHP

application: ack 'think' or ack 'thinkphp|THINK_VERSION|ThinkPHP'

- The list of files containing "ThinkPHP" and specific information will be printed.
- Based on the characteristic string "ThinkPHP" and the file list retrieved by the characteristic string, fill in the identification fingerprint list.
 - Note: The file path is a relative path. A '/' symbol needs to be added before the file path. When the web framework performs identification fingerprint comparison, it will search for fingerprint files in the website root directory and its first-level subdirectories for matching.
- Specific example description shown in table format.

* Identif... : Match Framework name from fingerprint file content. The web Framework is considered present when more than three fingerprint files match. To support different Framework versions, it is recommended to provide about 10 fingerprint entries.

* Fingerprint file path	* Framework Name ⓘ
/application/common.php	ThinkPHP
/build.php	ThinkPHP
/config/app.php	ThinkPHP
/LICENSE.txt	ThinkPHP
/public/index.php	ThinkPHP
/route/route.php	ThinkPHP

+ Add

2. Version Acquisition: Fill in the version identification information of the framework. One or more entries can be filled. If the first rule does not match, continue matching subsequent rules. If there are differences between versions, enter multiple entries for version compatibility. Optional field.

The meanings of each field are as follows:

-

- **Version File Path:** The path of the file containing the version number. It is the relative path of the file under the site directory. Required field.

- **Version Number:** The regular expression that can obtain the version based on characteristics in the corresponding file containing the version number. Required field.
- **Parameter Filling Method:**
 - Prerequisite: Need to install ack on the machine where the web application is installed. Use ack to execute commands to obtain path information.
 - Take ThinkPHP as an example:
 - Enter the directory of the PHP framework ThinkPHP: cd /var/www/html/ThinkPHP/
 - Use ack to search for files where the application's version number exists. If the downloaded version is known, use the command: ack 'version_number' to search for the file path containing this version number. If the downloaded version is unknown, use ack 'version' to manually determine possible files containing the version number, and open the corresponding file to check if the content describes the application's version information.
 - Based on the obtained characteristic information of the version number, the surrounding strings, and the file where the version number exists, create the version acquisition list.
 - The version file path is the directory of the file containing the version number.
 - The version number regex is the regex containing the characteristic string of the version number. Since the version number needs to be written as a regex to capture the version, and the version number

usually follows (or precedes) a string, the regex needs to first check if the string before the version number indicates its location, then the regex returns the version number following the string.

- The regex is generally: `(?<=Version\s)((\d)+(\.(\\d)+)+.*),` where Version\s is the regex for the string before the version number and can be replaced.
- Note: The file path is a relative path. A '/' symbol needs to be added before the file path. When the web framework performs identification fingerprint comparison, it will search for fingerprint files in the website root directory and its first-level subdirectories for matching.
- Specific example description shown in table format.

Version ... : Version Detection

Enter file paths containing version numbers and corresponding regular expressions for version matching. Multiple entries are allowed to support different Framework versions.

*Version file path	*Version Number ⓘ
/thinkphp/base.php	<code>(?<='THINK VERSION',\s')((\d)+(\.(\\d)+)+)</code>
OR /CHANGELOG.md	<code>(?<=V)((\d)+(\.(\\d)+)+)</code>
+ Add	

3.6.3.2. Python Framework

3.6.3.2.1. Rule Parameter Description

3.6.3.2.1.1. Basic Information

1. **Framework Name:** Fill in the framework name. Must strictly match the official application name and letter case from the official website. Required field.
2. **Xinchuang (信创):** Whether the framework to be identified is a Xinchuang application.
3. **Description:** Fill in a brief introduction of the framework, which can be obtained from

the official website. Optional field.

3.6.3.2.1.2. Rule Content

1. **Identification Fingerprint:** Locate the file name and path containing the module fingerprint, and fill in the module fingerprint string in the file to identify the Python framework. Multiple identification fingerprints have an "AND" relationship. The meanings of each field are as follows:

- **Module Name:** Fill in the Python module name.
- **Fingerprint File Path:** Fill in the folder path containing the module fingerprint.
Find the module path based on the module name. You can execute modules.__path__ or modules.path command in Python interactive mode to get the module path. You can fill in a string or regex; regex needs to be written within [[]].
- **Fingerprint File Name:** Fill in the file name containing the module fingerprint.
Find the characteristic file in the folder containing the module fingerprint.
- **Framework Name:** Fill in the regular expression for the module fingerprint string in the characteristic file. The official domain name must be used because there are risks of multiple packages or modules with the same name in the Python ecosystem. To avoid naming conflicts, clarify official attributes, standardize dependency management, and follow the agreed representation convention of Apache projects. Example: Use airflow.apache.org instead of airflow.

* Identif... : Locate files containing module fingerprints; enter the module fingerprint string from the file to identify the Python framework.

* Module Name	* Fingerprint file path	* Fingerprint File Name	* Framework Name ⓘ
django	[[Django-\d+\.\d+\.\d+\.dist\-\info]]	METADATA	www.djangoproject.com
django	/EGG-INFO	PKG-INFO	www.djangoproject.com

[+ Add](#)

2.Version Acquisition: After obtaining the fingerprint file, version identification can be completed through version matching in the fingerprint file content, version attribute information matching, or command line result matching. Multiple rules can be entered to accommodate differences between versions; multiple rules have an "OR" relationship. The meanings of the identification methods are as follows:

-

- **File Content Matching:** Match version information in the fingerprint file content using a regular expression.
- **Version Attribute Matching:** Match version information by obtaining __version__ or module.version using a regular expression.
- **Command Line Result Matching:** Match the version result returned in the command line using a regular expression.
- **Parameter Filling Method:**
 - **Version Matching Regex:** Fill in the regular expression to match the version. The version regex will be used to match the version in the characteristic file from the fingerprint file identification or the command line return result.
 - Example: \s*Version:\s+(\d+\.\d+\.\d+)
 - **Version Attribute:** Generally fill in as version or __version__. Fill if exists, otherwise leave blank.
 - Example: Django version attribute is __version__.
 - **Version Acquisition Command:** For frameworks that require command line execution to obtain the version, fill in the execution command.

- Example: web2py requires executing the command web2py.py --version.
- Specific example description shown in table format.

Version ... : Version Detection
After obtaining the fingerprint file, version identification can be completed by matching file content, version attributes, or command-line output. Multiple rules can be entered to accommodate differences across versions.

* Identification Method	* Version Detection
File Content Matching	<code>^Version:\s+(\d+\.\d+\.\d+)</code>
OR	<code>_version_</code>
OR	<code>web2py.py -version</code>
+ Add	

3.6.3.3. Java Framework

3.6.3.3.1. Rule Parameter Description

3.6.3.3.1.1. Basic Information

1. **Framework Name:** Fill in the framework name. Must strictly match the official application name and letter case from the official website. Required field.
2. **Xinchuang (信创):** Whether the application framework to be identified is a Xinchuang application.
3. **Description:** Fill in a brief introduction of the framework, which can be obtained from the official website. Optional field.

3.3.1.2 Rule Content

1. **Identification Fingerprint:** After the application is installed, check if the correct version information is displayed in the process. If correctly identified, this parameter content may not need to be filled, and the version information is obtained directly from the process; if not correctly identified, the framework's fingerprint information needs to be filled to identify different Java frameworks.

One or more of the following identification methods can be selected. The identification priority decreases in order. If a high-priority rule matches successfully, the identification process ends and does not continue matching.

- **MD5 Matching:** Obtain the MD5 value of the corresponding framework version from the application's official website and compare it with the framework information on the host. If they are consistent, confirm the framework and version information.

Multiple matching entries have an "OR" relationship.

- **Version:** Fill in the Java framework version.
- **MD5 Value:** Fill in the MD5 value of the corresponding version of the Java framework. The MD5 value can be obtained from the official website.
- **Example:**

MD5 Matching
Obtain the MD5 hash of the target framework version from the official website and compare it with the framework file on the host. A match confirms the framework and its version.

Version	* MD5 Value
2.3.20	d2727badff5ec6c76e1d741ff53cf43

+ Add

- **pom.xml File Content Matching:** Obtain framework fingerprints from the content of nodes like groupId, artifactId, name in the pom.xml file. Multiple file content matching entries have an "AND" relationship.
 - **Locate Framework Name Node:** Fill in the XPath syntax for the characteristic string of the Java framework.
 - **Framework Name:** Fill in the regular expression to match the characteristic string of the framework.
- **Example:** The pom.xml file content for struts2 is shown.

```

<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/pom-4.0.0.xsd">
  <parent>
    <groupId>org.apache.struts</groupId>
    <artifactId>struts-master</artifactId>
    <version>13</version>
  </parent>
  <modelVersion>4.0.0</modelVersion>
  <artifactId>struts2-parent</artifactId>
  <version>2.5.22</version>
  <packaging> pom </packaging>
  <name>Struts 2</name>
  <url>http://struts.apache.org/</url>
  <description>Apache Struts 2</description>

```

pom.xml File Content Matching

Extract framework fingerprints from nodes in pom.xml such as groupId, artifactId, or name

* Locate Framework Name Node	* Framework Name
/*[name()='project']/*[name()='name']/text()	^Struts2\$
<input style="margin-right: 10px;" type="button" value="+"/> Add <input style="margin-left: 10px;" type="button" value="Delete"/>	

- **Jar Package Information Matching:** Obtain framework fingerprint

characteristics by matching the package name and version information in the jar package. Multiple jar package information entries have an "AND" relationship.

- **Jar Package Name:** Fill in the regular expression to match the jar package name.
- Example: The jar package name corresponding to struts2 is ^struts2\-\core\-\d.*.

JAR package information matching

By matching the package name and version information in the JAR package, framework fingerprint characteristics can be obtained.

* JAR File Name	
^struts2\-\core\-\d.*	
<input style="margin-right: 10px;" type="button" value="+"/> Add <input style="margin-left: 10px;" type="button" value="Delete"/>	

- **Framework Class Fingerprint Matching:** Based on Java's package rules,

confirm that a specific class is contained under a specific package name, which can serve as a rule characteristic.

- **Package Name:** Fill in the specific package name. The package name is a string and must be filled in strictly according to case.
- **Class Name:** Fill in the specific class name in the specific package. The class name is a string and must be filled in strictly according to case.
- Example: The package name and class name for the struts2 framework are shown.

Framework class fingerprint matching

Based on Java's package rules, the presence of specific classes under a given package name can serve as a rule characteristic.

* Package Name	* Class Name
<input type="text" value="org.apache.struts2"/>	<input type="text" value="StrutsConstants.class"/>
+ Add	

4. Intrusion Detection

Traditional intrusion protection solutions are effective at defending against known attacks, but cannot deal with unknown and rapidly evolving attack methods. Therefore, achieving effective intrusion detection and providing real-time alerts and response mechanisms has become an urgent issue in security infrastructure. While current attack methods are constantly changing, the actions taken after a successful attack are standardized. As a result, intrusion detection shifts its focus from understanding hackers' attack methods to continuously monitoring and analyzing internal indicators. By integrating various analytical methods such as IoC (Indicators of Compromise), big data, and machine learning, it accurately detects intrusion events and provides notification methods including SMS, email, WeCom, and DingTalk, ensuring users are informed of intrusions in real-time. Additionally, depending on the intrusion scenario, Intrusion Detection offers multiple response methods such as manual/automatic process termination, file isolation, network blocking, and host isolation, enabling users to fundamentally resolve intrusion incidents with "high efficiency and diversity."

Note: Features in the document are tied to licensing. If the corresponding license is not purchased, the related features will not be visible.

4.1. Intrusion Detection Configuration and Response

4.1.1. Monitoring Configuration

4.1.1.1. Detection Configuration

The screenshot shows the 'Detection Configuration' page. At the top, there are four configuration steps: 'Install Plugins', 'Enable Driver', 'Enable Event Source', and 'Install Local Antivirus Engine'. Below these are tabs for different platform types: 'Linux-Server' (selected), 'Windows-Server', 'Linux-PC', 'Windows-PC', and 'Cluster'. A red box highlights the 'Linux-Server' tab. Under 'System Default Configuration', there is a table with columns for 'Include' (18 Item Configuration), 'Application Scope' (10.106.108.215 Total 9 devices), 'Detection Sensitivity' (Broad), and 'Update Time' (2025-02-07 14:25:27). In the 'User Defined Configuration' section, there is a table header with columns for 'Configuration Name', 'Application Scope', 'Update Time', 'Operation', and a delete icon. A note at the bottom states: 'Custom detection configurations primarily address scenarios where specific devices need individual detection items. The host scope of custom configurations cannot be duplicated, meaning each device can only have one detection configuration applied (if there is a conflict between host and group configurations, the host configuration takes priority). When a new host is onboarded, if no matching custom configuration is found, the system's default configuration will be applied.' A blue 'Create Configuration' button is located at the top right of this section.

The system provides default detection configurations for different platform types. After installing the probe, users can protect against most intrusion capabilities without additional configuration. Some intrusion capabilities depend on plugins, event sources, or drivers, which require prior configuration for proper protection. For example, Linux process injection protection requires enabling one of the audit event source, ebpf event source, or driver event source. Windows process injection protection requires enabling the driver, and suspicious command auditing requires installing the corresponding plugin. PC devices' intrusion blocking capabilities require enabling the driver. Dependencies can be viewed in the detection configuration interface.

The screenshot shows the 'Detection Configuration' page with the same configuration steps and tabs as the previous screenshot. A red box highlights the 'Enable Driver' step. A note at the top states: 'To ensure proper functionality, please configure the following:' followed by the four configuration steps: 'Install Plugins', 'Enable Driver', 'Enable Event Source', and 'Install Local Antivirus Engine'.

If users need the following capabilities, the driver must be enabled:

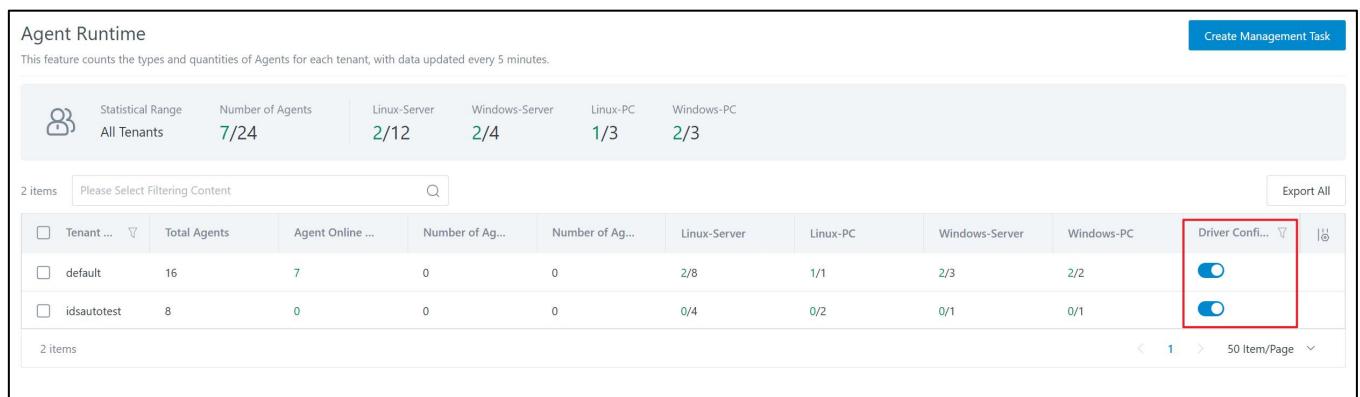
分类	功能	Linux-Server	Linux-PC	Windows-Server	Windows-PC

Intrusion Detection Capability	Malicious Driver Protection (also requires enabling the driver event source)	✓	✓		
	Windows Process Injection Detection		✓	✓	
	Shellcode Abnormal Process Loading Detection		✓	✓	
Alarm Response Capability	Blocking based on Process Hash	✓		✓	
	Blocking based on Process Behavior	✓		✓	
	Maliciou Driver Blocking	✓		✓	
	Malicious Modecule Loading Blocking	✓		✓	
	Access to Malicious IP and Domain Name Blocking	✓		✓	
	Credential Theft Blocking	✓		✓	
	Whitelist Application Exploitation Blocking	✓		✓	
	Windows Process Injection				✓

	Blocking				
	shellcode Abnormal Process				✓
	Loading Blocking				

Driver enabling steps:

- Enable the driver master switch. Go to Tenant Management - Agent - Agent Runtime. The "Driver Configuration" column in the list represents the tenant's driver master switch. Only when this switch is turned on will the driver-related configuration switches appear on the tenant's intrusion function configuration pages.



The screenshot shows the "Agent Runtime" section of the Sentry CWPP interface. At the top, it displays tenant statistics: All Tenants (7/24), Linux-Server (2/12), Windows-Server (2/4), Linux-PC (1/3), and Windows-PC (2/3). Below this is a table with two items. The columns include Tenant ID, Total Agents, Agent Online, Number of Agents, Number of Ag..., Linux-Server, Linux-PC, Windows-Server, Windows-PC, and Driver Config... (which is highlighted with a red box). The first row shows a tenant with 16 total agents, 7 online, and 0 drivers enabled. The second row shows a tenant with 8 total agents, 0 online, and 0 drivers enabled. The bottom right corner of the table shows a "50 Item/Page" dropdown.

- Enable Agent driver. After the administrator enables the driver master switch, each Agent needs to enable the driver switch again to allow the use of the driver. The system supports enabling the driver for individual Agents or batch enabling through management tasks.
 - Enable driver individually:
 - Go to Probes Probes Management- Agent, click "Details" in the Agent list, and select "Enable Driver" in the upper right corner "Operation and Maintenance" menu.

The screenshot shows the 'Agent Details' page for an agent with Agent ID [REDACTED] and Agent Version 3.8.0.0-250. A context menu is open under 'Operation and Maintenance' with options: Restart, Uninstall, Upgrade, and Enable Driver (which is highlighted with a red box).

•

- Enable driver in batch:

- Method 1: Go to Probe Management - Agent Management page, click **Create Management Task**, select "Enable Driver" as the task type, and specify the Agent range.

The 'Create Management Task' dialog box is shown. The 'Task Ty... : Enable Driver' dropdown is highlighted with a red box. Other fields include 'Task Na... : Agent_Enable Driver_20250225121224', 'Push S... : 100 hosts/min', 'Executi... : Once' (radio button selected), 'Duration: 0 Minutes', and 'Executi... : All Hosts' (radio button selected). Below 'All Hosts' are three other options: 'Select Hosts by List', 'Select Hosts by Business Group', and 'Select Hosts by Cluster'. The 'All Hosts' option is highlighted with a blue background.

•

-

- Method 2: In the Agent list, check the boxes of the Agents that need to enable the driver, and select "Enable Driver" in the more operations menu.

2/16 selected		Please Select Filtering Content										Export	More Operations
Running...	Agent ID	Host	Host Ty...	Agent Version	Running ...	Latest Online Time	Last...	Restart					
<input checked="" type="checkbox"/> Host	●	Host	Server Version	Normal	2025-02-25 11:16:13	20	Uninstall						
<input checked="" type="checkbox"/> Host	●	Host	PC Version	Normal	2025-02-25 10:43:15	-	Upgrade						
<input type="checkbox"/> Host	●	Host	PC Version	Normal	2025-02-25 10:39:19	-	Set Log Level						
<input type="checkbox"/> Host	●	Host	Server Version	Normal	2025-02-25 09:57:37	20	Set Run Level						
<input type="checkbox"/> Host	●	Host	Server Version	Normal	2025-02-24 17:20:16	-	Performance						
<input type="checkbox"/> Host	●	Host	Server Version	Normal	2025-02-21 16:29:36	20	Enable Driver						
<input type="checkbox"/> Host	●	Host	Server Version	Normal	2025-02-21 16:29:36	20	Disable Driver						

The system also supports custom configurations. A host can only apply to one detection configuration. When a host is customized, it will be removed from the application scope of the system default configuration, and the host will use the custom configuration for security protection.

- System default configuration: Newly added hosts use the system default configuration by default.
- User custom configuration: When specific devices require separate detection capabilities, click "Create Configuration" to create a custom configuration.

Select the corresponding platform type, enter the configuration details interface, and configure the intrusion detection capabilities for that type. Click  to configure specific detection capabilities, as shown below:

Linux-Server System Default Configuration

Cancel Save

Detection Sensitivity Configuration

Strict
Only report high-confidence alarms.

Balance
Report all suspicious alerts

Broad
Report all alerts
⚠ Enabling this may generate a large number of low-confidence alerts. Proceed with caution!

Configuration Details

Malicious Process Protection	Opened 6	Not Enabled 0
Process Injection Detection	<input checked="" type="checkbox"/>	
Real-time monitoring of running processes in the system. If process injection behavior is detected, alarms will be reported in real-time.		
Malicious Module Loading Detection	<input checked="" type="checkbox"/>	
For devices with installed drivers, monitor the loading behavior of processes. If a loaded module is suspected to be malicious, an alert will be reported.		
Binary Padding Detection	<input checked="" type="checkbox"/>	
Real-time monitoring of process startup in the system. If an attempt is made to pad the binary file to bypass detection, alarms will be reported in real-time.		
Process Access to Malicious IP Monitoring	<input checked="" type="checkbox"/>	
Real-time monitoring of the network connection behavior of processes in the system. If a process is found accessing malicious IPs, alarms will be reported.		
Hidden Process Scan	<input checked="" type="checkbox"/>	
Scans for potentially hidden processes in the system. Users can customize the specified scanning period, and the system will execute scans according to the set schedule.		
Scan Management	View Scanned Records	
Malicious File Self-Deletion Detection	<input checked="" type="checkbox"/>	
Real-time monitoring of file deletion behavior; an alert will be reported if a process is detected deleting its own files or its parent process files.		

Note:

- The configuration details interface does not display all detection capabilities. Detection capabilities that do not require configuration, such as reverse shell, will not appear in the configuration details interface.
- The number of "Not Enabled" can be used to determine if all functions of the corresponding detection capability are enabled.
- The default configuration includes "Alert Sensitivity Configuration." Different alert sensitivity levels can be selected based on actual conditions. It is recommended to choose "Strict Mode" or "Balanced Mode" to avoid generating too many low-confidence alerts, which can increase operational burden. The system defaults to "Strict Mode."
 - Strict Mode: Only reports high-confidence alerts, meaning only "Critical" and "High" severity alerts will appear in the alert list.
 - Balanced Mode: Only reports suspicious alerts, meaning only "Critical," "High," and "Medium" severity alerts will appear in the alert list.
 - Broad Mode: Reports all alerts. Using this mode, users may receive a large number of low-severity alerts.
- Different platform types can have different alert sensitivity settings. The same platform type's alert sensitivity also applies to custom detection configurations. For example, if the alert sensitivity is set to "Broad" in the system default configuration for Linux-Server, all alerts will be reported for Linux-Server hosts, whether in the system default configuration or custom configuration.
- Historical alerts are not affected by alert sensitivity. For example, if the alert sensitivity is initially set to "Strict Mode," only critical alerts will be reported. After changing to "Broad Mode," newly generated alerts will include "High," "Medium," and "Low" severity alerts.

4.1.1.2. Scan Detection

Some intrusion detection capabilities support scan detection, such as Webshell protection. By creating scan tasks, the system can scan the web directories on hosts to detect the presence of Webshells. The system supports single or scheduled scan tasks.

4.1.1.2.1. Single Scan

In the "Detection List" interface, click "Manual Scan" in the upper right corner of the table to display supported scan capabilities. Select the desired type to create a single scan task.

Click "Scan Records" to view all historical scan task information, including single and scheduled scan task execution records.

The screenshot shows the 'Detection List' interface. At the top, there are filters for 'Group by' (All, Host, Container, Cluster), a total count of '194 alarms', and a 'Select All' button. Below this is a table with columns: Risk Level, Detection Time, Alarm Type, Description, and Affected Devices. Three rows of data are visible, each with a checkbox and a yellow diamond icon. To the right of the table is a context menu with a red border, containing options: 'Manual Scan' (with a dropdown arrow), 'Export all', 'Webshell防护', 'Virus File Sear...', '内存后门检测', 'WMI扫描', '计划任务', '注册表扫描', '程序劫持', and 'Scan Records'. Each option has a small icon next to it.

4.1.1.2.2. Scheduled Scan

Scheduled scan tasks need to be configured in the "Detection Configuration" page, such as Webshell protection, as shown below:

- Scan Management: Create scheduled scan tasks.
- View Scanned Records: Same as the "Scan Records" function in the "Alert List" interface, it allows viewing all historical scan task execution records.

Hidden Process Scan

Scans for potentially hidden processes in the system. Users can customize the specified scanning period, and the system will execute scans according to the set schedule.

[Scan Management](#) [View Scanned Records](#)

4.1.1.3. Custom Detection Rules

Whether in "Detection Configuration" or "Scan Detection," threat alerts are detected based on system-built detection rules. The system also supports users creating custom detection rules based on their needs.

4.1.1.3.1. Custom IOA

In the "Custom IOA" interface, users can customize rules from multiple dimensions such as processes, files, and suspicious commands. When a custom rule is triggered, the system will report an alert.

Note: To avoid frequent synchronization consuming significant resources, custom rules are not synchronized to the Agent side immediately after saving. It is recommended to complete all rule creation before clicking the "Synchronize" button to synchronize the rules to the Agent side, ensuring the rules take effect.

The screenshot shows the "Custom IOA" section. On the left, a sidebar lists various file types: Executable File, Kubernetes Log, Script File, Configuration File, Web File, Suspicious cmd Opera..., PowerShell Suspicious..., and Suspicious bash Oper... A red box highlights the "Process Behavior" category. The main area displays a table of detected processes. The table has columns: Rule ID, Status, Alarm Type, Detection Title, Affected Alar..., Update Time, and Operation. One entry is shown: U-26deb80c02fd4ee75, which is a self-defined suspicious process. The detection title is "发现进程命中进程行为自定义规则". The update time is 2025-02-18 10:17:54.

4.1.1.3.2. Custom IOC

If users obtain black hashes, malicious IPs, or malicious domains from threat intelligence, real alerts, or other sources, they can enter this information in the "Custom IOC" interface to enable the system to detect and block threat behaviors promptly.

Note:

- Only Agents with the driver enabled have blocking capabilities. Without the driver, Agents only report alert information. The driver can be enabled in the "Tenant Management - Agent - Agent Runtime".
- Malicious hashes found in high-confidence alerts will be automatically added to the black hash list to notify other devices to avoid infection by the malicious file.

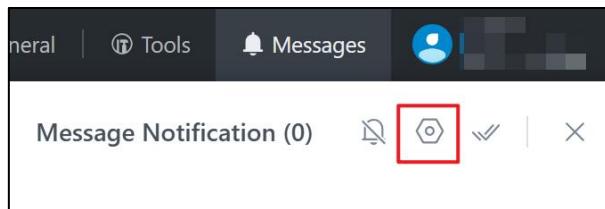
The screenshot shows the "Custom IOC" section. At the top, there are three tabs: Malicious Hash (highlighted with a red box), Malicious Ip, and Malicious Domain. Below the tabs, a note states: "Supports users in marking executable file hash values as black hash through new entries and alert detection reporting. Once blacklisted, the driver will block its execution. Note: During driver detection, the whitelist has a higher priority than the blacklist." The main area displays a table of blacklisted hashes. The table has columns: Rule ID, Value Type, Value, Notes, Update Time, Data Source, and Operation. There are 213 items listed.

4.1.2. Detection Notification

The system reports alerts immediately upon detecting threats. Before using the system, configure

alert notifications to receive alerts promptly.

Go to the "Message Center - Notification Configuration" interface and configure alert notifications as needed, such as configuring alert types, notification methods, recipients, and setting notifications based on severity levels.



4.1.3. Detections Viewing

Users can view each alert in the "Alert List" and view threat events in the "Event List."

- **Alert List:** Displays each reported alert. When an alert is associated with an event, click in the alert list to view the associated event.
- **Event List:** Aggregated from alerts, it is a collection of related alerts aimed at helping users view the complete intrusion process from an attack chain perspective.

4.1.3.1. Detection List

The screenshot shows the "Detection List" interface with the following data:

Risk Level	Alarm Type	Affected Device Type	Status	Time Range
危急	本地提权	主机	未处理	今天 12
高危	BypassUAC	容器	处理中	Last 1 Hour 3
中危	反弹shell	集群	已确认	Last 1 Day 21
低危	自定义可疑进程 可疑网络扫描 可疑注册表操作		已忽略	Last 7 Days 195 Last 30 Days 1937 Custom...

Group by: All Host Container Cluster Total 195 alarms Select All Last active Descending | Mark All | Manual Scan | Export all

Click to enter the "Detection List" interface, which by default only displays "Critical Risk," "High Risk," and "Medium Risk" severity alerts from the last 7 days. Alerts can be filtered and viewed from different dimensions, and only alerts within the user's permission scope can be viewed.

To view low-severity alerts in the "Detection List" interface, configure as follows:

- Step 1: Set the alert sensitivity to "Broad" in the "Detection Configuration" interface.
- Step 2: Filter alerts with "Low Risk" severity in the "Detection List" interface.

Note: Changing the alert sensitivity only affects future alerts. Only newly generated low-severity alerts will appear in the "Detection List" interface.

Click in each alert in the alert list or directly click the alert to view alert details, including alert ID, affected devices, techniques or tactics, detection information such as hit content, file information such as affected file paths and types, process chain information such as process names and command lines, and handling suggestions.

Different alerts display different information in the details interface. Users can perform relevant analysis based on the alert details.

The screenshot shows an alert titled "Medium Risk Abnormal Login". The main message is: "Detected IP 192.168.1.10 logging into device 192.168.1.10 using account vagrant, which is outside the normal login range." Below this, there are three action buttons: "Network Ban" (disabled), "Add to Normal Login Range" (selected), and "Pending". The "Detection Information" section includes fields for Detection Time (2025-02-25 11:21:13), ID (redacted), Response Result (-), Affected Devices (Windows 10), and Tactic & Technique (Cloud Account (T1078.004) / Initial Access).

Click the search box in the figure below to display search options. Users can filter alert information through search options, such as host IP, business group, alert description, operating system, etc.

The search bar at the top of the interface includes filters for "Time Range: Last 7 Days", "Risk Level: Critical Risk, High Risk, Medium Risk", and a placeholder text field: "Please manually enter the content you want to inquire after the colon and press Enter to finish."

The system also supports exporting filtered alert data in full or in batches.

4.1.3.2. Event List

Events are collections of related alerts aimed at viewing the complete intrusion process.

The "Incidents" page displays a single event entry. The summary shows a score of 10/10, detections for "Customize Suspicious Processes: Custom..." and "+6 alarms", affected devices (1 redacted), timeline from 2025-02-24 14:48:41 to 2025-02-25 12:17:38, status "In Progress", and operation "Details".

Note:

- The score is calculated by the system's internal algorithm, with 10 being the highest score. The higher the score, the greater the event risk.
- Events with scores below 5 are not displayed in the event list.
- Event scores may change and are recalculated based on associated alerts. If new associated

alerts are reported, the event score will be recalculated.

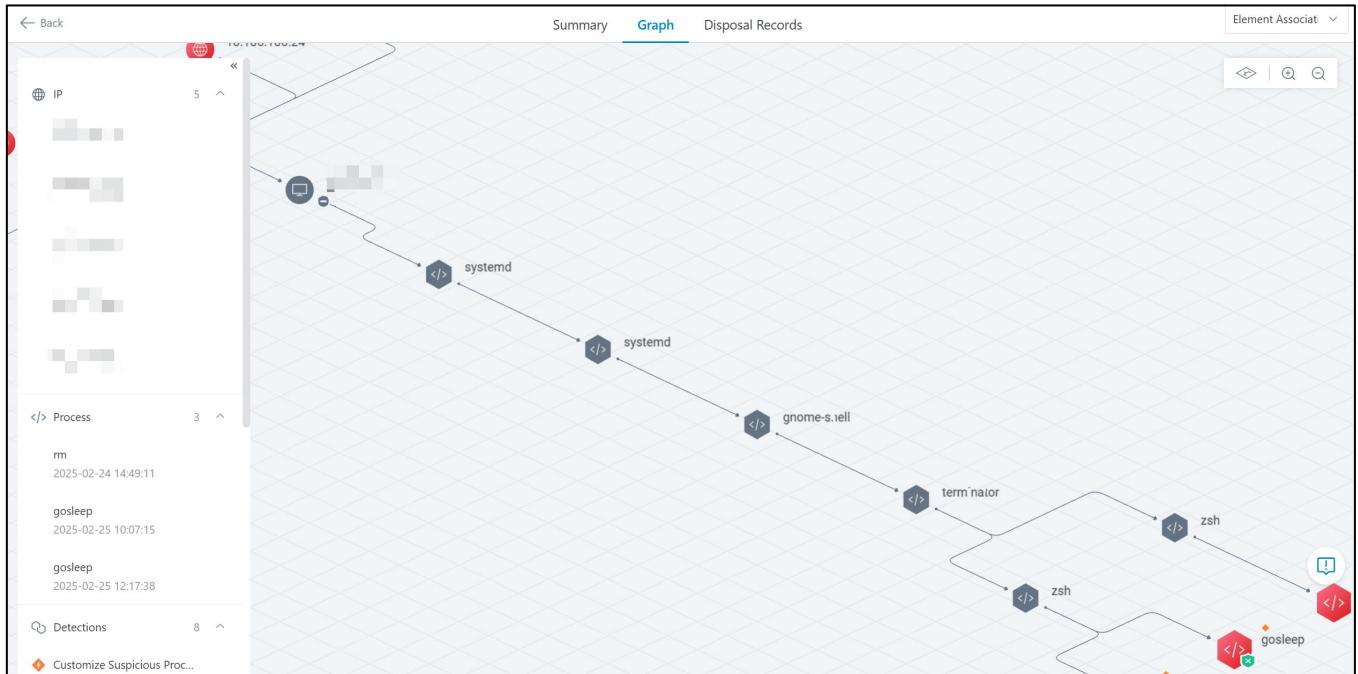
Click

▶ to expand the alert overview list included in the event. The list displays alerts associated with the event in reverse chronological order.

Click "Event Details" in the event list operation bar to enter the event details, mainly including event overview, analysis board, and handling records.

- Event Overview: Displays overall event information, such as event description, event score, tactics & techniques used in the event, affected hosts, alert timeline information, etc.

- **Analysis Board:** Graphically displays the entire intrusion process of the event at the granularity of processes, files, registries, etc.



- **Handling Records:** Records event response logs.

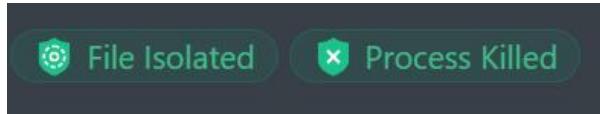
Disposal Records					
<input type="text" value="Please Enter Search Term"/> <input type="button" value="Q"/>					
Operation Time	Operation Type	Operation Content	Operating Account	Note	
2025-02-25 12:18:21	Alarm Status Modification	The status of alarm <input type="button" value="Customize Suspicious Processes"/> has been modified to Confirmed	admin	<input type="button" value=""/>	
2025-02-25 12:18:21	Element Response	The process <code>gosleep</code> is being killed	admin	<input type="button" value=""/>	
2025-02-25 10:29:36	Incident Status Modification	The event status has been modified to In Progress	admin	<input type="button" value=""/>	
2025-02-25 10:07:29	Alarm Status Modification	The status of alarm <input type="button" value="Customize Suspicious Processes"/> has been modified to Confirmed	admin	<input type="button" value=""/>	
2025-02-25 10:07:29	Element Response	The process <code>gosleep</code> is being killed	admin	<input type="button" value=""/>	
2025-02-24 14:48:53	Create Incident	Event <code>[REDACTED]</code> has been automatically created by the system	system	<input type="button" value=""/>	

4.1.4. Detection Response

The system not only informs users of intrusions in real-time but also provides various response methods based on different intrusion scenarios, including manual/automatic process termination, file isolation, network blocking, host isolation, etc., enabling users to fundamentally resolve intrusion

incidents with "high efficiency and diversity."

Responded alerts will have a response identifier, such as:



Note: Only responses to elements such as processes and files will have this identifier. Simply changing the alert handling status will not result in this identifier.

4.1.4.1. Automatic Response

Go to the "Security Response - Auto Response" page to create automatic response policies. Policies can be created based on host types, response elements, alert severity levels, application periods, etc.

Create Auto-Response Policy

Basic Information

Status:

* Policy Na... : Please enter the policy name

Policy Desc...: Please enter a policy description

* Host Type: Please select a host type

* Applicatio...: All Day Custom Time Range

Trigger Conditions

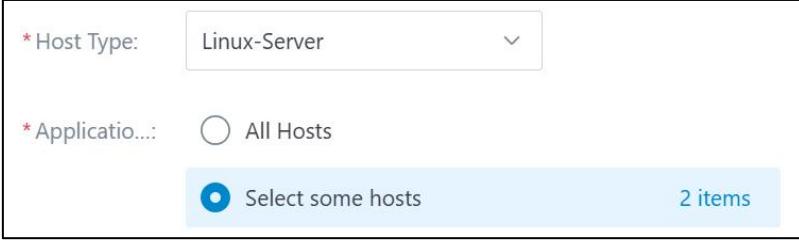
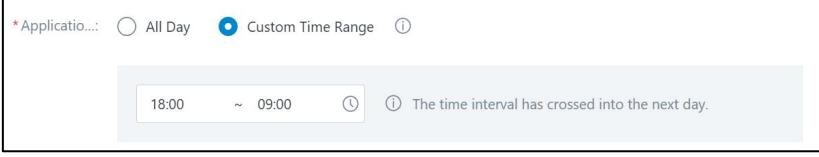
When the alarm meets the following conditions, the response will be automatically triggered.

* Response... : Please select a respo... Please select an alarm type

* Alarm Level: Please select the alert level

Alert frequ... : Single Alert
An alert triggers a response each time it is generated.
 Repeated Alert
If the same device triggers alerts repeatedly in a short period, it is considered to have a high credibility of being a real alert, and more forceful response measures can be taken.

Redeploy

Scenario	Instruction
Only set auto response for some hosts	<p>Set the host type and application scope.</p> <p>For example, in the following figure, only set auto response policy for 2 Linux Server hosts.</p> 
Only set auto response for some period	<p>Set application period, For example, in the following figure, only set auto response for off work hours(18:00 - 9:00)</p> 
Set auto response elements	<p>Auto response policy is setted at the element granularity, including processes, files, hosts, containers, etc.</p> <p>For example, when a threat alarm is detected in real-time and only the process needs to be terminated without isolating files or hosts, the response element can be selected as "process", and the alarm type drop-down box will only display the alarm types related to "process". Users can choose which alarm types to terminate the process according to their needs.</p> 
Set risk level	You can set automatically respond for detections with certain risk levels, such as the

following figure: only automatically respond to "critical risk" alarms.



Detection	If you want automatic response for each alarm, select 'Single Alarm';
Frequency	Set up auto response when "frequent alarms" occur to avoid false detection, because when the same device frequently experiences alarms, it is considered that the credibility of the real alarm is relatively high, and compared to "single alarm", it will reduce the probability of accidental killing.



Note:

- Auto response policies take effect after being enabled.
- When multiple conflicting policies are matched, the latest policy takes precedence.
- Auto response policies only apply to "post-event response," i.e., responses after the event occurs.

Pre-event response requires enabling the corresponding blocking switch in the "Detection Configuration" interface and enabling the driver. For example, if detecting malicious module loading by a process, to prevent the process from loading immediately, the corresponding blocking switch and the driver must be opened.

4.1.4.2. Manual Response

In Detection Detail page, you can respond to detection elements manually, like process, file, host and container. Elements varies from different alarm type.

Response Elements	Response Instruction
Process	<p>Terminate Process: Only terminates the process that exhibits malicious behavior in the alert.</p> <ul style="list-style-type: none">• Terminate merged processes associated with the current alert at the same time: If multiple processes are spawned from the same file, enabling this option will terminate all processes with the same command line.• Isolate the current process file at the same time: The executable file corresponding to the process will be isolated (the process will be terminated before isolation). This is generally applicable when the process in the alert is malicious. If the process in the alert is a system process (merely exploited by hackers to perform malicious actions), do not select file isolation. <p>Custom process termination: Use this feature to terminate other processes in the process chain. For example, if the process in the alert is malicious and its parent process is also malicious, both the parent process and the alert process can be terminated together.</p>

File	<p>Isolate File: Encrypts the alert file and moves it to the quarantine area (the process is terminated before isolation, and then the file is isolated). The file can be restored from the "Response - Response List."</p> <p>Delete File: Directly deletes the alert file, which cannot be recovered. Please use this option with caution.</p> <p>You can configure the quarantine area size and file retention period in the Response Center.</p> <ul style="list-style-type: none">• Quarantine Area Size: When the quarantine area exceeds the size limit, the system will automatically delete the earliest isolated files.• File Retention Period: The system periodically checks the files in the quarantine area and deletes expired data to ensure available space in the quarantine area.
Host	<p>Network Isolation: Supports isolating affected hosts from the network. You can set the isolation duration, and the system will automatically lift the isolation once the duration expires.</p> <ul style="list-style-type: none">• Bidirectional Isolation: Blocks both incoming and outgoing network traffic. The isolated host cannot initiate external access nor be accessed. Note: If you need to allow specific incoming traffic, configure open local ports, such as port 22 for remote login.• Unidirectional Isolation: Blocks outgoing network traffic. The host cannot initiate external access. <p>Currently, only the "Ransomware Attack" alert supports host isolation.</p> <p>For other scenarios, please go to the "Response - Response List" interface to manually create isolation rules for the devices you wish to isolate.</p>

	<div data-bbox="266 208 1065 1275"><p>Create New Isolation Configuration</p><p>Affected Devices</p><p>Please select a host ></p><p>Isolation Method</p><p> Isolate Host (Bi-directional) After selection, both network ingress and egress will be prohibited. Host isolation can be lifted in the 'Response List'. <input type="checkbox"/> Open local ports (optional)</p><p> Isolate Host (Uni-directional) After selection, network egress will be prohibited, and the host will be unable to initiate outbound connections. Host isolation can be lifted in the 'Response List'.</p><p>Isolation Duration</p><p><input checked="" type="radio"/> Forever <input type="radio"/> Custom</p><p>Response Reason</p><p>Please Enter Response Reason</p><p></p><p>Cancel OK</p></div>
Container	<p>Supports taking action on infected containers. Depending on the situation, you can choose to isolate, pause, or terminate the container.</p> <p>You can lift the isolation of a container or restart a paused container in the "Response - Response List."</p>
Network	<p>When suspicious network behavior alerts occur, you can use the Network Blocking response method. For example:</p> <ul style="list-style-type: none">Upon detecting a reverse shell, block its network access to prevent further external connections.

	<ul style="list-style-type: none">When an attacker connects to a honeypot port, block their access to prevent further interaction.
Account	<p>When a user's login source IP is not within the whitelist, the [Account Blocking] response method can be adopted to prohibit the account from logging in to all hosts within the effective scope.</p> <p>Unblocking can be performed in "Security Response - Response List".</p>

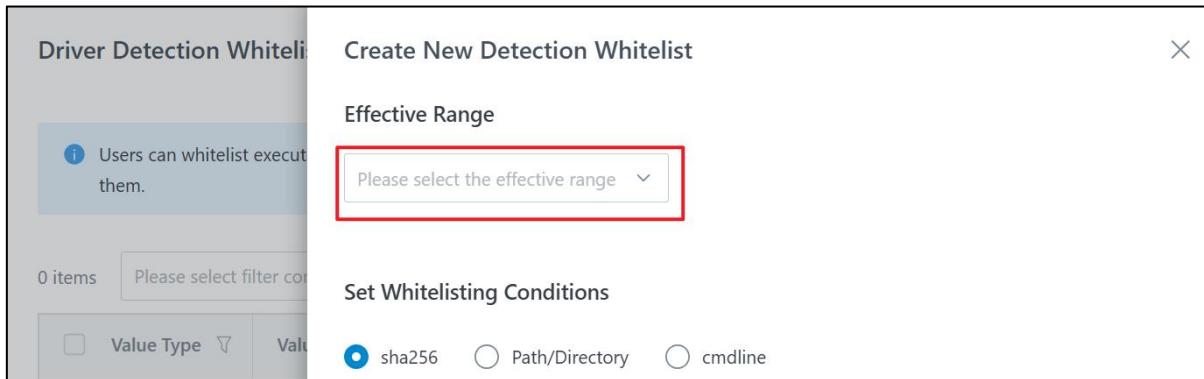
4.1.4.3. Response Logs

No matter it's automatic or manual response, each response will be logged. Click on "Response - Response List" to view the relevant response records

- Operation history: Record every response, whether successful or failed.
- Response List: Record the elements that have been successfully responded to, and restore some of the elements that have been partially responded to. For example, under the "Files" tab, you can view files that have been successfully isolated and lift the isolation.

The screenshot shows a user interface titled "Response List". At the top right, there is a red-bordered button labeled "Operation History". Below the title, there is a horizontal navigation bar with several tabs: "Process" (which is highlighted in blue), "File", "Container", "Host Isolate", "Net Blocking", "IP Blocking", "Domain Blocking", "Module Block", and "Driver Response". A tooltip below the "Process" tab explains: "The process response list is used to display processes that have been terminated and automatically blocked." At the bottom left, it says "16 items". There is also a search bar with the placeholder "Please Enter Search Term" and a magnifying glass icon.

4.1.4.4. Handle False Alarm



4.1.4.4.1. Add to Whitelist from Alerts

On the Alert Details interface, you can add an alert to the whitelist. Once whitelisted, the false positive alert will disappear from the alert list, and no further alerts of this type will be generated.

Alerts can be divided into two categories:

1. Alerts Not Blocked by the Driver
2. Alerts Blocked by the Driver

The handling methods for these two types differ.

Scenario	Instruction
Alerts Not Blocked by the Driver	<p>Click "Add to Whitelist" in the details page to avoid false alarm again.</p> <p>The process svchost.exe was found to start the process sc.exe through shellcode</p> <p>< Process Response Add to Whitelist Pending ↴</p>

The condition of adding varies from different alarm type.

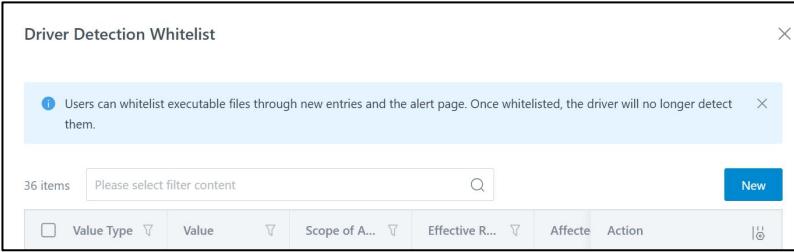
Alerts	Click "Add to Detection Whitelist" to avoid being blocked by driver again.
Blocked by the Driver	When detection is performed at the driver level, the supported whitelisting conditions are limited, typically including Process Hash and Process Path.

4.1.4.4.2. Add to Whitelist Manually

If you are aware of information that needs to be excluded in advance, you can add it to the whitelist before false positive alerts occur. Depending on the situation, you can decide whether to add it to the Alert Whitelist or the Driver Detection Whitelist.

Scenario	Instruction

Add to Whitelist	Click "New" in the "Monitoring Management - Whitelist" page, fill the table and save.
Add to Detection Whitelist	Click "New" in the "Monitoring Management - Whitelist - Driver Detection Whitelist" page, fill the table and save. The system will automatically synchronize the detection whitelist to the Agent side.



4.1.4.5. Change Alarm Status

The alarm list or alarm details interface allows you to view the current status of the alarm and make modifications to the alarm status.

Status	Instruction
Pending	Default status.
Processing	<p>During the process of handling alerts, you can mark the alert status as "Progressing" to indicate that the alert is being addressed.</p> <p>If the alert analysis is completed quickly, you may skip marking it as "Progressing" and directly update it to the final status after analysis.</p>
Ignored	For alerts that do not require action, you can mark them as "Ignored", such as alerts generated during internal testing by staff.

Confirmed	For genuine alerts, you can mark them as "Confirmed". When a manual or automatic response is applied to the alert, its status will automatically be updated to "Confirmed".
Whitelisted	For false positive alerts, after adding them to the whitelist, the alert status will automatically change to "Whitelisted" and the alert will disappear from the alert list. You can view the false positive alerts in the "Affected Records" in Whitelist or "Affected Records" in Driver Detection Whitelist sections.

Whitelist

The creation, modification, and deletion of whitelist rules are all asynchronous operations. It may take a long time for large data volumes. Please manually refresh the page after a while to get the latest data.

#	Whitelist Condition	Application Scope	Affected Re...	Note	Update Time	Operation
1	Alert Type Equals Process Hijacking Attack	Process Name In Xmind.exe File Path Match	All Hosts	(9)	2025-02-24 16:17:46	Edit Delete

Driver Detection Whitelist

Users can whitelist executable files through new entries and the alert page. Once whitelisted, the driver will no longer detect them.

#	Value Type	Value	Scope of A...	Effective R...	Affected	Action
1	Path/Directory	C:\Windows\SoftwareDistribution\Download	10.102.108.86	Suspicious process behavior	(1)	Edit Delete

4.2. Memory Backdoor

Memory Backdoor defends against an advanced fileless attack technique. Traditional antivirus software scans files saved to disk to determine if they are malicious. However, fileless attack techniques do not leave executable files on the target system's disk. Instead, they reside entirely in memory, leveraging built-in system tools or scripts to execute malicious code or webshell files,

thereby bypassing traditional security measures. Due to their effectiveness and difficulty in detection, fileless attacks are more likely to result in widespread exploitation.

Memory webshells exploit vulnerabilities to make web processes execute malicious code, downloading webshells into the memory space of the web process or loading malicious classes into the process. This allows backdoors to be implanted without writing to disk, and the webshell in memory can still be accessed via normal URLs to receive responses. Memory malicious code, on the other hand, injects malicious code instructions sent remotely into running processes on the host through vulnerabilities or hacker toolkits, enabling attacks.

The Memory Backdoor feature detects fileless attacks by monitoring the core technical process–process memory. It accurately captures malicious files injected into process memory, matches the characteristics of files running in process memory, and promptly detects and reports malicious code and webshell files in memory, effectively identifying fileless attacks and safeguarding user host security.

Memory Backdoor aims to address the following issues:

1. Helps users detect malicious code running in process memory and promptly sends alerts.
2. Provides feature analysis and explanations of malicious file content to help users understand alerts and make informed decisions for further action.
3. Uses precise detection capabilities to help users verify the results of memory backdoor repairs, enabling lifecycle management of incidents.

Feature Advantages:

1. Multi-type Memory Trojan Detection: Supports detecting memory webshells, process memory injections, malicious code files, and other common memory trojans, covering typical memory trojan attacks.

2. Integration with In-house Engine: Detected memory webshells are analyzed by Qingteng's in-house engine, ensuring accurate detection.
3. Flexible Configuration: Users can configure whether to enable detection capabilities on hosts based on business needs, minimizing unnecessary resource consumption and ensuring stable business operations.
4. One-click Verification: Supports one-click verification of handled memory trojans, allowing users to immediately determine if the remediation was effective and if the memory trojan still poses a threat.
5. Automatic Response: Users can configure rules to automatically handle reported memory backdoors, isolating memory files to mitigate intrusion risks promptly.

4.2.1. Feature Authorization

Only Agents with the "Host Security Extension Pack" product purchased and authorized will have the Memory Backdoor detection feature.

To add container memory backdoor functionality, assign the Container Security Extension Pack authorization to the Agent.

Method 1: Authorize During Agent Installation

Assign authorization during Agent installation. Navigate to the "Probes - Installation - Agent" interface, select the corresponding operating system and authorization features. For host memory backdoor:

Agent

Here you can view the objects that the probe can protect, the supported systems, and the dependent environments. You can also follow the installation steps to try deploying and ins

Linux

Windows

Kubernetes

Openshift

Install on Linux

Recommended Host Docker

Basic Configuration

Default Aut... : Server Version PC Version

To ensure the normal operation of the system when enabling container security authorization, please make sure that the CPU limit threshold and memory limit threshold of the Agent are not less than 1C and 1000M respectively.

Server Security [Select All](#)

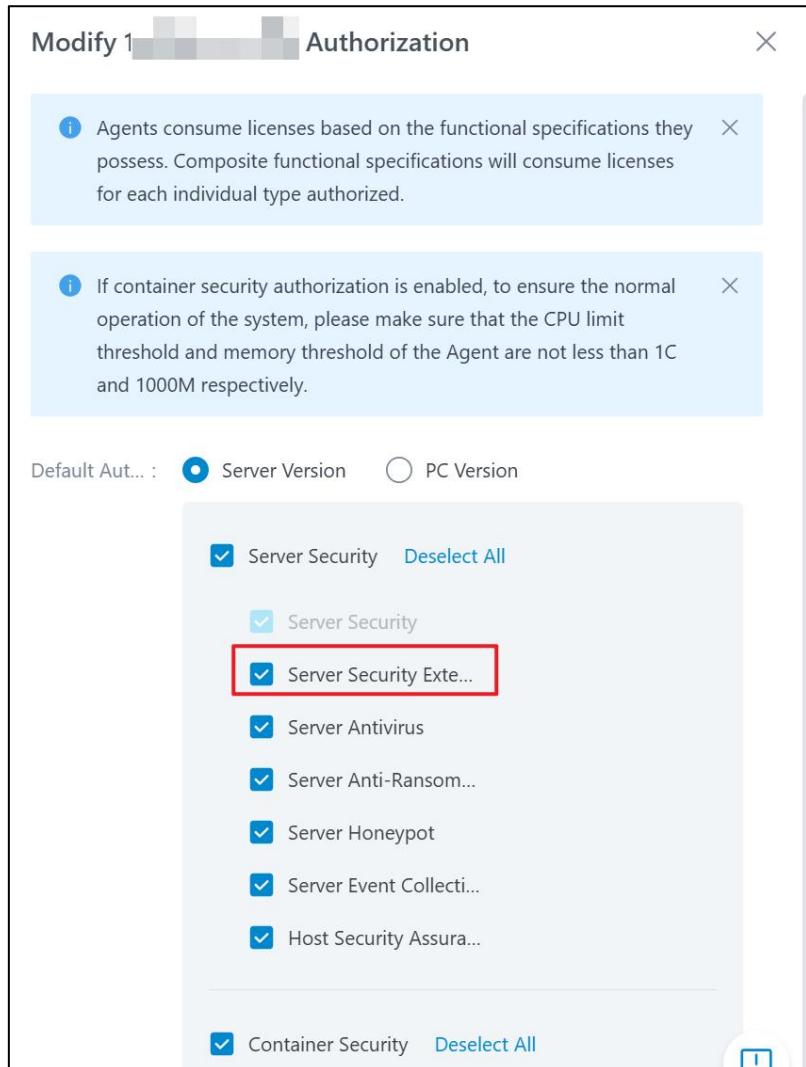
Server Security Server Security Ext... Server Antivirus

Server Anti-Ransom... Server Honeypot Server Event Collecti...

Host Security Assura... Container Security

Method 2: Modify Agent Authorization

After Agent installation, you can modify the authorization information and assign the "Server Security Extension" authorization. Navigate to the "Probes - Probe Management - License" interface, click "Configuration Authorization", and modify the authorization as shown below:



4.2.2. Detection Configuration

By combining real-time monitoring with behavior-triggered scanning, the system detects whether backdoors have been injected into the process memory of each host, effectively identifying fileless attack incidents, including common memory code injections, memory webshells, and remotely loaded dynamic link libraries.

- **Memory Malicious Code:** Detects process memory to monitor whether malicious dynamic link libraries are loaded or malicious code is injected and executed. Supports detection on Linux-PC, Linux-Server, Windows-PC, and Windows-Server systems.
- **Memory Webshell:** Uses multiple engines and detection methods to detect whether webshells

have been injected into web process memory and restores the injected content. Supports injection and detection only on Linux-Server and Windows-Server web processes.

4.2.2.1. Real-time Monitoring

By default, real-time monitoring for memory backdoors is disabled. To enable real-time memory backdoor protection, first turn on this feature in the detection configuration.

- **Enable Memory Protection for Newly Installed Agents:** Navigate to the "Detection Configuration" page, select the corresponding platform type, enter the default configuration details, find the "Memory Backdoor Detection" section, and toggle the switch to enable it.
- **Enable for Specific Hosts:** If not enabling memory protection for all newly installed hosts, keep the memory backdoor switch off in the default configuration. Click "New Configuration" to create a custom detection configuration and enable the memory backdoor detection switch.

The screenshot shows the "Detection Configuration" page with the following interface elements:

- Header: "Detection Configuration". Below it, a note: "To ensure proper functionality, please configure the following:"
- Top navigation bar with four items: "Install Plugins", "Enable Driver", "Enable Event Source", and "Install Local Antivirus Engine".
- Platform selection tabs: "Linux-Server" (selected), "Windows-Server", "Linux-PC", "Windows-PC", and "Cluster".
- Section titled "System Default Configuration" with the following details:
 - Icon: A gear icon with a plus sign.
 - Label: "Include" followed by "18 Item Configuration".
 - Label: "Application Scope" with a progress bar showing "Total 9 devices".
 - Label: "Detection Sensitivity" set to "Broad".
 - Label: "Update Time" showing "2025-02-07 14:25:27".
 - A small edit icon at the end of the row.

Last Scan Time: 2024-12-05 09:16:00 , if you need to scan immediately, please click [Scan Now](#)

Memory Malicious Code Detection

Detect the process memory. If it is found that the process has loaded malicious dynamic link libraries or has been injected with malicious code, an alert will be generated. Enabling this feature will consume some performance, please enable it with caution.

[View Scanned Records](#)

Memory Webshell Detection

Use multiple engines and detection methods to detect whether the Web process memory has been injected with Webshell, and restore the injected content. This feature will inject running java class processes. It is recommended to enable this feature only on hosts running java-related services. Once disabled, the system will automatically clear the injected content.

[View detection status](#) [View Scanned Records](#)

4.2.2.2. Manual Scanning

Real-time monitoring only detects process files running in memory after the feature is enabled. For existing process files, users can use manual scanning to supplement detection.

- Method 1: Create a Scan Task from the Alert List Interface

- In the "Intrusion Detection - Alert List" interface, click "Manual Scan" in the upper right corner and select "Memory Backdoor Detection."

Risk Level	Alarm Type	Affected Device Type	Status	Time Range
Critical Risk	Suspicious Process Parameters	Host	Pending	Last 1 Hour
High Risk	Customize Suspicious Processes	Container	Processing	Last 1 Day
Medium Risk	Web Backdoor	Cluster	Confirmed	Last 7 Days
Low Risk	Malicious Process Initiation		Ignored	Last 30 Days
	Reverse Shell			Custom...
	Malicious file writing to disk			

Group by: All Host Container Cluster Total 2002 alarms Select All Last active Descending Mark All Manual Scan Export all

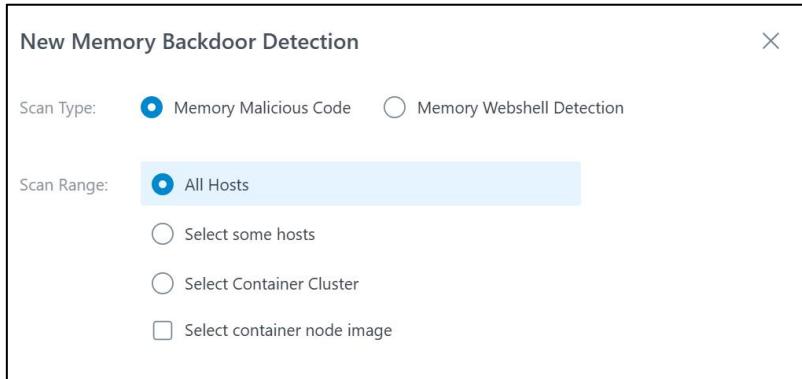
Risk Level Detection Time Alarm Type Description Affected Devices

High Risk 2025-02-26 08:14:01 Customize Suspi... Memory Backdoor Detection

2025-02-26 09:30:01

Risk Level Detection Time Alarm Type Description Affected Devices WMI Scan

- Select the appropriate scan type, fill in the parameters, and click "Save" to start the scan.



- Method 2: Create a Scan Task from the Detection Configuration Interface

- Navigate to the "Intrusion Detection - Monitoring Configuration - Detection Configuration" interface, find the "Memory Backdoor Detection" section under the corresponding platform type, click "Scan Now," select the scan type, fill in the parameters, and click "Run."

	Opened	Not Enabled
Memory Backdoor Detection	2	0

Last Scan Time: 2024-12-05 09:16:00 , if you need to scan immediately, please click **Scan Now**

Memory Malicious Code Detection

Detect the process memory. If it is found that the process has loaded malicious dynamic link libraries or has been injected with malicious code, an alert will be generated. Enabling this feature will consume some performance, please enable it with caution.

[View Scanned Records](#)

Memory Webshell Detection

Use multiple engines and detection methods to detect whether the Web process memory has been injected with Webshell, and restore the injected content. This feature will inject running java class processes. It is recommended to enable this feature only on hosts running java-related services. Once disabled, the system will automatically clear the injected content.

[View detection status](#) [View Scanned Records](#)

Note:

- Click "View Scanned Records" to check if the task was executed successfully.
- After enabling memory webshell detection, click "View Detection Status" under the feature configuration to understand the injection status. Devices and processes that fail to inject will be recorded in the injection failure list. Disabling memory webshell detection will automatically clear the injected content.

Scan Records							
Scan Start Time		Detection ...	Scan Type	Scan Range	Scan St...	Num#	Operation
2025-01-13 14:47:05	Memory Back...	Memory Webshell D...	[REDACTED]	Failed	1	Details	
2024-12-05 09:16:00	Memory Back...	Memory Webshell D...	[REDACTED]	Comp...	0	Details	

4.2.3. Alarm Viewing

When the system detects memory malicious code or memory webshells through real-time monitoring or scanning, it will promptly report alerts. Users can view alert information in the "Detection List" interface.

In the "Intrusion Detection - Detection List," filter alerts by type (In-memory webshell or Memory Malicious Code) and click to view alert details.

Detection List							
Time Range: Last 7 Days		Risk Level: Critical Risk, High Risk, Medium Risk	Affected Device Type				
Time Range: Last 7 Days	Risk Level: Critical Risk, High Risk, Medium Risk	Alarm Type: Memory-Resident Malware, In-memory Webshell Please manually enter the content you want to inquire after the colon and press Enter to finish.					
Risk Level	Memory	Alarm Type	Affected Device Type	Status	Time Range		
<input checked="" type="checkbox"/> Critical Risk	<input checked="" type="checkbox"/> Memory-Resident Malware	Suspicious Process Parameters	Host	2015	Pending	2002	Last 1 Hour
<input checked="" type="checkbox"/> High Risk	<input checked="" type="checkbox"/> In-memory Webshell	Customize Suspicious Processes	Container	101	Processing	0	Last 1 Day
<input checked="" type="checkbox"/> Medium		Web Backdoor	Cluster	0	Confirmed	13	Last 7 Days
<input checked="" type="checkbox"/> Low Risk		Malicious Process Initiation		0	Ignored	0	Last 30 Days
		Reverse Shell					Custom...
		Malicious file writing to disk					

4.2.3.1. Memory Malicious Code Alert

The memory malicious code alert details display the process and process chain information containing malicious code in memory, as well as the memory segment information where the malicious code was detected.

- **Detection Information:**

- **Hit Process:** The process detected by the system that contains malicious code.
- **Hit Memory Segment Information:**

- **Start Address:** The location of the code segment in memory.
 - **Permissions:** The current permissions for memory operations on this segment.
 - **Corresponding File Path:** The local file path corresponding to this code segment on the host. Since memory backdoors are fileless attacks, there is usually no corresponding file on disk.
 - **Hit Rule:** The rule library that the system matched to identify the memory malicious code.
- **Process Chain Information:** Includes the process with malicious code and its child processes.
 - **Handling Suggestions:** Investigate the alert process to confirm if it is a legitimate process or a common antivirus process. Antivirus software's built-in virus rule libraries may also trigger alerts. If confirmed as malicious, terminate the process.

The screenshot shows a Sentry CWPP alert window for a 'Memory-Resident Malware' detection. The alert title is 'Malicious code has been detected in the memory of the process YDUtils, suspected to be Proxy Penetration Tool,Crypto Mining Trojan.' The alert is categorized as 'Critical Risk'. The main panel displays 'Detection Information' including the detection time (2025-02-21 05:43:58), ID (redacted), response result (-), affected devices (redacted), tactic & technique (Process Injection (T1055) and Evasion Defense), and detection method (Memory Engine). The detection explanation states: 'There are malicious code segments in the process memory, indicating that the process itself is malicious or that a normal process has been injected with malicious code.' Below this, rule ID, hit process (YDUtils(25582)), command line (/usr/local/qcloud/YunJing/YDUtil/YDUtils scan_memshell), and hit memory segment information are listed. The memory segment table shows two entries: one from 0xc000000000 to 0xc004000000 with permission Read, Write, Private and status 'No Corresponding Landed File'; and another from 0x7f2ada909000 to 0x7f2ada9f0000 with the same permissions and status. A 'Process Chain Information' section is also present at the bottom.

Start Address	End Address	Permission	Corresponding ...	Rule ID
0xc000000000	0xc004000000	Read, Write, Private	No Corresponding Landed File	
0x7f2ada909000	0x7f2ada9f0000	Read, Write, Private	No Corresponding Landed File	

4.2.3.2. Memory Webshell Alert

The memory webshell alert details display the injected application and site information, the injected process and process chain information, the malicious class name, and support downloading the original class file for decompilation.

- **Detection Information:**
 - **Injected Process:** The system needs to inject into Java class processes before detecting memory webshells.
 - **Injected Application:** The application to which the injected process belongs.
 - **Malicious Class Name:** The malicious class to which the memory webshell file belongs.
 - **Engine Detection Result:** The rule library that the system matched to identify the

memory webshell alert.

- **Class File Information:**

- Malicious class files are usually placed in a project directory and loaded into memory by Java class loaders to perform dangerous operations, such as stealing user information or tampering with data.
- After finding the memory webshell, the system can further identify the malicious class file by checking which project started the process containing the memory webshell. Users can view the class name, class loader, and other information.
- The system will decompile the malicious class file. If further analysis is needed, users can download the decompiled Java file or the original class file.

- **Process Chain Information:** Includes the process with malicious code and its parent process.
- **Site Information:** The web service used by the injected process. Different Java processes may be started by different application services.
- **Handling Suggestions:** Memory backdoors are fileless attacks, meaning they only run when loaded into memory. Therefore, users can delete the root class file and restart the service after confirming that the file is a malicious webshell and the class file is local. If the class file is not local, simply restart the service.

The screenshot shows a detection alert for a malicious class in a Java process. The alert details are as follows:

- High Risk** In-memory Webshell
- The Thunderfire Engine has detected a malicious class:** org.sparkproject.jetty.server.handler.ContextHandler\$StaticContext in the process java
- Detection Information:**
 - Detection Time: 2025-02-28 19:25:47 - 0 times - 2025-02-28 19:25:47
 - ID: [REDACTED]
 - Response Result: -
 - Affected Devices: 1 device (kylin)
 - Impact on Container: kylin
 - Image Name: rec [REDACTED]
 - Tactic & Technique: Web Shell ([REDACTED]) Privilege Persistence All (2)
 - Detection Method: Memory Engine
 - Detection Explanation: A class containing malicious code was discovered in the memory of a Java process, suspected to have been maliciously injected by an attacker.
 - Rule ID: [REDACTED]
 - Injected Process: [REDACTED]
 - Injected Application: -
 - Malicious Class: org.sparkproject.jetty.server.handler.ContextHandler\$StaticContext
 - FireEye Engine Details:

Malicious Function Name	Malicious Parameters
getClassLoader	[getRequest]

4.2.4. Alarm Response

The system supports both automatic and manual responses to memory backdoor alerts. To enable automatic responses upon alert detection, configure the automatic response strategy in advance.

4.2.4.1. Auto Response

Navigate to the "Security Response - Automatic Response" page and create an automatic response strategy. When specified types of alerts (e.g., memory malicious code or memory webshell) are detected, the system will automatically handle them without requiring manual intervention.

Users must first select the host type before setting trigger conditions.

- **For Memory Malicious Code:**

- Supported Device Types: Linux-Server, Linux-PC, Windows-Server, Windows-PC,

Containers.

- Supported Automatic Response Elements: Process.
- Supported Automatic Response Methods: Terminate Process.

- **For Memory Webshell:**

- Supported Device Types: Linux-Server, Windows-Server, Containers.
- Supported Automatic Response Elements: Process.
- Supported Automatic Response Methods: Terminate Process.

Create Auto-Response Policy

Basic Information

Status:

* Policy Na... :

Policy Desc...:

* Host Type:

* Applicatio...: All Day Custom Time Range

Trigger Conditions

When the alarm meets the following conditions, the response will be automatically triggered.

* Response... :

* Alarm Level:

Alert frequ... : Single Alert
An alert triggers a response each time it is generated.
 Repeated Alert
If the same device triggers alerts repeatedly in a short period, it is considered to have a high credibility of being a re

4.2.4.2. Manual Response

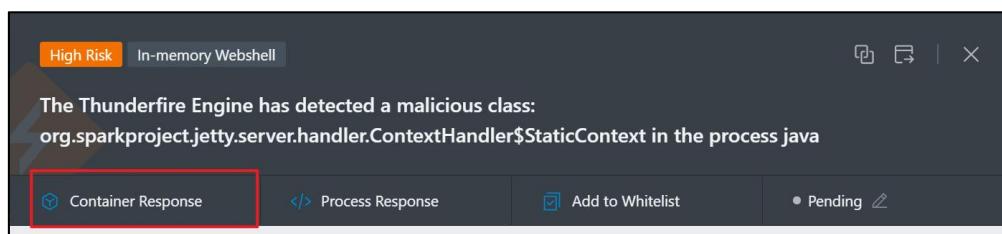
In the alert details, users can manually handle alert information. For malicious files detected by the memory backdoor feature, users can follow the system's handling suggestions.

- **For Memory Malicious Code:** Supported actions include process response, adding to whitelist, and changing the handling status.
- **For Memory Webshell:** Supported actions include container response, process response, adding to whitelist, and changing the handling status.

4.2.4.2.1. Container Response

For container processes with memory backdoors, users can choose to isolate, pause, or terminate the container.

- Isolate Container: Isolates the container's network environment, preventing it from requesting or sending network resources.
- Pause Container: Pauses the container, putting it into a "pause" state.
- Terminate Container: Stops the container's operation. The container will be destroyed and cannot be recovered. Use with caution.



Processing Containers

Please select the handling method for container kylin:

 **Isolate Container**
Isolate the container network environment, prohibit network traffic in and out, and communication with the outside. The container can be unisolated in 'Response Records'.

 **Pause Container**
Choosing to pause the container will suspend its execution, and the container will enter a 'pause' state. It can be restarted in 'Response Records'.

 **Terminate Container**
Choosing to kill the container will stop its execution, and the container will be terminated and cannot be recovered. Please proceed with caution.

Response Reason

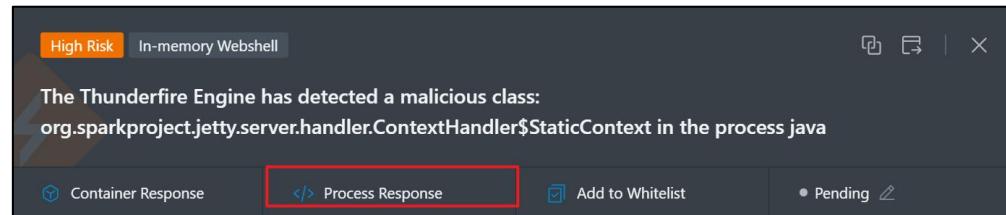
Please Enter Response Reason

4.2.4.2.2. Process Response

For dangerous process files, users can choose to terminate the process first.

- **Terminate Process:** Only terminates the process exhibiting malicious behavior in the alert.
- **Custom Terminate Process:** Use this feature to terminate other processes in the process chain.

For example, if the alert process is malicious and its parent process is also malicious, both can be terminated together.



Process Handling

Please select the handling method for process java(788536):

Terminate Process

Terminate the current process java(788536).

Terminate all processes merged with the current alert.

Also isolate the current process file; please choose carefully.

Custom Terminate Process

Select the process you want to terminate in the process chain of the detection. Once the process is terminated, it cannot be recovered. Please proceed with caution.

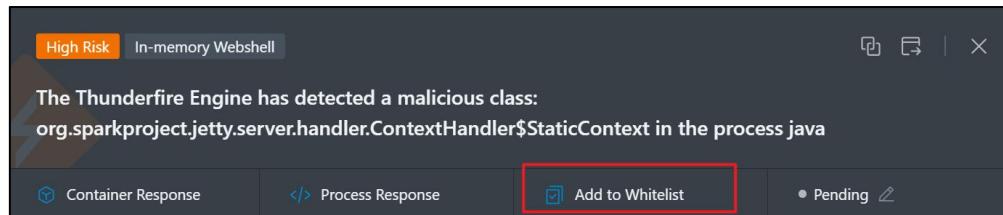
Response Reason

Please Enter Response Reason

Cancel Ok

4.2.4.2.3. Add to Whitelist

In case of false positives, users can add the process to the whitelist, and no further alerts will be generated for this process.



New Whitelist

Set Whitelist Conditions
Please set the whitelist conditions. The conditions are connected with 'AND,' which means that detection information can only apply the whitelist when it completely meets all the set whitelist conditions.

Condition	Matching Method	Value	Reset
Alert Type	Equals	In-memory Webshell	
Class Name	Equals	[REDACTED] ContextHandler\$Sta	
Process File Path	Equals	[REDACTED] /bin/java	
Process File SHA256	Equals	[REDACTED] 2f3ae5bc63da87	

+ Add Condition

Application Scope
Please select the range of hosts to which the whitelist applies. Only containers within the range can apply the whitelist.

All Hosts
 Select some hosts
 Current Host

All Clusters
 Select Container Cluster

Cancel **Save**

- **Set Whitelist Conditions:**

- Conditions are combined with an "AND" relationship, meaning only alerts that meet all conditions will be whitelisted.
- The system automatically fills in the process-related information for the alert. Users can reset, add, or delete conditions as needed. Resetting will revert the conditions to the last saved state.

- **Affected Alert Range:**

- If "Affect Alerts from the Past 30 Days" is selected, past alerts will be marked as whitelisted and removed from the alert list. They can only be viewed in the whitelist, and future alerts will also be whitelisted.
- If "Only Affect Current and Future Alerts" is selected, the whitelist will only apply to the current alert and future alerts, leaving historical alerts unaffected.

4.2.5. Repair Verification

The system supports repair verification for unhandled memory webshell and memory malicious code alerts. If the issue is found to be resolved, the system will automatically mark the alert as a genuine alert.

In the alert list, click "Manual Scan" to create a "Repair Verification" task.

The screenshot shows the Sentry CWPP Detection List interface. At the top, there is a search bar with 'Time Range: Last 7 Days' and 'Risk Level: Critical Risk, High Risk, Medium Risk'. Below the search bar is a table with columns: Risk Level, Alarm Type, Affected Device Type, Status, and Time Range. The table data includes:

Risk Level	Alarm Type	Affected Device Type	Status	Time Range
Critical Risk	Local Privilege Escalation	Host	Pending	Today
High Risk	Bypass User Account Control	Container	Processing	Last 1 Hour
Medium Risk	Reverse Shell	Cluster	Confirmed	Last 1 Day
Low Risk	Suspicious network scan		Ignored	Last 7 Days
	Accessing Malicious IP Address			236
	Web Backdoor			236

Below the table, there is a group by dropdown set to 'All', a total count of 236 alarms, and a 'Select All' button. To the right of the table is a 'Mark All' button and a 'Manual Scan' button, which is highlighted with a red box. A context menu is open over the second row (High Risk, Bypass User Account Control), showing options like 'Program Hijack', 'Phishing Detect...', 'Internal Tunnel', 'Configuration ...', 'Dynamic Link ...', 'Repair Verification' (which is also highlighted with a red box), and 'Repair Verificat...'. At the bottom right of the interface, there are buttons for 'Scan Records' and 'Export all'.

4.3. Network Monitoring

When the host performs routine operations, it often needs to access different **IP addresses or domain**

names. However, some IP addresses and domain names are exploited or manipulated by malicious programs such as viruses, trojans, and network zombies. These are referred to as malicious IP addresses and malicious domain names. Once a malicious IP address or domain name is accessed by the host, it can conduct network connection-related activities to detect sensitive information on the host or even initiate direct attacks. For example, a malicious IP address might frequently perform network scans to identify open ports on the host's network, detect system vulnerabilities for subsequent attacks, or send a large number of malicious requests to exhaust or crash the target host's resources. Additionally, when network services are disrupted or interfered with by malicious IP addresses or domain names, normal business operations are often unable to proceed, leading to losses for the user's business.

Network Monitoring real-time monitors network connection behaviors within processes. If it detects that the host has connected to a malicious IP address or domain name, it will promptly alert and support blocking.

4.3.1. Functional Authorization

Only if the "Host Security Extended Package" product has been purchased and the Agent has been assigned the "Host Security Extended Package" authorization can the Agent monitor whether the host's process has accessed malicious IP addresses or malicious domain names.

Monitoring of container processes accessing malicious IP addresses or malicious domain names requires purchasing and assigning the "Container Security Standard Edition" authorization.

Method 1: Authorization during Agent Installation

During Agent installation, assign the authorization. Enter the "Probe Management - Agent Installation Guide" interface, select the corresponding operating system and authorization function.

Network monitoring requires the Host Security Extension.

Agent

Here you can view the objects that the probe can protect, the supported systems, and the dependent environments. You can also follow the installation steps to try deploying and ins

Linux

Windows

Kubernetes

Openshift

Install on Linux

Recommended Host Docker

Basic Configuration

Default Aut... : Server Version PC Version

To ensure the normal operation of the system when enabling container security authorization, please make sure
① that the CPU limit threshold and memory limit threshold of the Agent are not less than 1C and 1000M respectively.

Server Security Select All

Server Security Server Security Ext... Server Antivirus

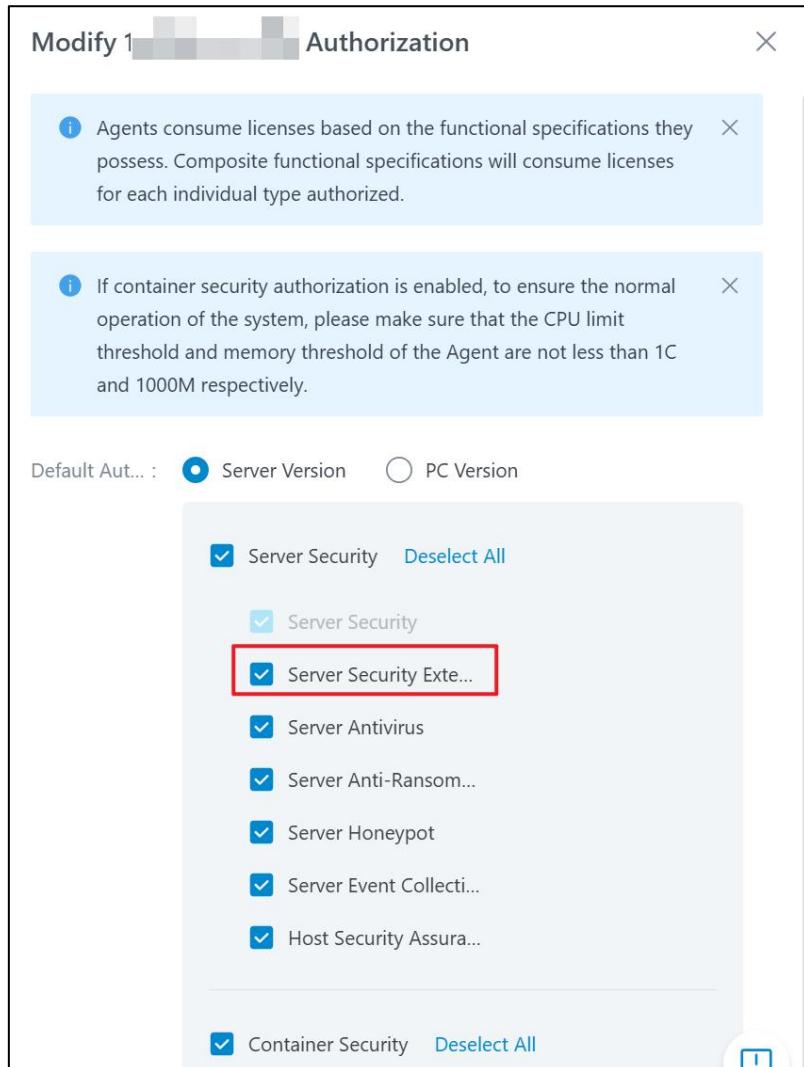
Server Anti-Ransom... Server Honeypot Server Event Collecti...

Host Security Assura...

Container Security

Method 2: Modify Agent Authorization

After Agent installation, you can modify the authorization information and assign the "Host Security Extension Pack" authorization. Navigate to the "Probe Management - Operation Management - Authorization Configuration" interface, click [Authorization Configuration], and modify the authorization as shown below:



4.3.2. Preconditions

In a Linux system, monitoring malicious domain name access depends on DNS plugins, ebpf, or driver event sources. Before enabling malicious domain name monitoring, you need to install a DNS plugin (container process malicious domain name monitoring does not support DNS plugins) or enable the relevant event sources to perform Linux malicious domain name access monitoring.

Malicious domain name access monitoring for Windows does not depend on plugins or additional event sources.

Method 1: Enable Event Sources

Enter the "Probes - Probes Management - Agent - Event Source Configuration" interface, or click

"Linux-Server Detection Configuration - Malicious Domain Name Monitoring" and then click "Event Source Configuration." This will directly take you to the event source configuration interface.

Monitoring process access to malicious domains 

Perform DNS domain name resolution. When accessing a malicious domain, an alert will be reported. This feature depends on the DNS plugin (not supported in container environments), eBPF, or driver event source. Please install the DNS plugin or enable the corresponding event source before using.

[Install DNS Plugin](#)  [Event Source Configuration](#) 

Find the Linux host you need to enable event sources for, click "Config," and enable eBPF or driver event sources.

Note:

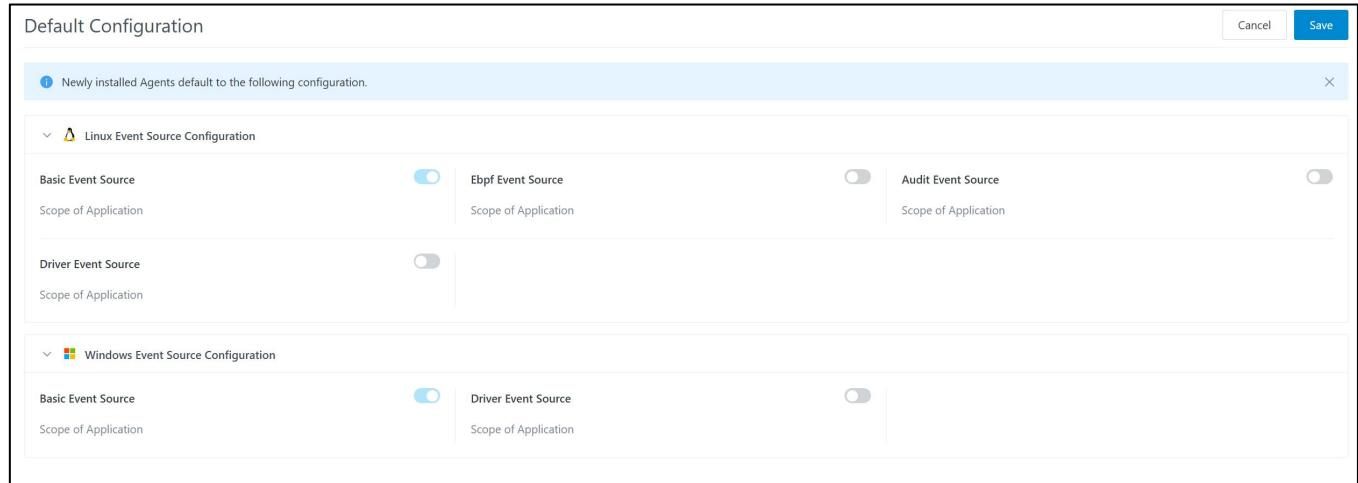
Driver event sources depend on drivers. To enable driver event sources, go to the "Agent - Event Source Configuration" interface, find the corresponding Agent, and enable the driver.

Event Source Configuration 

Linux operating system environment supports four types of event sources: basic event source, eBPF event source, audit event source, and driver event source. Windows operating system environment supports two types of event sources: basic event source and driver event source; multiple event sources can be enabled simultaneously, and after enabling multiple event sources, the Agent will automatically select the appropriate event source based on the actual environment. [View more details](#)

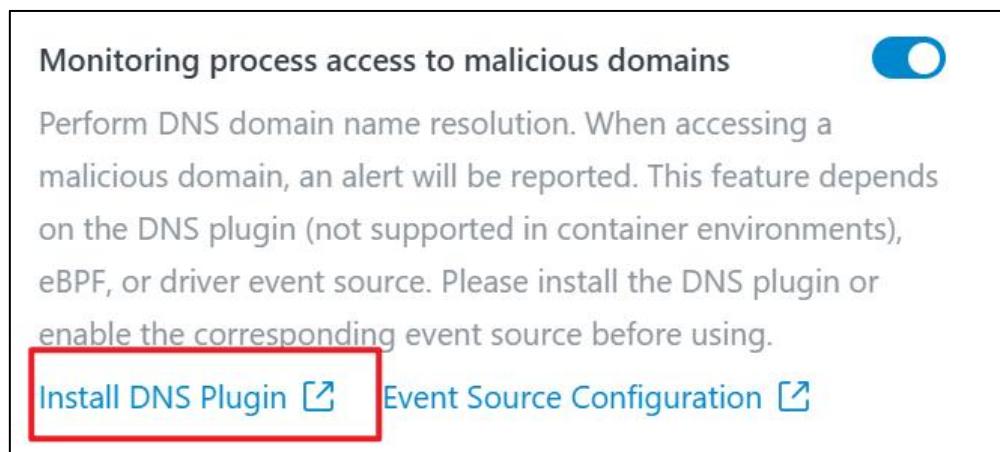
Agent ID	Host	Enable Event Source	Audit Subscription ...	Driver Status	eBPF status	Operation
 7	 LAPTOP-S3CQHBNR	Basic Event Source	Total 2 items	Unsupported	Enabled	Not Supported
 4	 LAPTOP-B5HF0H...	Basic Event Source	Total 2 items	Unsupported	Enabled	Not Supported

If you need to enable the corresponding event source for a newly installed host, click the "Default Configuration" button in the upper right corner to enable the malicious domain name access switch.



Method 2: Install DNS Plugin

In the "Probes - Components - Plugins" interface, click "DNS Plugin" to enter the DNS plugin installation interface, or click "Linux-Server Detection Configuration - Malicious Domain Name Monitoring" and then click "Install DNS Plugin" to directly jump to the DNS plugin installation interface.



Use the search box to search for the host you need to install, then click the "Install" action under the "Actions" column.

Agent ID: ccfe3ff810ac686c		Uninstall	Upgrade	Install		
1 items	Host	Plugin Status	Last Exec...	Last Execution Time	Installation Time	Operation
<input type="checkbox"/> ccfe3ff810ac686c	10.42.2.0 shuqin	未安装	-	-	-	<input type="button" value="Install"/>
1 items						

4.3.3. Detection Configuration

The default detection configuration has malicious IP and malicious domain name access monitoring enabled.

- For newly installed Windows hosts: They automatically possess malicious IP and malicious domain name access detection capabilities.
- For newly installed Linux hosts: If default ebpf or driver event sources are enabled, the Linux newly installed host also has these two detection capabilities.

If you do not want the default malicious IP and malicious domain name access monitoring capability enabled, go to the detection configuration interface, find the corresponding platform type, and change the default configuration to disable the malicious IP and malicious domain name access monitoring switch.

If you want to enable malicious IP and malicious domain name access monitoring for specific hosts,

go to the detection configuration page, click **Create Configuration** to customize, and enable the two monitoring switches.

The screenshot shows the 'Linux-Server System Default Configuration' page with the following details:

- Configuration Details:** Malicious Process Protection (Opened: 6, Not Enabled: 0).
- Process Injection Detection:** Enabled (switch is blue).
- Malicious Module Loading Detection:** Enabled (switch is blue).
- Binary Padding Detection:** Enabled (switch is blue).
- Process Access to Malicious IP Monitoring:** Enabled (switch is blue). This section is highlighted with a red border. Description: Real-time monitoring of the network connection behavior of processes in the system. If process injection behavior is detected, alarms will be reported in real-time.
- Hidden Process Scan:** Scans for potentially hidden processes in the system. Users can customize the specified scanning period, and the system will execute scans according to the set schedule.
- Malicious File Self-Deletion Detection:** Enabled (switch is blue). Description: Real-time monitoring of file deletion behavior; an alert will be reported if a process is detected deleting its own files or its parent process files.
- Custom Process Behavior Rules:** You can view the current host protection status and determine whether to enable virus file removal on the host.
- Custom Executable File Rules:** Supports users in detecting executable files by uploading Yara rules. Alarms will be generated when executable file names match Yara detection rules.
- Monitoring process access to malicious domains:** Enabled (switch is blue). Description: Perform DNS domain name resolution. When accessing a malicious domain, an alert will be reported. This feature depends on the DNS plugin (not supported in container environments), ebPF, or driver event source. Please install the DNS plugin or enable the corresponding event source before using. This section is highlighted with a red border. Buttons: 'Install DNS Plugin' and 'Event Source Configuration'.

4.3.4. Custom Rules

After completing the above steps, the system will listen for network connection events, monitor the IP and domain names accessed by the host, and match them against the system's built-in malicious IP library and malicious domain name library. If a match is found, a warning will be issued.

Users can also customize malicious IP and malicious domain names.

Enter the "Monitoring Configuration - Custom IOC" interface, input the malicious IP and malicious domain names you obtained, and save them. Once the system discovers that the host has accessed the system's built-in malicious IP library or malicious domain name library, it will immediately issue a warning.

Custom IOC

Malicious Hash Malicious IP Malicious Domain

Supports users in marking executable file hash values as black hash through new entries and alert detection reporting. Once blacklisted, the driver will block its execution. Note: During driver detection, the whitelist has a higher priority than the blacklist.

213 items Please select filter content

4.3.5. Alarm Viewing

In the "Intrusion Detection - Detection List" interface, filter for alarms of types "Accessing Malicious IP" or "Accessing Malicious Domain Name," then click to view the alarm details.

Risk Level	Alarm Type	Status	Time Range
Critical Risk	Parent process PID spoofing	8131 Pending	Last 1 Hour 413
High Risk	Process Injection	7144 Processing	Last 1 Day 2339
Medium Risk	Malicious file writing to disk	1446 Confirmed	Last 7 Days 8136
Low Risk	Malicious Process Initiation	1302 Ignored	Last 30 Days 10000+ Custom...
	Abnormal process loading	550	
	Process command line spoofing	517	
		264	

4.3.5.1. Accessing Malicious IP

The alarm details for accessing malicious IP include rules that triggered the detection, the process

that accessed the malicious IP, the malicious IP, the process chain, and suggestions for handling.

- Triggering Rule: The rule that detected the malicious IP.
- Process/Process Command Line: Information about the process that accessed the malicious IP.
- Malicious IP: The malicious IP accessed by the process.

The screenshot shows a detailed view of a security alert. At the top, a red 'Critical Risk' box contains the text 'Accessing Malicious IP Address'. Below this, the main title is 'Process svchost.exe accesses malicious IP [REDACTED]'. The interface is divided into several sections:

- Process Response:** Includes buttons for 'Add to Whitelist' and 'Pending'.
- Detection Information:** Contains fields for Detection Time (2025-03-03 22:57:13), ID (redacted), Response Result (-), Affected Devices (multiple icons), Tactic & Technique (Stealing through C2 channel (T1041) - steal), and All (4). It also includes Detection Method (Threat Intelligence Engine), Detection Explanation (The host accessing a known malicious IP indicates that the host may have been compromised.), Rule ID (All (2)), Process Name (redacted), Command Line (nscache), and Malicious IP (redacted).
- Process Chain Information:** Shows a process chain starting with '2025-02-26 10:12:19' and 'Process Name... wininit.exe(760)'.

4.3.5.2. Accessing Malicious Domain Name

The alarm details for accessing malicious domain names include triggering rules, the process that accessed the malicious domain name, the malicious domain name, the process chain, and suggestions for handling.

- Triggering Rule: The rule that detected the malicious domain name.
- Process/Process Command Line: Information about the process that accessed the malicious

domain name.

- **Malicious Domain Name:** The malicious domain name accessed by the process.

The screenshot shows a Sentry CWPP alert window. At the top, it says "High Risk Accessing Malicious Domains". Below that, a message states "The process curl accessed the malicious domain btc.f2pool.com". The main pane is titled "Detection Information" and contains the following details:

- Detection Time: 2025-02-27 08:30:29 — 1 times — 2025-02-28 08:30:28
- ID: [REDACTED]
- Response Result: -
- Affected Devices: [REDACTED]
- Tactic & Technique: Web Services (T1102) | Command and Control | All (3)
- Detection Method: Threat Intelligence Engine
- Detection Explanation: The host accessing known malicious domains indicates that the host may have been compromised.
- Rule ID: 1124852
- Process Name: [REDACTED]
- Command Line: [REDACTED]
- Malicious Domain: [REDACTED]

Below this is a "Process Chain Information" section, which is collapsed. It shows a timeline entry for 2025-02-11 12:45:59 with a Process Name of systemd(1).

4.3.6. Alarm Response

Supports blocking access to malicious IP and malicious domain names and can terminate the process.

4.3.6.1. Block Accessing

The system monitors network connection behaviors in real-time for the host's processes. If it detects that a process is accessing a malicious IP or malicious domain name, it can block the access and interrupt the network connection behavior.

Step 1: Enable the driver

Blocking network connections requires installing a driver. Enter the "Probes - Probe Management - Agent" interface, find the corresponding Agent, and click "More Operations" to enable the driver.

The screenshot shows the "Agent" management interface. At the top, there are four cards: "Agent Running Status" (Total Agents: 16, Offline Agents: 13; Online Agents: 3, Disabled Agents: 0), "Agent Running Trend" (Line chart for Total Agents and Online Agents from 02.20 to 02.26), "Innovation Agent Statistics" (Donut chart for Innovation and Non-Innovation), and "Agent Running Mode" (Donut chart for Host, Docker, and Pod). Below these is a search bar and a table titled "Please Select Filtering Content". The table lists 1/16 selected agents, with two rows highlighted. The first row has a red box around its checkbox and the "Running..." column. The second row has a red box around its checkbox and the "主机" column. The table columns include: Running..., Agent ID, Host, Host Type, Agent Version, Running L..., Host, Host Type, Agent Version, Running L..., Set Log Level, Set Run Level, Performance, Enable Driver, Disable Driver. The "Enable Driver" button for the second row is also highlighted with a red box.

Step 2: Enable the block switch

Enter the "Detection Configuration" interface, find the corresponding platform type and detection configuration, enable the two block switches under "Malicious Process Protection."

The screenshot shows the "Auto Blocking" settings page. It includes a summary section with "0/5 Not Enabled" and a note: "For devices with drivers installed, malicious process launches or behaviors will be automatically blocked upon detection. Please configure with caution." Below this are three links: "Auto Blocking Settings", "Configure detection whitelist", and "List of Devices with Disabled Driver Functionality".

Auto Blocking Settings

For devices with drivers installed, the system supports blocking malicious behaviors. You can enable the driver in the [Agent Management](#) interface.

Name	Description	Status
Process Hash-based Blocking	When a binary file's hash matches the blacklist hash database, its launch will be blocked.	<input type="button" value=""/>
Behavior-based Process Blocking	When a process exhibits confirmed malicious behavior, the malicious behavior will be automatically blocked.	<input type="button" value=""/>
Block Process Loading Malicious Modules	When a process loads a malicious module, the module loading will be automatically blocked.	<input type="button" value=""/>
Block Process Access Malicious Ip	When a host process accesses a malicious IP, it will be automatically blocked.	<input type="button" value=""/>
Block Process Access Malicious Domain	When a host process accesses a malicious domain, it will be automatically blocked.	<input type="button" value=""/>

4.3.6.2. Terminate Process

In addition to being able to block network connection behavior as described above, you can also terminate the process when a process accesses a malicious IP or malicious domain name. This includes both automatic termination of the process and manual termination of the process.

4.3.6.2.1. Automatic Termination of Process

Enter the "Response - Auto Response" page. When a warning of the specified type ("Access Malicious IP address" or "Access Malicious Domain Name") is issued, the system will automatically handle it, and no further manual intervention is needed.

You must first select the host type before setting up the trigger conditions.

If you want to set up automatic response strategies for **accessing malicious IP address**:

- Supported device types: Linux-Server, Linux-PC, Windows-Server, Windows-PC, Container

- Supported response elements: Process
- Alarm types: Choose "Access Malicious IP"
- Supported automatic response methods: Terminate the process

If you want to set up automatic response strategies for **accessing malicious domain names**:

- Supported device types: Linux-Server, Linux-PC, Windows-Server, Windows-PC, Container
- Supported response elements: Process
- Alarm types: Choose "Access Malicious IP"
- Supported automatic response methods: Terminate the process

Create Auto-Response Policy

Basic Information

Status:

* Policy Na... : Please enter the policy name

Policy Desc...: Please enter a policy description

* Host Type: Please select a host type

* Application: All Day Custom Time Range (i)

Trigger Conditions

When the alarm meets the following conditions, the response will be automatically triggered.

* Response... : Please select a response Please select an alarm type

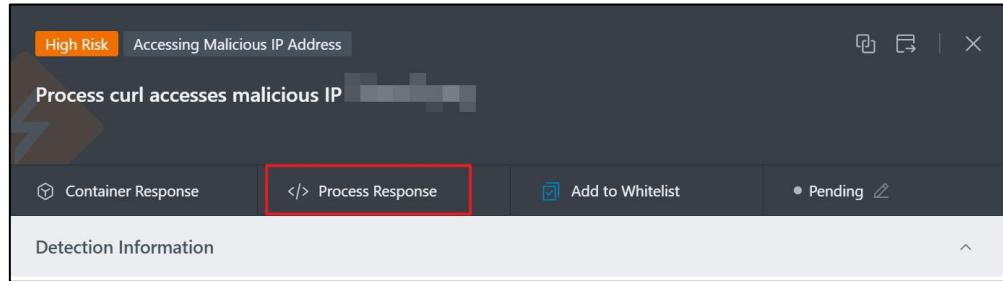
* Alarm Level: Please select the alert level

Alert frequ... : Single Alert
An alert triggers a response each time it is generated.
 Repeated Alert
If the same device triggers alerts repeatedly in a short period, it is considered to have a high credibility of being a real threat, and more forceful response measures can be taken. (i)

4.3.6.2.2. Manual Termination of Process

If no automatic response strategy is set up, when a malicious IP address or malicious domain name

access warning is issued, you can manually terminate the process in the "Alarm List" interface by finding the corresponding alarm and clicking "Terminate Process."



4.3.6.3. Add to Whitelist

If there is a false positive, click the "Add to Whitelist" button in the alarm details interface, adding the process, IP, or domain name information to the whitelist. The host will then no longer produce alarms when accessing this IP or domain name.

New Whitelist

Set Whitelist Conditions

Please set the whitelist conditions. The conditions are connected with 'AND,' which means that detection information can only apply the whitelist when it completely meets all the set whitelist conditions.

Condition	Matching Method	Value	Reset
Alert Type	Equals	Accessing Malicious IP Address	
Process Name	In	curl	
Process Command Line	Equals	curl -m 5 1 ²	
Target IP	In	1 ²	

+ Add Condition

Application Scope

Please select the range of hosts to which the whitelist applies. Only containers within the range can apply the whitelist.

All Hosts

Select some hosts

Current Host

All Clusters

Select Container Cluster

4.4. Container Behavior Model

Containers enable more flexible and cost-effective software development and application deployment. However, container security construction lags far behind the speed of business development. Container images are usually obtained from external sources and may contain vulnerabilities or malicious software. If these images are deployed into orchestration systems without verification or review, attackers can exploit these vulnerabilities or malicious images to gain

shell access within the container, using it as a starting point to execute various commands and malicious operations within the container, such as information gathering and privilege escalation. In a container cluster, compromising a single container allows lateral movement to other containers or escape to the node for persistence, controlling the entire node. Next, attackers can exploit vulnerabilities to control the entire cluster, causing significant losses to the victim.

Container Behavior Model function collects data on processes and network behaviors within containers to establish a set of normal behavior characteristics. Once the model is in monitoring mode, any behavior that violates the model will immediately trigger an alert.

4.4.1. Function Authorization

Only after purchasing the "Container Security Extension Pack" product and assigning the "Container Security Extension Pack" authorization to the Agent will the Agent have the Container Behavior Model function.

Method 1: Authorize during Agent Installation

Assign authorization during Agent installation. Navigate to the "Probes - Installation - Agent" interface, and select Container Security - Container Security Extension Pack.

Agent

Here you can view the objects that the probe can protect, the supported systems, and the dependent environments. You can also follow the installation steps to try deploying and installing the probe.

Linux

Windows

Kubernetes

Openshift

Install on Linux

Recommended Host Docker

Basic Configuration

Default Aut... : Server Version PC Version

To ensure the normal operation of the system when enabling container security authorization, please make sure
① that the CPU limit threshold and memory limit threshold of the Agent are not less than 1C and 1000M
respectively.

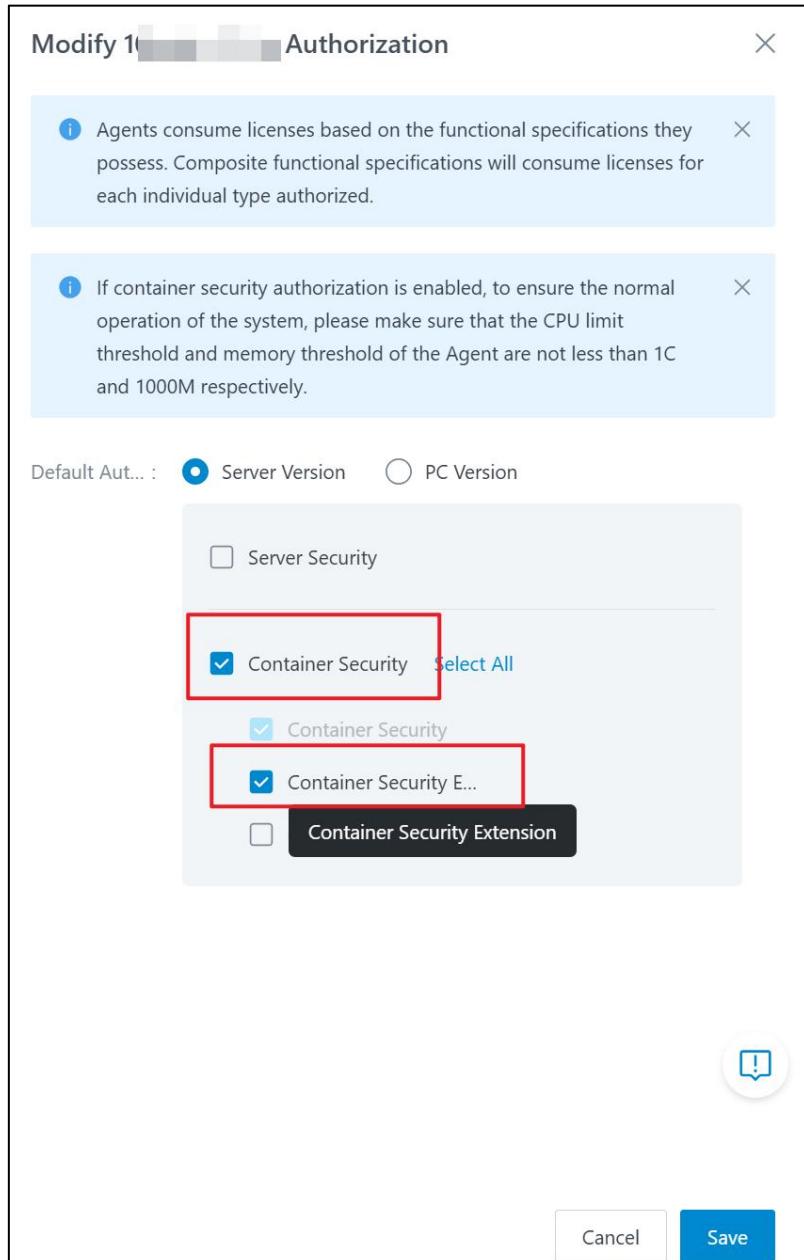
Server Security

Container Security Select All

Container Security E... Container Event Coll...

Method 2: Modify Agent Authorization

After the Agent is installed, you can also modify the authorization information to assign the "Container Security Extension Pack" authorization. Navigate to the "Probes - Probes Management - Liscense" interface, click "Configuration Authorization" to modify the authorization.



4.4.2. Precondition

The system default settings only enable basic event sources. It is recommended to enable ebpf or driver event sources; otherwise, the Container Behavior Model will only have partial behavior monitoring capabilities such as process startup monitoring.

Navigate to "Probes - Probe Management - Agent" click "Event Source Configuration" to enter the event source configuration page, find the Linux host that needs to enable event sources, click "Configuration", and enable ebpf or driver event sources.

Note: Driver event sources depend on drivers. To enable driver event sources, ensure that the Agent also enables the driver. Navigate to the "Agent" interface, find the corresponding Agent, and enable the driver.

Agent ID	Host	Enable Event Source	Audit Subscription Status	Driver Status	ebpf status	Operation
		<input type="checkbox"/>	<input type="button" value="禁止订阅"/>	<input type="button" value="Disabled"/>	<input type="button" value="Disabled"/>	<input type="button" value="Configurable"/>

If a newly installed host needs to enable the corresponding event sources, click the "Default Configuration" button in the upper right corner to enable the corresponding event source switches.

Basic Event Source	<input checked="" type="checkbox"/>	Ebpf Event Source	<input type="checkbox"/>	Audit Event Source	<input type="checkbox"/>
Scope of Application		Scope of Application		Scope of Application	

Driver Event Source	<input type="checkbox"/>	Driver Event Source	<input type="checkbox"/>
Scope of Application		Scope of Application	

4.4.3. Detection Configuration

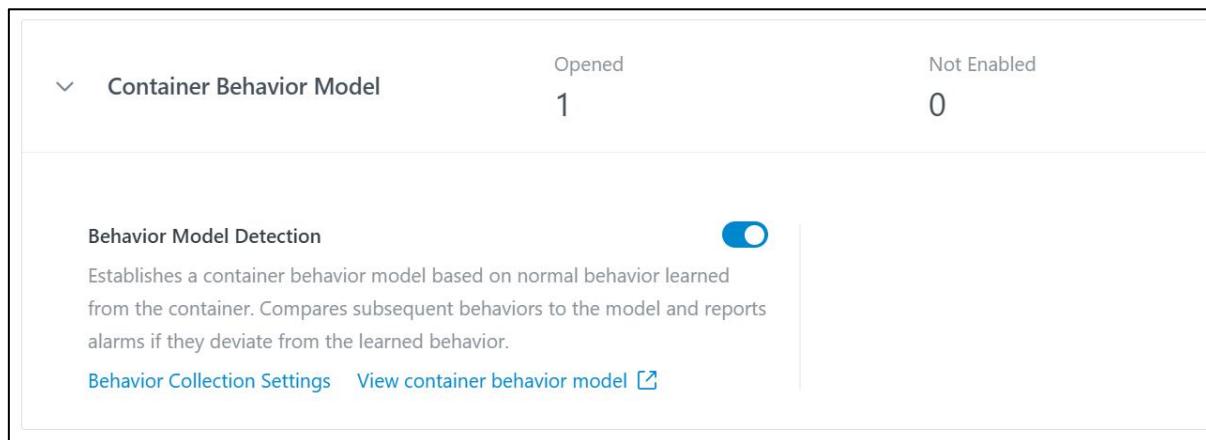
4.4.3.1. Function Activation

The system defaults to disabling the container behavior learning function. After the host obtains the authorization for the container behavior learning model, it needs to be manually enabled. Under the Linux-Server label, find the corresponding detection configuration, and turn on the "Behavior Model Detection" switch in the configuration details.

- Newly installed hosts: If you want newly installed hosts to automatically enable container

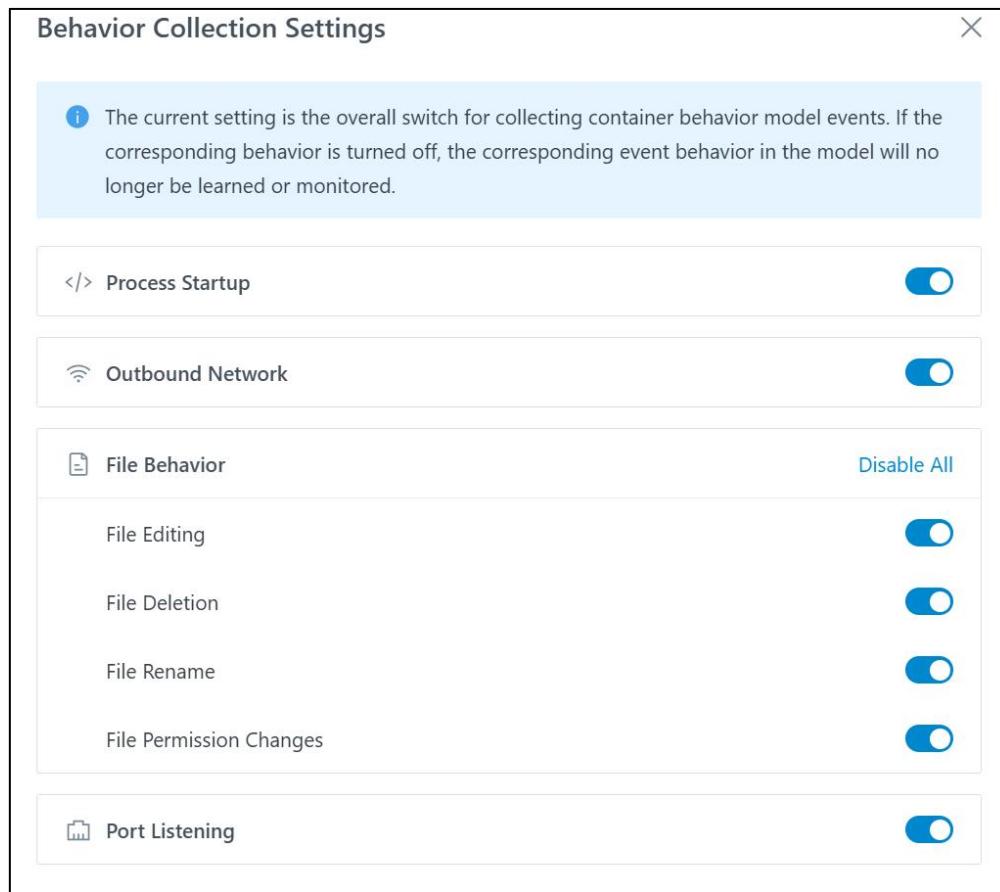
behavior learning capabilities, modify the default detection configuration and turn on the behavior model detection switch.

- Enable container behavior learning function only for specific hosts: Keep the behavior model detection switch off in the default detection configuration, and create a custom detection configuration to turn on the behavior model detection switch in the custom detection configuration.



4.4.3.2. Behavior Collection Settings

In the detection configuration details interface, click "Behavior Collection Settings" to configure the behaviors to be collected by the behavior model. By default, all behaviors are collected. This configuration is a global switch; after modification, all models will collect behaviors according to the new settings.



4.4.4. Model Viewing and Adjustment

The system provides default settings for model creation. When the user enables the Container Behavior Model function on the host, the model will be automatically created using the default parameters. The generated model can be viewed in the "Detection Configuration - Container Behavior Model" interface.

Container Behavior Model

Behavior models are generated by learning the normal business behavior of containers. Behaviors that violate the model are considered suspicious and reported as alarms.

Monitoring Learning Archived

The monitoring container behavior model will generate alarms if the behavior in the container is not within the normal behavior of the model. If the conditions for relearning are met, the model status can be manually or automatically changed from 'Monitoring' to 'Learning'. If no behavior occurs in the corresponding container under the model for more than 30 days, the current model will be automatically archived, and the model status will automatically change from 'Monitoring' to 'Archived'.

	Status	Model ID	Image Name	Associated...	Associated...	Cluster Name	Namespace	Belongs to Controller	Monitor	Operation
<input checked="" type="checkbox"/>	[REDACTED]	[REDACTED]	[REDACTED]	0	0	Non-Cluster	NO Namespace	-	5 days 1	View Details Relearn Archive

	Descriptions
Learning	<ul style="list-style-type: none">Models in the learning phase do not generate alerts. All collected behaviors are considered normal, and users can manually adjust the set of normal behaviors.If "Smart Online" mode is selected, the model will automatically enter monitoring mode if no new process behaviors occur within a specified time (starting from the model creation). If "Manual Intervention" mode is selected, the user needs to manually put the model into use; otherwise, the model will remain in the learning state.If no behavior occurs in the container corresponding to the model for more than 30 days, the current model will be automatically archived and moved to the archived list.
Monitoring	<ul style="list-style-type: none">Models in the learning phase support manual and automatic monitoring.Once the model is in monitoring mode, the behaviors in the model will serve as the behavior baseline. If a behavior outside the baseline occurs within the container, an alert will be generated.If "Smart Offline" mode is selected, the monitoring model will automatically revert to "Learning" mode when the offline conditions are met.If no behavior occurs in the container corresponding to the model for more than 30 days, the model will be automatically archived and moved to the archived list, and no further alerts will be generated.
Archived	<ul style="list-style-type: none">When no behavior occurs in the container corresponding to a monitoring or learning model for more than 30 days, the model will be automatically moved to the archived list. Users can also manually archive models.

- If a new behavior occurs in the container corresponding to an automatically archived model, the model will automatically enter the learning list and start relearning. If the model was manually archived by the user, it must be manually operated by the user to start relearning.
- If a container is archived for more than 30 days, the model will be automatically deleted. Manual deletion of models is also supported.

If the user wishes to change the system default parameters, click

Model Parameter Settings

on the "Detection Configuration - Container Behavior Model" page to make modifications.

The screenshot shows the 'Container Behavior Model' configuration page. At the top, there is a header with 'Container Behavior Model' and two buttons: 'Update Cluster Information' and 'Model Parameter Settings' (which is highlighted with a red box). Below the header, there is a note: 'Behavior models are generated by learning the normal business behavior of containers. Behaviors that violate the model are considered suspicious and reported as alarms.' Underneath this note, there are three tabs: 'Monitoring' (selected), 'Learning', and 'Archived'. The main content area displays a table with one row. The table has columns for 'Model Name', 'Status', 'Last Update', and 'Actions'. The single row shows 'Container Behavior Model' as the model name, 'Monitoring' as the status, '2023-10-10 10:00:00' as the last update, and 'Edit' (with a red box around it) as the actions. There is also a note below the table: 'The monitoring container behavior model will generate alarms if the behavior in the container is not within the normal behavior of the model. If the conditions for relearning are met, the model status can be manually or automatically changed from 'Monitoring' to 'Learning'. If no behavior occurs in the corresponding container under the model for more than 30 days, the current model will be automatically archived, and the model status will automatically change from 'Monitoring' to 'Archived'.' At the bottom of the page, there is a search bar with 'Please Enter Search Term' and a magnifying glass icon, along with buttons for 'Enable', 'Disable', 'Archive', and 'Relearn'.

If the user wishes to modify the model information for a specific model, they can view the model details in the model list under "Detection Configuration - Container Behavior Model" and click [Edit] to make changes.

Container Behavior Model Details

Monitoring | Monitored 5 days 1 hours 6 minutes | Relearn | Archive Model | Close Model

Image N... r | Associate... 0 | Namespa... 无命名空间 | Image ID: | Cluster Na... 非集群 | Belongs to ... -

Model Information Edit

Directory Ag... If the number of file behaviors in the same directory exceeds 10, the file behaviors are automatically aggregated

Behavior ... Process Startup Outbound Network Port Listening
 File Editing File Deletion File Rename
 File Permission Changes

4.4.5. Alarm Viewing

For models in monitoring mode, when a behavior not in the model occurs within the container, an alert will be generated. There are two ways to view Container Behavior Model alerts:

Method 1: View from the Alert List

In the "Intrusion Detection - Alert List," filter alerts by type "Container Behavior Model" or search by "Model ID" to view alerts related to a specific Container Behavior Model.

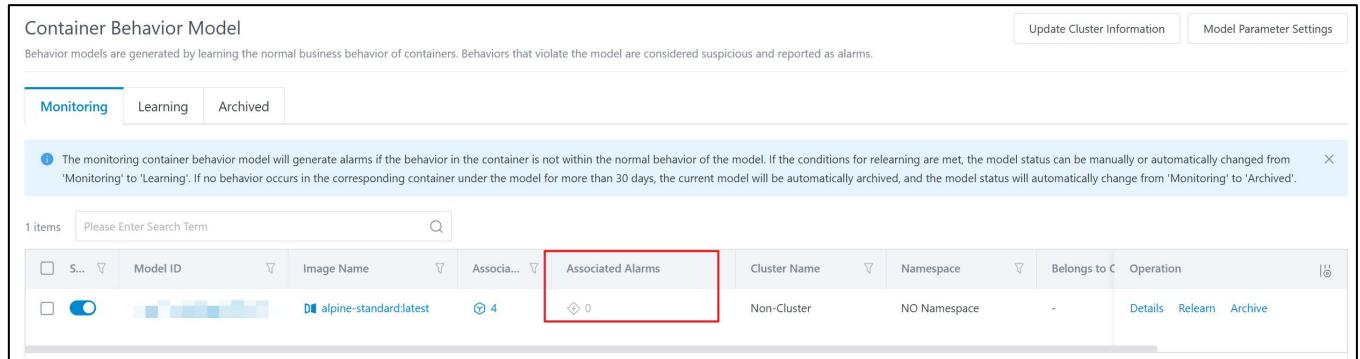
Detection List

Time Range: Last 7 Days | Risk Level: Critical Risk, High Risk, Medium Risk | **Alarm Type: Container Behavior Model** | Please manually enter the content you want to inquire after the colon and press Enter to finish. | Q

Risk Level	Alarm Type	Status	Time Range
Critical Risk	Parent process PID spoofing	8104 Pending	Last 1 Hour
High Risk	Malicious file writing to disk	7123 Processing	Last 1 Day
Medium Risk	Process Injection	609 Confirmed	2016
Low Risk	Malicious Process Initiation	339 Ignored	8104
	Abnormal process loading	3462 Select All	Last 7 Days
	Process command line spoofing	1505 <input type="checkbox"/> Parent process PID spoofing	8100+
		1308 <input type="checkbox"/> Malicious file writing to disk	Custom...
		543 <input type="checkbox"/> Process Injection	
		511 <input type="checkbox"/> Malicious Process Initiation	
		255 <input type="checkbox"/>	

Method 2: View from the Model List

Navigate to the list of monitoring Container Behavior Models, and in the model details interface, you can view the associated alerts for that model.



The screenshot shows the 'Container Behavior Model' section of the Sentry CWPP interface. At the top, there are buttons for 'Update Cluster Information' and 'Model Parameter Settings'. Below this, a navigation bar has tabs for 'Monitoring' (which is selected), 'Learning', and 'Archived'. A note below the tabs explains that monitoring models generate alarms if behavior is outside normal. The main area displays a table with one item. The columns include: a checkbox, 'Model ID' (alpine-standardtest), 'Image Name' (alpine), 'Associated Alarms' (4, highlighted with a red box), 'Cluster Name' (Non-Cluster), 'Namespace' (NO Namespace), 'Belongs to C' (empty), and 'Operation' (Details, Relearn, Archive). A search bar at the top says 'Please Enter Search Term'.

The Container Behavior Model alert details will display different alert details based on the behavior type. For example, if an abnormal network connection is detected from a container process, the connected port and IP information will be displayed, along with specific behavior logs (up to TOP100 due to performance considerations).

4.4.6. Alert Response

For Container Behavior Model-related alerts, the system supports both automatic and manual responses.

4.4.6.1. Automatic Response

Navigate to the "Security Response - Automatic Response" page to create an automatic response strategy. When a Container Behavior Model alert occurs, the system will automatically handle it without requiring manual user intervention.

- Device types that can be configured: Linux-Server
- Supported automatic response elements: Containers
- Supported automatic response methods: Pause container, Isolate container, Delete container

Create Auto-Response Policy

Basic Information

Status:

* Policy Na... : Please enter the policy name

Policy Desc...: Please enter a policy description

* Host Type: (highlighted with a red box)

* Application...: All Hosts Select some hosts

* Application...: All Day Custom Time Range

Trigger Conditions

When the alarm meets the following conditions, the response will be automatically triggered.

* Response...: (highlighted with a red box) Please select an alarm type

* Alarm Level: Please select the alert level Reverse Shell

Alert freq...: Single Alert (An alert triggers a response each time it is generated.) Repeated Alert

4.4.6.2. Manual Response

In the alert details, users can manually handle the alert information. For suspicious container behaviors detected by the Container Behavior Model, users can refer to the system's handling suggestions and manually respond to the container and process.

High Risk Container Behavior Model

The container behavior detection engine identified a process named kafka-scheduler renaming the file /bin/kafka-scheduler -checkpoint, which is suspected to be anomalous behavior.

• Pending

Add to Model

4.4.6.3. Response Logs

Whether it is an automatic or manual response, each response will be logged. Click "Security

"Response - Response List" to view related response records.

- Operation History: Records every response, whether successful or failed.
- Response List: Records successfully responded elements. Some responded elements can be restored. For example, isolated containers can be unisolated under the "Container" tab.

The screenshot shows the "Response List" page with the "Container" tab highlighted by a red box. Below the tabs, there is a note explaining the purpose of the container response list. Underneath the note, there are three categories: "Paused Container", "Isolated Container", and "Restored Container". A search bar with placeholder text "Please Enter Search Term" and a magnifying glass icon is present. At the bottom, there is a table header with columns: "Response Time", "Affected Devices", "Reason", "Disposal Mechanism", "Execution Account", "Operation", and a column with a gear icon. The "Response Time" and "Affected Devices" columns have dropdown arrows.

4.4.6.4. False Alarm

When a false alarm occurs, it can be whitelisted.

4.4.6.4.1. Whitelisting from Alerts

In the alert details interface, click **[Add to Model]**, enter the relevant information about the false positive container behavior, and save it. The false positive alert will be automatically removed from the alert list and will not trigger alerts in the future.

New Whitelist

Set Whitelist Conditions

Please set the whitelist conditions. The conditions are connected with 'AND,' which means that detection information can only apply the whitelist when it completely meets all the set whitelist conditions.

Condition	Matching Method	Value	Reset
Process Command Line	Equals	[REDACTED]	

+ Add Condition

Application Scope

Please select the range of hosts to which the whitelist applies. Only containers within the range can apply the whitelist.

All Hosts

Select some hosts

All Clusters

Select Container Cluster

Select container node image

Scope of affected alarms

Please select the range of alarms affected by the whitelist. If you choose to affect alarms in the past 30 days, past alarms will be marked as whitelisted and removed from the detection list. Users need to check in the whitelist, and future new alarms will be whitelisted and not displayed.

4.4.6.4.2. Whitelisting from Models

On the "Detection Configuration - Container Behavior Model" page, view the model details. Under the corresponding behavior labels, such as process startup or network outbound, click

New

Container Behavior Model alerts that meet the whitelist conditions will be automatically removed from the alert list and will not trigger alerts in the future.

The screenshot shows the 'Container Behavior Model Details' page. At the top, there's a monitoring status bar with a green 'Monitoring' button, a timestamp 'Monitored 31 days 11 hours 41 minutes', and three buttons: 'Relearn', 'Archive Model', and 'Close Model'. Below this, there are several status indicators: 'Image N...' (blue progress bar), 'Associate...' (4 icons), 'Namespa...' (NO Namespace), 'Image ID' (hex code), 'Cluster Na...' (Non-Cluster), and 'Belongs to ...' (-). A 'Model Information' section includes a 'Edit' link, a note about directory aggregation, and a list of monitored behaviors: Process Startup, Outbound Network, Port Listening, File Editing, File Deletion, File Rename, and File Permission Changes. Below this are learning thresholds: Process 2000, Network 100, File 2000, and Port Listening 100. It also shows learning mode (Auto Deployment, Exceeded 7 days and continuously 3 days), monitoring mode (Auto Offline, Within 5 minutes, cumulative alarms generated 20 unit), and a summary bar with 'Process Startup (100)', 'Outbound Network (3)', 'File Behavior (32)', 'Port Listening (7)', and 'Associate Alarms (0)'. A search bar at the bottom left says 'Please Enter Search Term' with a magnifying glass icon, and a blue 'New' button is highlighted with a red border on the right.

4.5. Antivirus

Computer virus is a malicious code written by cyber criminals that can attach itself to host programs by modifying other programs and inserting its own code. This malicious code is typically characterized by its ability to spread, hide, and cause damage, posing significant threats to computer systems and information security.

Antivirus functionality combines multiple virus detection engines to monitor running processes and files in real-time, perform static file scanning, and immediately isolate or remove viruses upon detection. The system supports both local and cloud-based scanning, ensuring high detection rates while maintaining timely response capabilities to help users address issues related to viruses, trojans, and other malicious software, ensuring host security.

- **Process Monitoring:** When a process starts, the virus engine scans the process file for viruses.

If a virus is detected, an "Unauthorized Process Startup" alert is issued immediately.

- **File Monitoring:** When files meet certain conditions and are saved to the disk, the virus engine scans the file process for viruses. If a virus is detected, an "Unauthorized File Write" alert is issued immediately.
- **Static File Scanning:** A scan task is created to scan files on the host. If a virus is detected, an "Infection File" alert is issued immediately.

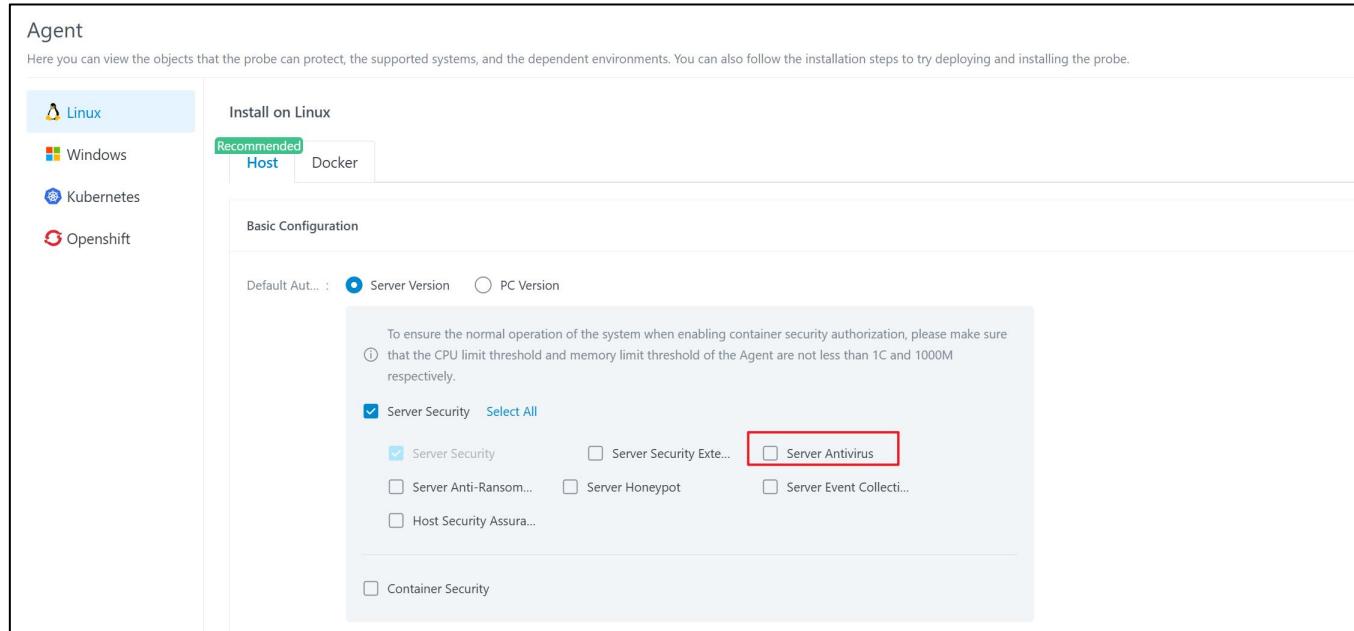
4.5.1. Functional Authorization

Only if the "Host Antivirus" or "PC Antivirus" product is purchased and the Agent is assigned the corresponding "Host Antivirus" or "PC Antivirus" authorization can the Agent enable antivirus protection for the host.

If you need to scan files within containers for viruses, please purchase and assign the "Container Security Extended Package" authorization to the Agent. The Container Security Extended Package includes the ability to scan and isolate viruses in container files.

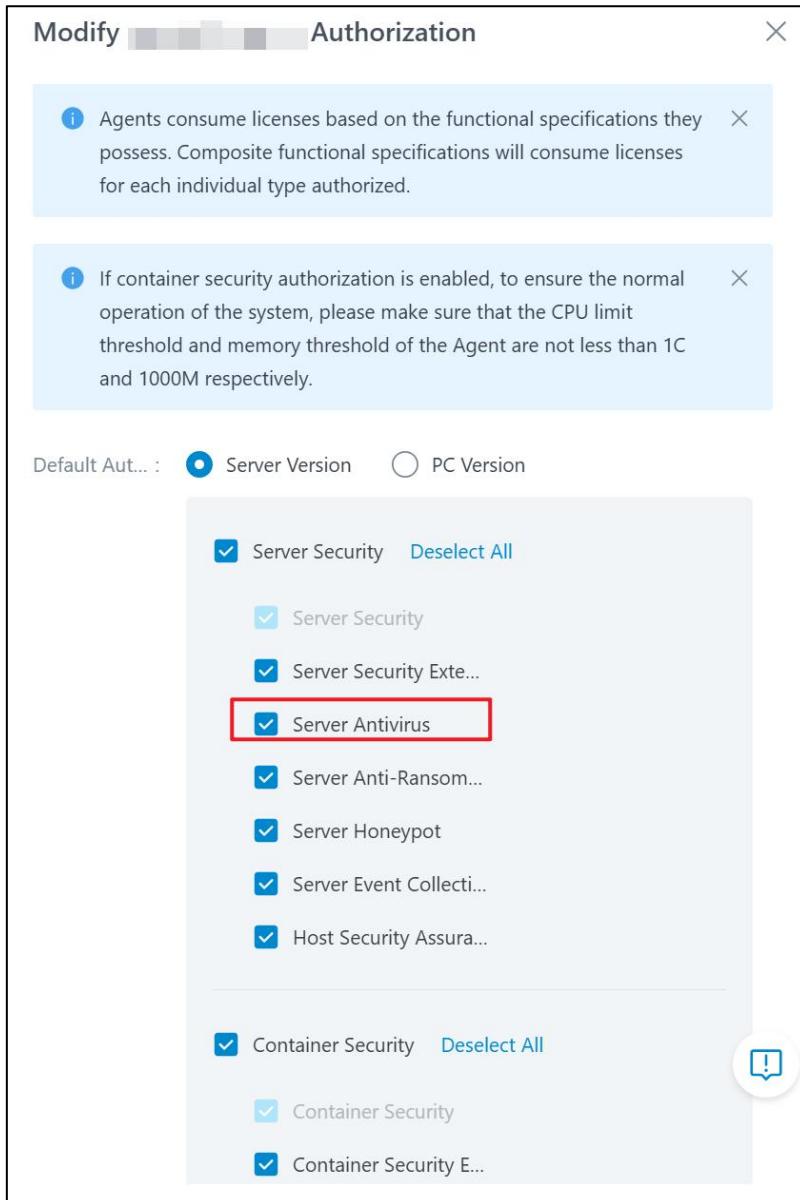
Method 1: Authorization during Agent Installation

During Agent installation, assign the authorization. Enter the "Probe Management - Installation Guide - Agent" interface, select the corresponding operating system and authorization function. For example:



Method 2: Modify Agent Authorization

After installing the Agent, you can also modify the authorization information and assign "Host Antivirus" or "Terminal Antivirus" authorization. Enter the "Probe Management - Runtime Management - Authorization Configuration" interface, click "Authorization Configuration," and refer to the example provided in the image.



Whether the Agent has antivirus enabled can be viewed in the "Probe Management - Runtime Management - Authorization Configuration" interface or in the detection configuration page, where you can find the corresponding platform type and configuration details, then click "Host Antivirus Management" to view the statistics of antivirus capabilities for the host.

- **Local Engine Installation:** Whether the Agent has a local virus engine installed.
- **Host Antivirus:** If the Agent is of Server host type, this indicates whether the Agent has been assigned "Host Antivirus" authorization. If the Agent is of PC host type, this indicates whether the Agent has been assigned "Terminal Antivirus" authorization.

- **Container Antivirus:** Only visible if the Agent is of Server host type, indicating whether the Agent has been assigned "Container Extended Package" authorization, which includes antivirus capabilities.

The screenshot shows a collapsed section titled "Virus File Searching And Killing". Inside, there are two sections: "Malicious File Write Detection" and "Protected Host Management". The "Protected Host Management" section contains a note about enabling virus file scanning on hosts or containers, mentioning the requirement for a local antivirus engine. A red box highlights the "Protected Host Management" button.

The page displays statistics on the number of hosts where Host Antivirus is enabled, the number of hosts where Container Antivirus is enabled, and local engine installation statistics for the user's managed hosts.

The screenshot shows the "Protected Host Management" statistics page. It features three main cards: "Host Antivirus" (0 Protected), "Container Antivirus" (0 Protected), and "Local Engine Installation Statistics" (0 Installed). Below these cards is a search bar with placeholder text "Please select filter content" and a filter dropdown menu. The menu includes columns for "Agent ID", "Host", "Host Type", "Is the local e...", "Host Antivi...", "Container ...", and a search icon.

4.5.2. Install Local Engine

Virus file scanning requires a local antivirus engine. Manual or automatic installation and updates are supported.

4.5.2.1. Manual Installation

Enter the "Probe Management - Component Management - Engine Management" interface, find the host you need to install, and click "Install."

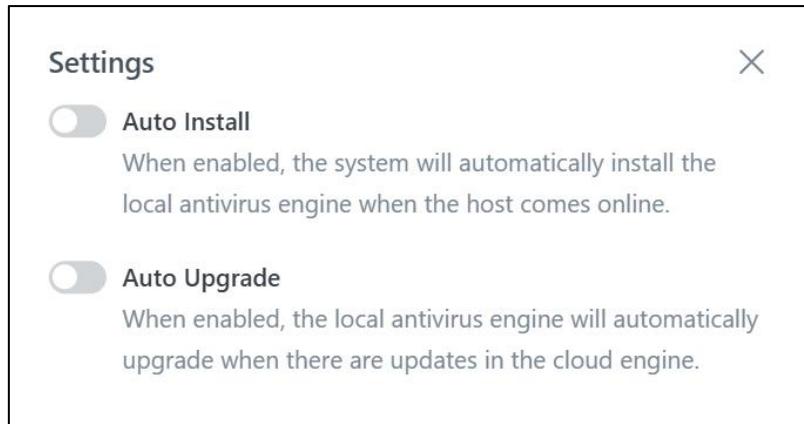
- The engine will automatically install the latest version of the virus engine during installation.
- If the local virus engine is not installed, the virus library status will be "Not Installed."
- If the virus engine is installed but not updated to the latest version, the virus library status will be "Outdated," and you can click "Upgrade" to upgrade to the latest engine version for free.
- If the engine is already installed with the latest version, the virus library status will be "Latest Version," and the "Install" and "Upgrade" buttons will be disabled.

The screenshot shows the 'Engines' management interface. At the top, it displays statistics: Total Hosts (14), Not Installed (11), Pending Upgrade (0), Latest Version (2), Installing (1), and Upgrading (0). Below this is a search bar and a toolbar with buttons for More, Export, Settings, Export All, and View Latest Virus Database Version. The main area is a table titled '14 items' with columns for Run Mode, AgentID, Host, Operating System, Host Type, Current Virus Database Version, Virus Definition Status, and Operation. Two hosts are listed: one Windows 10 PC with version 2025-02-06 06:52:00 and the latest definition, and one CentOS Linux Server with version 2025-02-06 06:51:53 and the latest definition.

Run Mode	AgentID	Host	Operating System	Host Type	Current Virus Database Version	Virus Definition St...	Operation
Host	9f1 [REDACTED]	1 [REDACTED]	Microsoft Windows 10 企业版 (build 18363)	PC	2025-02-06 06:52:00	最新版本	Install Upgrade
Host	55 [REDACTED]	1 [REDACTED]	CentOS Linux release 7.6.1810 (Core)	Server	2025-02-06 06:51:53	最新版本	Install Upgrade

4.5.2.2. Automatic Installation

In the "Probes- Components - Engines" interface, click "Settings" to enable automatic installation and updates for future hosts that are newly installed online. The local virus engine will also automatically update when a new engine version is released.



4.5.3. Detection Configuration

4.5.3.1. Unauthorized Process Startup

Supports scanning and isolation of viruses on processes for Server hosts, terminals, and containers.

After installing the Agent and assigning antivirus authorization, this functionality becomes available.

4.5.3.2. Unauthorized File Write

Supports scanning and isolation of viruses on files for Server hosts and terminals. After installing the Agent and assigning antivirus authorization, this functionality becomes available.

Users can also adjust file type and size parameters for detection. Enter the "Detection Configuration" interface, select the platform type, and under "Virus File Scanning" or "Unauthorized File Write Detection," click "Configuration" to adjust the malicious file types and sizes to be detected.

- **File Type:** Indicates the file types you want to detect. Files not selected will not be scanned.
- **File Size:** To prevent excessive performance consumption, you can set the maximum file size to be detected. The system defaults to 300MB, so files larger than this size will not be scanned.
- **Executable File Size Threshold:** The system will not scan files larger than this threshold. However, to bypass detection, cyber criminals may upload a large file. Therefore, an

additional "Over executable file size" low-risk alert is added. When an executable file reaches the threshold, a low-risk alert is issued.

- **Compression Package Level:** The system supports virus detection within compressed packages. Note: If multiple viruses are found within the same compressed package, multiple virus alerts will be generated. Responding to one alert will also handle the other viruses in the package. To prevent performance issues, you can set the maximum compression package level to be scanned. Packages with more than this level will not be scanned.
- **Enable Server-Side Detection:** The system prioritizes using the local virus engine for detection. If the "Server-Side Detection" switch is enabled (default), small executable files that are not detected locally will be uploaded to the server for detection using the server engine.

The screenshot shows a configuration interface for a Linux-PC system. At the top, there's a header bar with 'Linux-PC System Default Configuration' on the left and 'Cancel' and 'Save' buttons on the right. Below the header, there's a main content area with a red border around the 'Virus File Searching And Killing' section. This section contains three main items: 'Malicious File Write Detection', 'Protected Host Management', and 'Scan Period Configuration'. Each item has a brief description and a 'Settings' link. There are also 'Trust Zone' and 'Trust Zone Setting' sections at the bottom left. The 'Save' button is highlighted in blue at the top right of the content area.

Virus File Searching And Killing		
Malicious File Write Detection Users can customize the configuration for detecting malicious files, including type and size. Detection Settings	Protected Host Management Users can customize whether to enable virus file scanning on the host or container. This feature requires the installation of a local antivirus engine. Protected Host Management	Scan Period Configuration Users can customize the directories to be scanned and the scan frequency. The system will execute scans based on the settings and use multiple engines to detect whether the files are malicious. Scan Management View Scanned Records
Trust Zone Users can customize the trusted zone. When performing virus scanning, the trusted zone will be skipped and not scanned. Trust Zone Setting		

Malicious File Write Detection Settings X

Info: The client detection function requires the local engine to be installed to take effect. If the executable files are not detected as problematic by the client, they will be reported to the cloud for detection.

* Detect Files: Executable files Script files Document files
 Compression Package Files Other Files

* File Size: If the file size is greater than M, it will automatically skip detection.

* Oversized execut... When an executable file larger than M is detected, a low-risk alert will be generated.

* Archive Layer: Maximum detection of layers of archive

* Enable server-side de...

4.5.3.3. Scan

For potentially virus-infected files on the disk, users can create scan tasks. The system supports manual one-time scans or scheduling automatic periodic scans.

- A single host can only run one scan task at a time. If another scan command is sent while a scan is already in progress, the scan will fail.
- If a scan task is in progress and a virus library update or removal command is sent, the scan will be automatically terminated to prioritize the update or removal operation.

4.5.3.3.1. Scheduled Scans

In the detection configuration page, under "Virus File Scanning," click "Scan Management" and select

New

to configure the scan schedule.

This screenshot shows the 'Virus File Searching And Killing' section of the Sentry CWPP interface. It includes three main configuration panels: 'Malicious File Write Detection', 'Protected Host Management', and 'Scan Period Configuration'. The 'Scan Period Configuration' panel has a red box around the 'Scan Management' tab, which is currently selected.

Malicious File Write Detection
Users can customize the configuration for detecting malicious files, including type and size.

Detection Settings

Protected Host Management
Users can customize whether to enable virus file scanning on the host or container. This feature requires the installation of a local antivirus engine.

Scan Period Configuration
Users can customize the directories to be scanned and the scan frequency. The system will execute scans based on the settings and use multiple engines to detect whether the files are malicious.

Scan Management (highlighted with a red box)
[View Scanned Records](#)

Trust Zone
Users can customize the trusted zone. When performing virus scanning, the trusted zone will be skipped and not scanned.

[Trust Zone Setting](#)

This screenshot shows the 'New Virus File Kill' configuration dialog. It allows users to choose between 'Quick Kill', 'Full Disk Kill', and 'Custom Kill' modes. The 'Quick Kill' mode is selected. Below this, various scanning parameters are set: Scan Mode (Balanced), Scan Object (Host), Scan Range (All Hosts), Scan File (Executable files, Script files, Document files, Compression Package Files checked; Other Files unchecked), Scan Period (Daily), Start Time (00:00), and Scan Duration (120 minutes). A note states that if the duration exceeds the limit, the scan task will be terminated.

New Virus File Kill

Quick Kill
Scan only files under critical syste...

Full Disk Kill
Scan all files under disk directories

Custom Kill
Scan files under user-specified di...

Scan Mode: Low Speed (CPU usage ≤10%) Balanced (CPU usage ≤50%) High Speed (No Limit)

Scan Object: Host Container

Scan Range: All Hosts
 Select some hosts

Scan File: Executable files Script files Document files Compression Package Files Other Files

Scan Period: Daily Weekly Expression

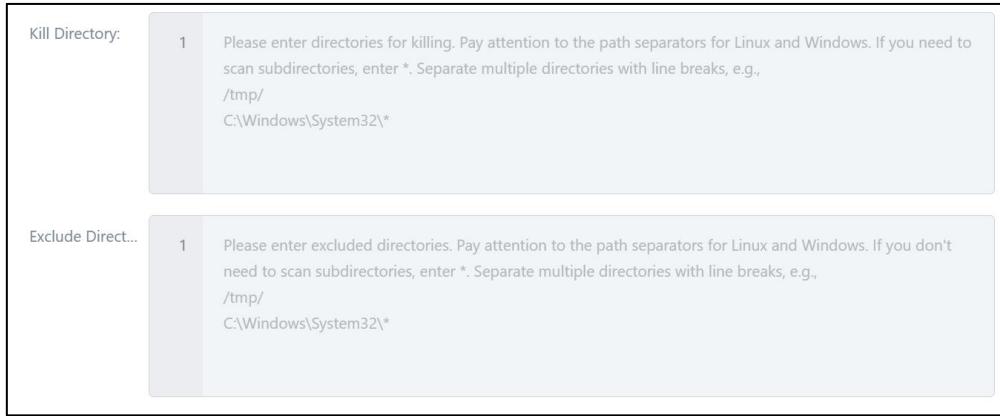
Start Time: 00:00

Scan Duration: Maximum scan duration per host: 120 minutes
If it exceeds the limit, the scan task on the host will be automatically terminated.

[More Settings](#) ▾

Note:

- **Scan Type:** The system provides three virus scanning modes.
 - **Quick Scan:** Scans only files in system directories.
 - **Full Scan:** Scans all files across all disk directories.
 - **Custom Scan:** Users can specify directories to scan and exclude certain directories. The system will only scan the directories specified by the user.



- **Scan Mode and Duration:** To prevent performance issues, users can set the scan mode and duration based on their needs.
- **Scan Schedule:** Users can set the schedule for when the scan task should start.
- **Users can also set parameters for the files to be scanned, such as file size, compression package level, and directory level.**

4.5.3.3.2. One-Time Scan

In the "Intrusion Detection - Detection List" interface, click the "Manual Scan" button in the top-right corner of the table, select "Virus File Scanning."

Risk Level	Alarm Type	Affected Device Type	Status	Time Range
Critical Risk	Suspicious Process Parameters	Host	Pending	Last 1 Hour
High Risk	Customize Suspicious Processes	Container	Processing	Last 1 Day
Medium Risk	Web Backdoor	Cluster	Confirmed	Last 7 Days
Low Risk	Malicious Process Initiation		Ignored	Last 30 Days
	Reverse Shell			Custom...
	Malicious file writing to disk			

Group by: All Host Container Cluster Total 2004 alarms Select All

Risk Level: Detection Time: Alarm Type: Description: Affected Devices: Virus File Searching And Killing

High Risk 2025-02-26 08:14:01 Customize Suspi... 发现进程命中进程行为自定义规则

2025-02-26 12:10:01

Virus File Sear... Memory Back...

Fill in the necessary parameters, and click "Save" to create a one-time virus scan task.

New Virus File Kill

Quick Kill
 Scan only files under critical syste...

Full Disk Kill
 Scan all files under disk directories

Custom Kill
 Scan files under user-specified di...

Scan Mode: Low Speed (CPU usage ≤10%) Balanced (CPU usage ≤50%) High Speed (No Limit)

Scan Object: Host Container

Scan Range: All Hosts
 Select some hosts

Scan File: Executable files Script files Document files Compression Package Files Other Files

Scan Duration: Maximum scan duration per host minutes
If it exceeds the limit, the scan task on the host will be automatically terminated.

[More Settings](#)

4.5.4. Alarm Viewing

In the "Intrusion Detection - Detection List" interface, filter for alerts of types "Malicious Process

Initiation" "Malicious file writing to disk" or "Virus File," and view the virus-related alerts.

Detection List					
Time Range: Last 7 Days		Risk Level: Critical Risk, High Risk, Medium Risk			
<input type="text" value="Alarm Type: Malicious Process Initiation, Malicious file writing to disk, Virus file"/> Please manually enter the content you want to inquire after the colon and press Enter to finish.					
Risk Level	Please enter the query	Alarm Type	Affected Device Type	Status	Time Range
<input checked="" type="checkbox"/> Critical Risk <input checked="" type="checkbox"/> High Risk <input checked="" type="checkbox"/> Medium Risk <input type="checkbox"/> Low Risk	<input type="checkbox"/> Select All <input checked="" type="checkbox"/> Malicious Process Initiation <input checked="" type="checkbox"/> Malicious file writing to disk <input type="checkbox"/> Reverse Shell <input type="checkbox"/> Malicious Module Loading	Suspicious Process Parameters 1640 Custom Suspicious Processes 176 Web Backdoor 89 Malicious Process Initiation 28 Reverse Shell 28 Malicious file writing to disk 14	Host 2017 Container 101 Cluster 0	Pending Processing Confirmed Ignored	2004 Last 1 Hour 4 0 Last 1 Day 28 13 Last 7 Days 2017 0 Last 30 Days 2623 Custom...
Group by: <input type="checkbox"/> Cancel Confirm		Total 2004 alarms Select All		Last active Descending Mark All Manual Scan Export all	

4.5.4.1. Malicious Process Initiation

The alert details for unauthorized process startup include engine detection results, file paths corresponding to malicious processes, and process chains.

The screenshot shows the Sentry CWPP interface for a detected threat. The alert is categorized as 'High Risk' for 'Malicious Process Initiation'. The main message states: 'The malicious file detection engine has identified that the binary file associated with the process pingtunnel located at /tn [REDACTED] tunnel contains malicious instructions.' Below this, there are tabs for 'Container Response', 'Process Response', 'File Response', and a status of 'Pending'. A checkbox for 'Add to Whitelist' is checked. The 'Detection Information' section provides details like Detection Time (2025-02-22 13:13:53), ID (redacted), Response Result (-), Affected Devices (multiple devices shown as colored squares), Impact on Container (poc_a), Tactic & Technique (User Execution (T1204)), and Detection Method (Feature Engine). The 'Detection Explanation' section notes that the binary file has malicious features threatening server security. The 'Virus Database Details' table lists three engines: Jiangmin Antivirus Engine (Non-Malicious), 360 Antivirus Engine (Non-Malicious), and In-house Developed Antivirus Engine (HackTool.pingtunnel.a, Network Proxy Penetration Tool). An information icon is present in the table header.

Detection Library	Detection Result	Detection Explanation
Jiangmin Antivirus Engine	Non-Malicious	-
360 Antivirus Engine	Non-Malicious	-
In-house Developed Antivirus Engine	HackTool.pingtunnel.a	Network Proxy Penetration Tool

4.5.4.2. Malicious file writing to disk

The alert details for unauthorized file writes include engine detection results, the location where malicious files were written, the process that wrote the files, and process chains.

The screenshot shows the Sentry CWPP interface for a detected alert. The alert is categorized as **High Risk** with the message **Malicious file writing to disk**. The main text states: **The malicious file detection engine has detected that the process cp has written a malicious file to /var/lib/4a82fa2170adae0a5e59f3ace9a558fed06d4b2/m...**

The interface includes tabs for **Container Response**, **Process Response**, **File Response** (selected), and **Pending**. A button to **Add to Whitelist** is also present.

Detection Information section:

- Detection Time:** 2025-02-22 13:10:16 (0 times) - 2025-02-22 13:10:16
- ID:** [REDACTED]
- Response Result:** -
- Affected Devices...**: [REDACTED] (Icon)
- Impact on Container...**: poc_a (Icon)
- Tactic & Technique...**: User Execution (T1204) **Execute** All (2)
- Detection Method...**: Feature Engine
- Detection Explanation...**: The files written by the process have been found to contain malicious features, which may pose a threat to the security and stability of the server, and immediate action is required to address this.
- Rule ID:** [REDACTED] All (3)
- Process Name:** cp(66220)
- Write Command ...**: cp -f /us [REDACTED]
- Write File Path:** /var/lib/ct [REDACTED] 58fed06d4b2/merged/bin/ps
↓ [REDACTED] (Icon)
- Virus Database D...**: [REDACTED]

Detection Library table:

Detection Library	Detection Result	Detection Explanation
Jiangmin Antivirus Engine	Non-Malicious	-

4.5.4.3. Virus File

The alert details for infection files include the malicious files detected, engine detection results, and file paths corresponding to malicious files.

The screenshot shows a 'High Risk' alert for a 'Virus file'. The message states: 'The malicious file detection engine scanned and detected a virus Trojan.Generic.2C9606E6, corresponding file: c:\users\...ript.php'. Below this, there are tabs for 'File Response' (disabled), 'Add to Whitelist' (checked), and 'Pending' (radio button). A 'Detection Information' section provides details: Detection Time (2025-02-21 17:31:58), ID (redacted), Response Result (-), Affected Devices (Windows icon), Tactic & Technique (User Execution (T1204) - Execute, All (2)), Detection Method (Feature Engine), Detection Explanation (The malicious file detection engine uses multiple detection engines to scan files, hitting known features, suspected back doors or other malicious programs. This file may pose a threat to the security and stability of the server and immediate action is required to address it.), Rule ID (redacted), File Path (c:\users\52pojie\...), and Virus Database Details. The database table shows results from four engines: Jiangmin Antivirus Engine (Trojan.Generic.2C9606E6), 360 Antivirus Engine (Non-Malicious), In-house Developed Antivirus Engine (Non-Malicious), and Qingteng Cloud Detection Library (Non-Malicious).

Detection Library	Detection Result	Detection Explanation
Jiangmin Antivirus Engine	! Trojan.Generic.2C9606E6	-
360 Antivirus Engine	✓ Non-Malicious	-
In-house Developed Antivirus Engine	✓ Non-Malicious	-
Qingteng Cloud Detection Library	✓ Non-Malicious	-

4.5.5. Alarm Response

Virus-related alerts support both automatic and manual responses.

4.5.5.1. Automatic Response

Enter the "Security Response - Automatic Response" page. Once a specific type of alert ("Unauthorized File Write," "Unauthorized Process Startup," or "Infection File") is issued, the system will automatically handle it, eliminating the need for manual intervention.

For Malicious Files Writing to Disk Auto Response:

- Supported Device Types: Linux-Server, Linux-PC, Windows-Server, Windows-PC
- Supported Response Elements: File
- Alert Types: Choose "Unauthorized File Write"

- Supported Automatic Response Methods: Isolate the file

For **Malicious Process Initiation** Auto Response:

- Supported Device Types: Linux-Server, Linux-PC, Windows-Server, Windows-PC, Container
- Supported Response Elements: Process
- Alert Types: Choose "Unauthorized Process Startup"
- Supported Automatic Response Methods: Terminate the process

For **Virus File** Auto Response:

- Supported Device Types: Linux-Server, Linux-PC, Windows-Server, Windows-PC, Container
- Supported Response Elements: File
- Alert Types: Choose "Infection File"
- Supported Automatic Response Methods: Isolate the file

Create Auto-Response Policy

Basic Information

Status:

* Policy Na... : Please enter the policy name

Policy Desc...: Please enter a policy description

* Host Type: Please select a host type

* Applicatio...: All Day Custom Time Range (i)

Trigger Conditions

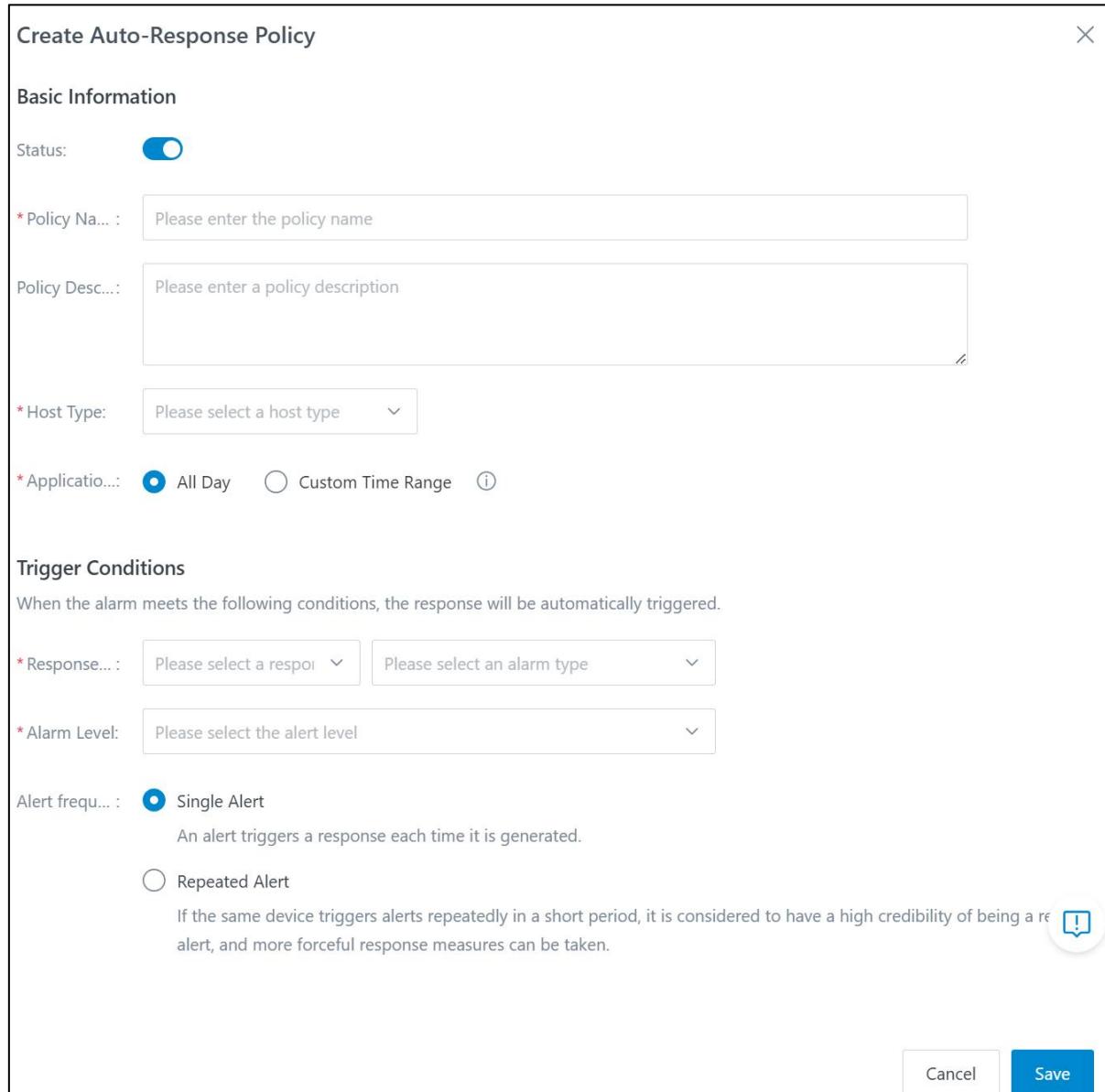
When the alarm meets the following conditions, the response will be automatically triggered.

* Response... : Please select a respoi v Please select an alarm type v

* Alarm Level: Please select the alert level v

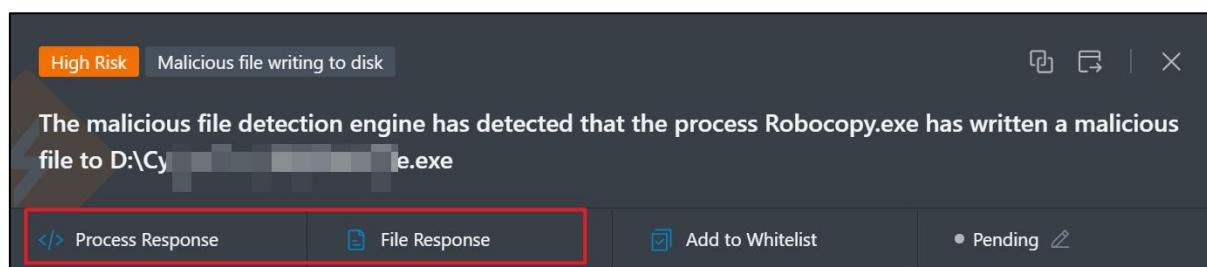
Alert frequ... : Single Alert
An alert triggers a response each time it is generated.
 Repeated Alert
If the same device triggers alerts repeatedly in a short period, it is considered to have a high credibility of being a re !

Cancel Save



4.5.5.2. Manual Response

In the alert details interface, you can manually respond to malicious processes or files.



4.5.5.3. Response Logs

Whether automatic or manual, each response is logged. Click "Response - Response List" to view

related response records.

- **Operation History:** Records each response, whether successful or failed.
- **Response List:** Records successfully responded elements. For example, isolated files can be unisolated or deleted under the "File" label.

The screenshot shows the 'Response List' interface with the 'File' tab selected. A tooltip provides information about file response types: Quarantined files, Recovered files, Repaired files, and Deleted files. Below the tooltip, a search bar and a table are displayed. The table has columns for Response Time, File Path, Affected Devices, Execution Account, Disposal Mechanism, Response Reason, and Operation. One row in the table is shown, corresponding to the tooltip's description of a deleted file.

Response Time	File Path	Affected Devices	Execution Account	Disposal Mechanism	Response Reason	Operation
2025-02-25 12:18:22	/home	[redacted]	admin	手动响应	shajinc	View Details Source Operation

4.5.5.4. False Positive

Handling If a false positive occurs, you can add it to the whitelist.

4.5.5.4.1. Add to Whitelist

In the alert details interface, click "Add to Whitelist," input related information such as SHA256 for the false positive file, and save it. The system will automatically remove the false positive alert from the alarm list, and no further virus alerts will be generated for this file in the future.

New Whitelist

Set Whitelist Conditions

Please set the whitelist conditions. The conditions are connected with 'AND,' which means that detection information can only apply the whitelist when it completely meets all the set whitelist conditions.

Condition	Matching Method	Value	Reset
Alert Type	Equals	Malicious Process Initiation	
Process File Path	Equals	/tmp/vi	
Process File SHA256	Equals	f4909816...7a63	

+ Add Condition

Application Scope

Please select the range of hosts to which the whitelist applies. Only containers within the range can apply the whitelist.

All Hosts

Select some hosts

Current Host

All Clusters

Select Container Cluster

Select container node image

4.5.5.4.2. Trust Zone

In the detection configuration interface, under "Virus File Searching And Killing," click "Trust Zone Settings" to set trust conditions based on file SHA256, file extensions, or directories. Files or directories that meet the trust conditions will be skipped during virus scanning.

The screenshot shows the 'Virus File Searching And Killing' section of the Sentry CWPP interface. It includes sections for 'Malicious File Write Detection', 'Protected Host Management', and 'Scan Period Configuration'. A 'Trust Zone' section is also present, with a 'Trust Zone Setting' button highlighted by a red box.

Malicious File Write Detection Users can customize the configuration for detecting malicious files, including type and size. Detection Settings	Protected Host Management Users can customize whether to enable virus file scanning on the host or container. This feature requires the installation of a local antivirus engine. Protected Host Management	Scan Period Configuration Users can customize the directories to be scanned and the scan frequency. The system will execute scans based on the settings and use multiple engines to detect whether the files are malicious. Scan Management View Scanned Records
Trust Zone Users can customize the trusted zone. When performing virus scanning, the trusted zone will be skipped and not scanned. Trust Zone Setting		

4.6. Honeypot

Honeypot refers to the proactive deployment of decoy hosts, network services, or information to lure attackers into attacking them. This allows defenders to capture and analyze attack behaviors, understand the tools and methods used by attackers, and infer their intentions and motives. It helps defenders clearly understand the security threats they face and enhances the security protection capabilities of actual systems through technical and management measures.

Honeypot involves monitoring specified ports on a host, establishing a whitelist through learning, and ultimately monitoring and recording various non-whitelisted access and connection behaviors.

Honeypot primarily addresses the following user issues:

1. Countering Hacker Intrusions: By setting up honeypots, users can confuse intruders, increase the difficulty of intrusion, and protect the security of real machines.
2. Real-time Monitoring of Suspicious Port Scanning: Records and analyzes the purpose and motives of hackers, enabling the system to promptly patch security vulnerabilities and prevent attacks.

Feature Advantages:

1. Comprehensive Security Protection: Deploys honeypots from a network perspective, providing

more comprehensive security protection for hosts.

2. Flexible Configuration: Users can flexibly choose the location of honeypot hosts and ports.

The Honeypot feature supports users in comprehensively managing honeypots and the alerts they generate, including:

- Honeypot Management
- Honeypot Alerts
- Alert Response

4.6.1. Feature Authorization

Only Agents with the "Host Honeypot" product purchased and authorized can use the Honeypot feature.

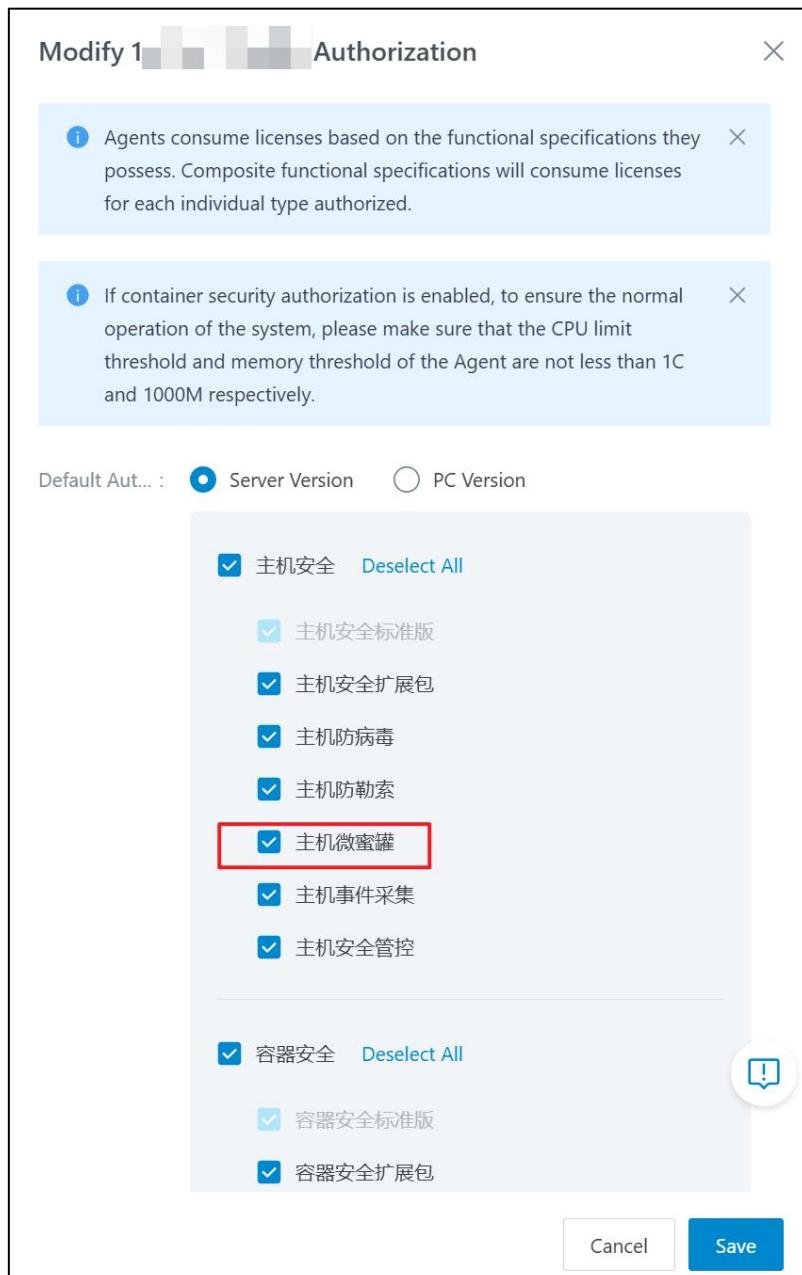
Method 1: Authorize During Agent Installation

Assign authorization during Agent installation. Navigate to the "Probes - Installation - Agent" interface, select the corresponding operating system, and authorize the feature.

The screenshot shows the "Agent" configuration interface for a Linux probe. On the left, there's a sidebar with icons for Linux, Windows, Kubernetes, and OpenShift. The "Linux" icon is selected. In the main area, there's a "Basic Configuration" section with a "Default Aut..." dropdown set to "Server Version". Below it, a note says: "To ensure the normal operation of the system when enabling container security authorization, please make sure that the CPU limit threshold and memory limit threshold of the Agent are not less than 1C and 1000M respectively." There are two radio button options: "Server Security" (selected) and "Select All". Under "Select All", several checkboxes are available: "Server Security" (checked), "Server Anti-Ransom...", "Server Honeypot" (highlighted with a red box), "Server Event Collecti...", "Host Security Assura...", and "Container Security".

Method 2: Modify Agent Authorization

After Agent installation, you can modify the authorization information and assign the "Host Honeypot" authorization. Navigate to the "Probes - Probes Management - License" interface, click "Configuration Authorization" , and modify the authorization as shown below:



4.6.2. Honeypot Management

Users can create honeypot models based on their needs, manage honeypot learning and usage, and

forward honeypot data to high-interaction honeypots.

4.6.2.1. Create Honeypot

Method 1: Navigate to the Honeypot page, click **Create Honeypot Model**, fill in the parameters, and click "Save" to successfully create a honeypot.

Create Honeypot Model

⚠ If there is an existing honeypot model on a host in the selected honeypot activation range, the honeypot ports in the newly created model will be merged with the historical ports. Other configurations, including detection scene, port forwarding address, learning mode, and recovery method, will be overwritten by new configurations. White lists, suspicious behaviors, and alarms generated during the previous learning process are still saved in the model.

*** Honeypot Activation Range**

Please select a host >

*** Port Listening Mode**

Occupy Mode ⓘ Monitoring Mode ⓘ

*** Detection Scene**

Full Connection ⓘ Half Connection ⓘ

*** Port Open**

Select Port Input Port

All data (70 items)

Please Enter Search Term

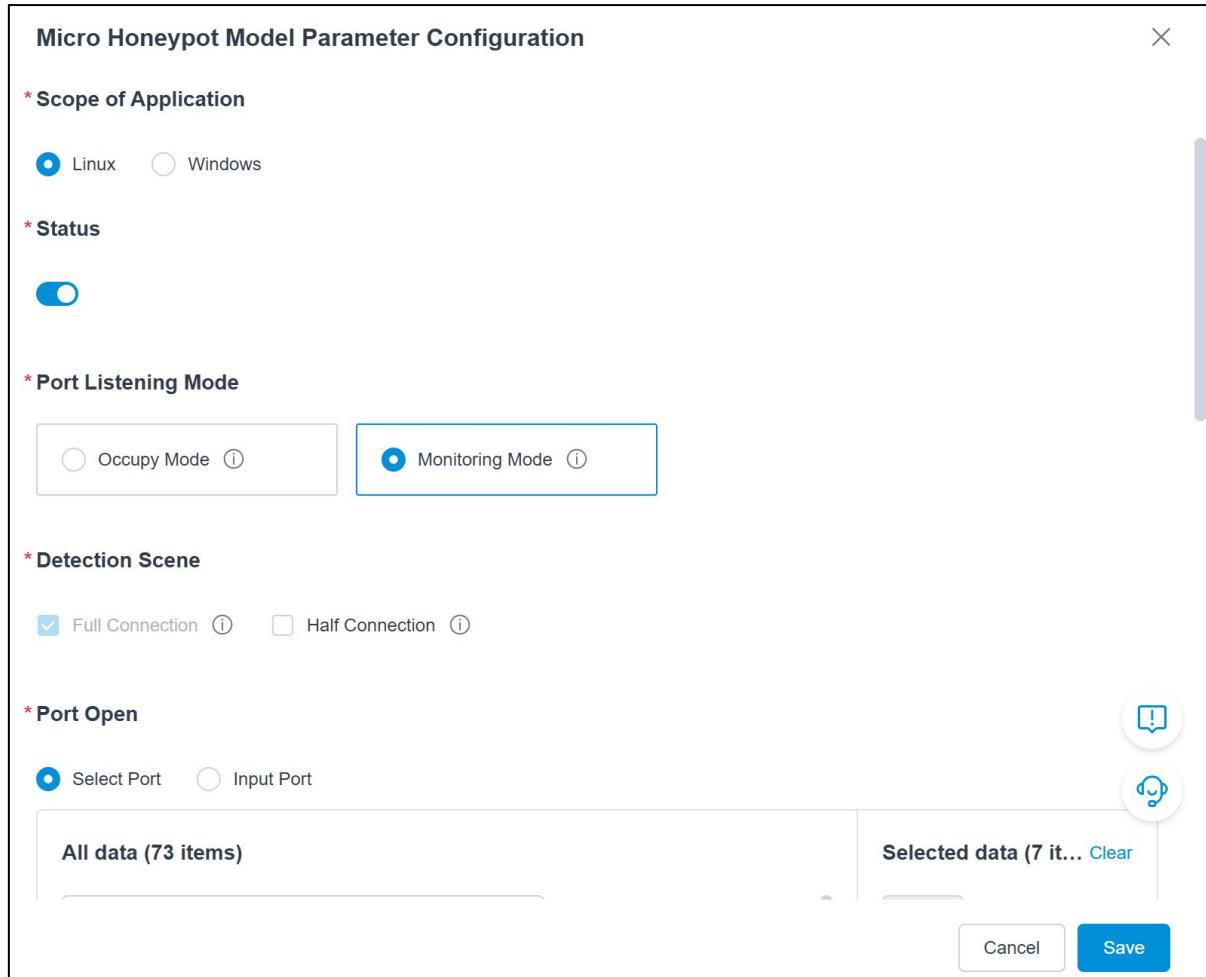
Common Ho... ▾ Service ▾ Possible Invasion Methods ▾

Selected data (0 ite... Clear

!

Cancel Save

Method 2: Go to the HoneyPot page, click **Model Parameter Settings**, fill in the parameters, and click Save. When the switch is turned on, a new host coming online can automatically generate a honeypot model based on the model parameters.



Note:

- Port Listening Mode: Determines whether the honeypot exclusively occupies the port.
 - Exclusive Mode: The honeypot exclusively occupies the monitored port, preventing other services from using it. This mode can monitor full or half connections.
 - Listening Mode: The monitored port can still be used for other services. This mode only monitors half connections.
- Detection Scenario: Specifies the type of connection that will trigger an alert.
 - Full Connection: Alerts are generated only after a three-way handshake is completed.
 - Half Connection: Alerts are generated even for port scans.
- Port Selection: Specifies the ports the honeypot will monitor.
 - The system provides common ports and their associated services and potential

- intrusion methods. Users can select from the list or directly input port numbers.
- If a port is already occupied, it will be automatically removed during honeypot creation.
 - Traffic Forwarding: Users can forward monitored traffic to a high-interaction honeypot by specifying the target IP and port. For details, refer to Traffic Forwarding.
 - Policy Learning Mode: Includes the honeypot's learning method and activation conditions. Typically, the model enters a learning phase to establish a whitelist before being activated for monitoring.
 - Smart Activation Mode: After saving, the honeypot enters the "learning" state. If no new connections are detected for three consecutive days, the model is automatically activated for monitoring.
 - Manual Activation Mode: After saving, the honeypot enters the "learning" state and can only be activated for monitoring manually.
 - Immediate Activation Mode: The honeypot skips learning and is immediately activated for monitoring. However, this may result in a high number of false positives due to the incomplete model.
 - The system defaults to "Smart Activation Mode," where the model is automatically activated if no new connections are detected for three consecutive days.
 - Honeypots in the "learning" state do not generate alerts. Connections during the learning phase are considered known tests and added to the whitelist.
 - Policy Recycling Mode: Users can set an alert frequency threshold. If the honeypot's alert frequency exceeds the threshold, it is deemed incomplete and recycled for further learning.
 - Manual Recycling: The honeypot can only be recycled manually.

- The system's default recycling condition is: 5 alerts within 1 hour.

4.6.2.2. Query Honeypot

Honeypot models created by users are displayed in the honeypot list. The list is divided into "monitoring" and "learning" sections, showing detailed information such as honeypot status, model ID, device name (host IP and host name), Business Group, honeypot ports, and conflicting ports.

Users can search for honeypots using the search box.

Intrusion Detection > Monitoring Configuration > Honeypot

Forwarding Address Configuration

Honeypot

Model Parameter Settings Create Honeypot Model

Monitoring Learning

Multiple filter tags are separated by the Enter key.

Status Model ID IP Host Name Operating System Business Group Honeypot Ports Conflict Ports Model Creation Time

ID	Device Name	Associate...	Honeypot Ports	Operation
				View Details Relearning More
				View Details Relearning More
				View Details Relearning More

View Details Relearning More

View Details Relearning More

View Details Relearning More

< 1 > 50 Item/Page

Note:

- Status: Indicates whether the honeypot is currently in the learning or monitoring state.
- Conflicting Ports: Ports specified for monitoring but already occupied by other services.

4.6.2.3. Honeypot Usage

After creation, honeypots can automatically learn and establish a whitelist. Once the whitelist is complete, the honeypot can be activated automatically or manually. If the connecting IP is in the whitelist, no alerts will be generated, reducing false positives and ensuring alerts are accurate and

meet user needs. Users can also disable or delete unnecessary honeypots.

4.6.2.3.1. Learning Honeypot

Honeypots created with the "Smart Activation" or "Manual Activation" learning modes will enter the "learning" state after being saved.

Learning Process:

- During learning, the honeypot does not generate alerts. All connection behaviors on the monitored ports are considered known tests, and the connecting IPs are added to the model whitelist.
- If "Smart Activation" is selected, the honeypot is automatically activated for monitoring if no new connections are detected for three consecutive days (starting from the creation time). If "Manual Activation" is selected, the user must manually activate the model; otherwise, it remains in the learning state.
- After activation, the honeypot traces the source IP of connection behaviors on the monitored ports and matches it against the model whitelist. If the IP is not in the whitelist, an alert is generated; if it is in the whitelist, no alert is generated.

If users need to activate a learning honeypot immediately, they can click "Enter Monitoring" under the "Operations" column to put the honeypot into actual use.

Status	Model ID	Device Name	Honeypot Ports	Conflict Ports	Operator	Operation
<input checked="" type="checkbox"/>	QT-M67b827eb25cc...	172.25.111.199 mock-agent-c502358...	22 21	-	admin	View Details Enter Monitoring More

4.6.2.3.2. Monitoring Honeypot

If you want a monitoring honeypot to relearn, click "Relearning" to restart the learning process.

The relearning policy follows the same standards set during honeypot creation. To modify the policy, click "More" under the "Operations" column, select "Edit" next to the basic information, and adjust the learning mode.

Honeypot

By enabling honeypot strategies on different devices and learning for a period of time, a port connection behavior model is established.

Monitoring Learning

Please Enter Search Term

2 items

Status	Model ID	Device Name	Associated ...	Honeypot Ports	Conflict Ports	Forwarding Target	Operation
<input checked="" type="checkbox"/>	[REDACTED]		◇ 0	22 21	-	-	View Details Relearning More
<input checked="" type="checkbox"/>	[REDACTED]		◇ 0	995 993 873 514 +16	-	-	View Details Relearning More

2 items

[Delete](#) [Relearn](#) [Clear Conflicts](#)

< 1 > 50 Item/Page

4.6.2.3.3. Clear Conflicting Ports

When other services on the host need to use ports monitored by the honeypot, a port conflict occurs.

For conflicting ports, select "More" under the "Operations" column in the honeypot list and click "Clear Conflict" to stop monitoring the conflicting ports.

Honeypot

By enabling honeypot strategies on different devices and learning for a period of time, a port connection behavior model is established.

Monitoring Learning

Please Enter Search Term

2 items

Status	Model ID	Device Name	Associated ...	Honeypot Ports	Conflict Ports	Forwarding Target	Operation
<input checked="" type="checkbox"/>	[REDACTED]		◇ 0	22 21	-	-	View Details Relearning More
<input checked="" type="checkbox"/>	[REDACTED]		◇ 0	995 993 873 514 +16	-	-	View Details Relearning More

2 items

[Delete](#) [Relearn](#) [Clear Conflicts](#)

< 1 > 50 Item/Page

4.6.2.4. Edit Honeypot Ports

When you need to edit the honeypot port, simply select the corresponding model to edit the

honeypot port.

The screenshot shows the Sentry CWPP interface for Monitoring Configuration > Honeypot. A red box highlights the 'Edit Honeypot Ports' button in the top right of the main panel. Below it, the 'Edit Honeypot Ports' dialog is open, showing a warning message: '⚠️ Batch edit honeypot ports for the selected models. Saving will overwrite the original ports. Please proceed with caution!' It includes a 'Port Open' section with a radio button for 'Select Port' (selected) and 'Input Port'. The 'All data (73 items)' table lists honeypot ports with columns for Common H..., Service, Possible Invasion Meth..., and Status (with a switch icon). The 'Selected data (0 it... Clear)' table is empty. At the bottom are 'Cancel' and 'Ok' buttons.

Note: Batch edit honeypot ports for the selected models. Saving will overwrite the original ports.

4.6.2.5. Disable Honeypot

When users temporarily do not need a honeypot, they can disable it. Once disabled, the honeypot will no longer record suspicious connections or automatically learn the whitelist.

In the honeypot list, find the honeypot to disable and toggle the switch under the "Status" column.

When the switch is , the model is disabled.

Honeypot

By enabling honeypot strategies on different devices and learning for a period of time, a port connection behavior model is established.

Monitoring **Learning**

Please Enter Search Term

2 items

<input type="checkbox"/>	Status	Model ID	Device Name	Associated ...	Honeypot Ports	Conflict Ports	Forwarding Target	Operation
<input checked="" type="checkbox"/>				◇ 0	22 21	-	-	View Details Relearning More
<input checked="" type="checkbox"/>				◇ 0	995 993 873 514 +16	-	-	View Details Relearning More

Delete **Relearn** **Clear Conflicts**

[View Details](#) [Relearning](#) [More](#)

4.6.2.6. Delete Honeypot

When a honeypot is no longer needed, users can directly delete it by selecting "Delete" under the "More" option in the "Operations" column of the honeypot list.

Deleting a honeypot removes all data except for historical alerts and events generated by the honeypot.

Honeypot

By enabling honeypot strategies on different devices and learning for a period of time, a port connection behavior model is established.

Monitoring **Learning**

Please Enter Search Term

2 items

<input type="checkbox"/>	Status	Model ID	Device Name	Associated ...	Honeypot Ports	Conflict Ports	Forwarding Target	Operation
<input checked="" type="checkbox"/>				◇ 0	22 21	-	-	View Details Relearning More
<input checked="" type="checkbox"/>				◇ 0	995 993 873 514 +16	-	-	View Details Relearning More

Delete **Relearn** **Clear Conflicts**

[View Details](#) [Relearning](#) [More](#)

[View Whitelist](#) [Delete](#)

4.6.2.7. Traffic Forwarding

When users need to forward access data received by honeypot ports to another high-interaction honeypot, they can configure traffic forwarding.

Click  **Forwarding Address Configuration**, enter the target IP and port, and click "Save." Access data captured by the honeypot after this setting will be forwarded to the specified address. Historical records before the setting will not be forwarded.

The screenshot shows a modal dialog titled "New Forwarding Address" with a close button (X) in the top right corner. It contains two input fields: "Target IP" and "Target Port", both with placeholder text "Please enter the target IP" and "Please enter the tar". Below these fields is a small trash can icon. At the bottom left is a blue "+ New Address" button.

4.6.3. Honeypot Alerts

When a honeypot detects non-whitelisted IP connections or scans on monitored ports, it promptly generates alerts. Users can view detailed alert information, aggregated event details, and handle alerts based on their needs.

4.6.3.1. Alert Information

Alerts generated by honeypots include detection information, attacker impact scope, and handling suggestions.

- Detection Information:
 - Displays the attacker's IP address and the attacked port.
 - Detection description includes the system's analysis of the connection behavior and attack trend predictions, helping users quickly understand the attack and respond.
- Attacker Impact Scope:
 - The system visually represents the attack path and ports through graphical data.
- Handling Suggestions: The system provides handling suggestions based on attack analysis, allowing users to take measures to prevent further losses.

Method 1: In the "Intrusion Detection - Detections," filter alerts by type "Cyber Honey Pot."

Method 2: Navigate to the honeypot details page, select "Related Alerts," to view alerts generated by the honeypot.

The system also supports exporting honeypot alert data in bulk or selectively.

Users can configure alert notifications based on their needs, such as setting alert types, notification methods, recipients, and notification levels based on severity.

4.6.4. Alarm Response

After the system reports an alert, users can respond based on the alert details. The system supports configuring automatic response strategies and manual responses.

4.6.4.1. Automatic Response

Navigate to the "Security Response - Automatic Response" page to create an automatic response strategy. When a honeypot alert occurs, the system will automatically handle it.

Users must first select the host type before setting trigger conditions.

- Supported Device Types for Honeypot Automatic Response: Linux-Server, Linux-PC, Windows-Server, Windows-PC.
- Supported Automatic Response Elements: Network.
- Supported Automatic Response Methods: Block Network.

Create Auto-Response Policy

Basic Information

Status:

* Policy Name:

Policy Description:

* Host Type:

* Application: All Day Custom Time Range

Trigger Conditions

When the alarm meets the following conditions, the response will be automatically triggered.

* Response: Please select an alarm type

* Alarm Level:

Alert frequency: Single Alert
An alert triggers a response each time it is generated.
 Repeated Alert
If the same device triggers alerts repeatedly in a short period, it is considered to have a high credibility of being a real alert, and more forceful response measures can be taken. 

Redeploy

4.6.4.2. Manual Response

In the alert details, users can manually handle alert information. For alerts reported by honeypots, users can perform network blocking, add to whitelist, or change the handling status.

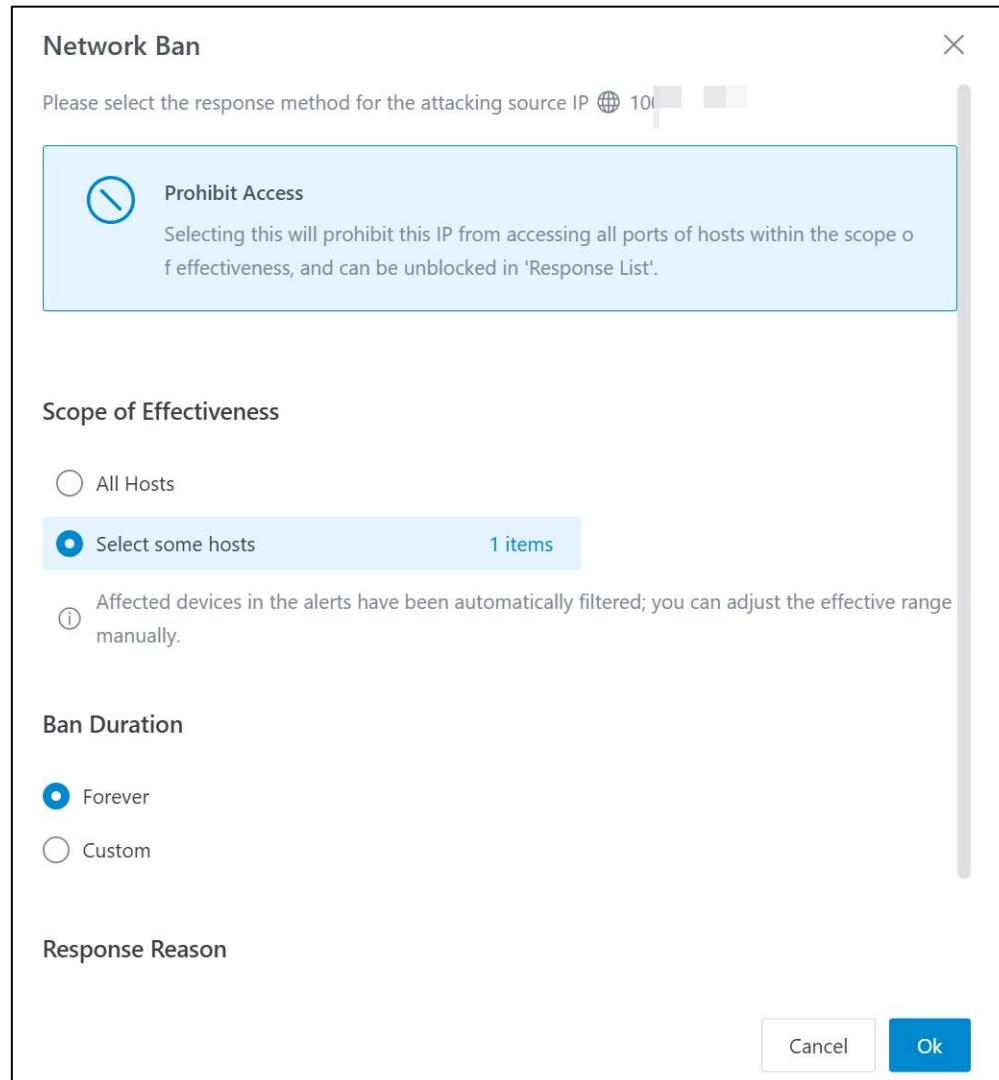
4.6.4.2.1. Network Ban

For alerts involving unknown dangerous IPs, users can block the IP to prevent further attacks.

Network blocking prevents the IP from accessing all ports on the affected hosts. Users can unblock the IP in the response list if needed.

Click "Network Ban" in the alert details.



**Note:**

- **Effective Scope:** By default, the blocking applies to the host where the alert occurred. Users can customize the scope.
- **Blocking Duration:** The system defaults to permanent blocking. Users can choose the duration, with options ranging from 1-59 minutes, 1-23 hours, or 1-30 days.

4.6.4.2.2. Add to Model Whitelist

If the source IP of a honeypot alert is deemed safe by the user, it can be added to the model whitelist.

This prevents alerts for the IP accessing the host and ports within the effective scope.

Method 1: Add from Alert

Click "Add to Model Whitelist" in the alert details.

New Whitelist

Set Whitelist Conditions

Please set the whitelist conditions. The conditions are connected with 'AND,' which means that detection information can only apply the whitelist when it completely meets all the set whitelist conditions.

Condition	Matching Method	Value	Reset
Target IP	In		
Login Source	In		

+ Add Condition

Application Scope

Please select the range of hosts to which the whitelist applies. Only containers within the range can apply the whitelist.

All Hosts

Select some hosts

Current Host

All Clusters

Select Container Cluster

Select container node image

Cancel Save

Method 2: Add from Model Whitelist

If users know in advance which information needs to be excluded, they can add it to the whitelist before false alerts occur.

In the honeypot list, click "More" under the "Operations" column, select "View Whitelist," and click "New."

Honeypot

By enabling honeypot strategies on different devices and learning for a period of time, a port connection behavior model is established.

Monitoring **Learning**

Please Enter Search Term

2 items

Status	Model ID	Device Name	Associated ...	Honeypot Ports	Conflict Ports	Forwarding Target	Operation
<input checked="" type="checkbox"/>	172.19.24...	Windows Server 2019	0	22, 21	-	-	View Details Relearning More
<input checked="" type="checkbox"/>	172.24.15...	Windows Server 2019	0	995, 993, 873, 514, +16	-	-	View Details Clear Conflicts View Whitelist

2 items

[Delete](#) [Relearn](#) [Clear Conflicts](#) [View Whitelist](#)

Model Whitelist (0) Related Alarms (0)

Please Enter Search Term

0 items

Whitelist Content	Last Modified Ti...	type	Operation
-------------------	---------------------	------	-----------

[Delete](#) [New](#)

Note:

- **Adding from Alert:** The whitelist conditions are automatically filled with the alert information.
- **Affected Alert Scope:** Specifies the time range of alerts affected by the whitelist.
 - If "Affect Alerts from the Past 30 Days" is selected, past alerts will be marked as whitelisted and removed from the alert list. Users can view them in the whitelist list. Future alerts will also be whitelisted and not displayed.
 - If "Only Affect Current and Future Alerts" is selected, only future alerts will be whitelisted and not displayed.

5. Ransom protection

A ransomware is a type of malware designed to force victims to pay a ransom to restore access by encrypting a user's files or system. Ransomware viruses typically spread to computer systems through email attachments, malicious links, or through vulnerabilities. Once infected, the virus encrypts the user's files (such as documents, photos, and databases) making them inaccessible, and the victim receives a notification, usually through a pop-up window or text file, demanding a ransom payment to unlock the file, the ransom is usually paid in cryptocurrencies such as Bitcoin, and the attacker may threaten to delete the file or leak sensitive information, increasing the pressure on the victim to pay the ransom.

There are many types of ransomware, such as lockscreen ransomware (which locks the user's computer screen and forces the user to pay to restore access), crypto ransomware (encrypts the user's files and the user must pay a ransom to decrypt them), etc. The pervasive ransomware protection system protects against encrypted ransomware viruses.

In the process of fighting ransomware, the common protection methods are mainly concentrated in "HIDS + antivirus + backup", although the ransomware protection methods are effective, but with the continuous evolution of ransomware attack methods, the traditional ransomware protection system does not play a good protection effect, enterprises and individuals need to combine modern technology and strategies, and adopt multi-level protection measures to enhance the overall security.

Through the analysis of more than 50 active ransomware families, Qingteng proposes a relatively complete ransomware solution:

- **Defend in advance**
 - Get a holistic view of your organization's assets and identify which assets are critical to

your business operations with asset inventory so you can prioritize protections to keep critical data and systems from threats.

- Through risk discovery, identify and assess possible threats and vulnerabilities, formulate response strategies in advance, remediate early, and reduce the entry point of attacks.
- Through intrusion detection, you can identify and detect ransomware pre-attack behaviors, including common ransomware APT teams' pre-new attack behaviors, and detect ransomware attack intentions as early as possible, such as brute-force attacks, phishing attacks, and fileless attacks.
- **In-process detection and blocking**
 - **Multi-virus detection engine:** By combining multiple virus engines, multi-level security protection can be achieved. Each engine has its own unique detection algorithms and technologies, which effectively cover different types of malware and attack vectors to provide more comprehensive protection.
 - **AI detection engine:** Traditional antivirus software generally detects malicious code based on signature codes, and the detection rate is limited. In order to solve the shortcomings of traditional pattern matching detection technology, the anti-ransomware system needs to introduce an artificial intelligence detection engine to identify unknown ransomware viruses.
 - **Intelligent decoy detection:** provides intelligent decoy technology, which dynamically delivers decoy files when the application traverses any directory, greatly increasing the exposure rate of decoy files, trapping ransomware viruses, making ransomware encrypt decoy files first, and improve the defense capability against ransomware

viruses.

- **Ransomware detection:** In some targeted extortion or APT attacks, the attack sample usually deletes the backup mechanism and shadow mechanism that exist in the system to prevent service recovery. In order to erase traces of an attack and avoid being traced to a hacker's identity, intrusion logs are often wiped after the attack is carried out. The anti-ransomware system needs to support ransomware behavior detection, and when typical ransomware behaviors are detected, it can immediately alarm and intercept ransomware behaviors to block ransomware behaviors.
- **File suffix detection:** Ransomware usually modifies the file extension to a specific format, and the Qingteng anti-ransomware system can detect ransomware viruses based on the file suffix, effectively identify known ransomware families, and carry out ransomware protection.
- **Automated response:** Automated response is a key safeguard against ransomware threats. The anti-ransomware system can take immediate action when a ransomware attack is detected, block the ransomware behavior, greatly shorten the response time, and effectively reduce data loss and business interruption.

- **Post-event traceability and recovery**

- Analyze reported alarms, obtain attack paths, clear hidden viruses or backdoors, and fix vulnerabilities.
- Restore backup data. If there is no backup or the backup data is invalid, Qingteng decryption scheme can be used to restore part of the encrypted files to reduce the company's losses, and at the same time, it is necessary to improve the backup mechanism.

This topic describes how to detect and block ransomware during an event.

5.1. Detection Configuration

Before you can use the ransomware protection feature, you must enable the driver at the same time, enable anti-ransomware authorization, and enable the ransomware protection feature.

Ransom Protection > Ransom Detection Configuration

Ransom Detection Configuration

To ensure the ransomware protection functions properly, please complete the following configuration:

- Enable global driver switch**
Global driver switch Enabled
[Go to settings](#)
- Activate ransomware protection authorization**
Ransomware protection authorization:2000
agent authorized:11, Not authorized:1989
[Go to settings](#)
- Enable the host driver switch**
Agent authorized for ransomware protection:11
Driver switch Enabled:3, Not enabled:8
[Go to settings](#)
- Enable ransomware protection**
Please check the 'Ransomware Protection' configuration on this page to enable detection or blocking for the specified host.

Linux-Server Windows-Server Linux-PC **Windows-PC**

System Default Configuration

	Include	Application Scope	Update Time	Edit
	1 Item Configuration	100.64.0.228 6	2025-06-30 18:14:59	

User Defined Configuration

Custom detection configurations primarily address scenarios where specific devices need individual detection items. The host scope of custom configurations cannot be duplicated, meaning each device can only have one detection configuration applied (if there is a conflict between host and group configurations, the host configuration takes priority). When a new host is onboarded, if no matching custom configuration is found, the system's default configuration will be applied.

Please Enter Search Term Delete Create Configuration

5.1.1. Enable the tenant driver master switch

Click "Ransom Detection Configuration - Enable global driver switch - Go to Settings" to turn on the driver status button, and you can enable the drivers of all agents under the account.

Agent management > Running Monitor > Agent > Configuration

Configuration

Monitor and alert on frequent Agent disconnections for Server-type hosts

Every 1 Days Alarm once, report close to 2 Offline for more than days

When the A depends on Enabling it attempts to

3 Times of the Agent

Agent self defense

After enabling protection, exiting the Agent program and uninstalling the terminal require validation of the protection password. This feature depends on the driver, so please ensure the driver is enabled.

*Type of protective equipment: Server version PC version

[View Self-Protection Interception Records](#)

*Protection password: Please enter the protection password

Function switch configuration

Driver Status

After turning on this switch, you can see the detection capability instructions related to the driver. Enabling the Agent driver enables the functions that depend on the driver to run normally. Driver operation will cause a certain burden on performance. Please be cautious when turning it on

Users can also go to "Tenant Management - Agent -Agent Runtime" and click on Create Management Task, select the task type as [Enable Driver], and specify the task scope, so as to enable the driver switch for the specified tenant.

Create Management Task

Task Type: Enable Driver

Task Name: Agent_Enable Driver_20250704153526

Push Rate: 100 hosts/min

Execution: Once (radio button selected), Daily, Weekly, Expression

Duration: 0 Minutes

Execution Scope:

- All Tenants (radio button selected)
- Customize Tenant: Please select
- Select hosts by tenant

5.1.2. Turn on the host driver switch

Click "Ransom Detection Configuration - Enable the host driver switch - Go to Settings". Go to Agent

- Agent Details and click Operation and Maintenance - Enable Driver

The screenshot shows the 'Agent Details' page with the status 'Offline'. A dropdown menu titled 'Operation and Maintenance' is open, listing several options: 'Restart', 'Uninstall', 'Upgrade', 'Configure Connect Address', and 'Enable Driver'. The 'Enable Driver' option is highlighted with a red rectangle.

5.1.3. Activate ransomware protection authorization

The agent can be protected against ransomware only if you have purchased the Host

Anti-Ransomware or Endpoint Anti-Ransomware product and assigned the Host Anti-Ransomware
or Endpoint Anti-Ransomware authorization to the agent.

Method 1: Grant permissions when the agent is installed

Permissions are assigned when the agent is installed. Go to "Agent

Management-Installation-Agent" and select the [Endpoint Ransomware Protection](#) and [Host Ransomware Protection](#).

Agent management > Installation > Agent > Virtual Machine Template Installation

Server Agent-Linux-Virtual Machine Template Installation

Basic Configuration

Business G...: Default Business Group

If you need to add a business group, please click [Business Group Management](#)

Connection...: Default connection address

To add a connection address, click [Connection Address Configuration](#)

Functional Configuration

Installation ...:

① To ensure the normal operation of the system when enabling container security authorization, please make sure that the CPU limit threshold and memory limit threshold of the Agent are not less than 1C and 1000M respectively.

Host Security		4 item(s) selected
<input type="checkbox"/> Select All	<input checked="" type="checkbox"/> Host Security Posture	<input checked="" type="checkbox"/> Host Intrusion Detection and Response
<input checked="" type="checkbox"/> Host Ransomware Protection	<input type="checkbox"/> Host Micro Honeypot	<input type="checkbox"/> Host Event Collection
		<input checked="" type="checkbox"/> Host Security Assurance

> Container Security 0 item(s) selected

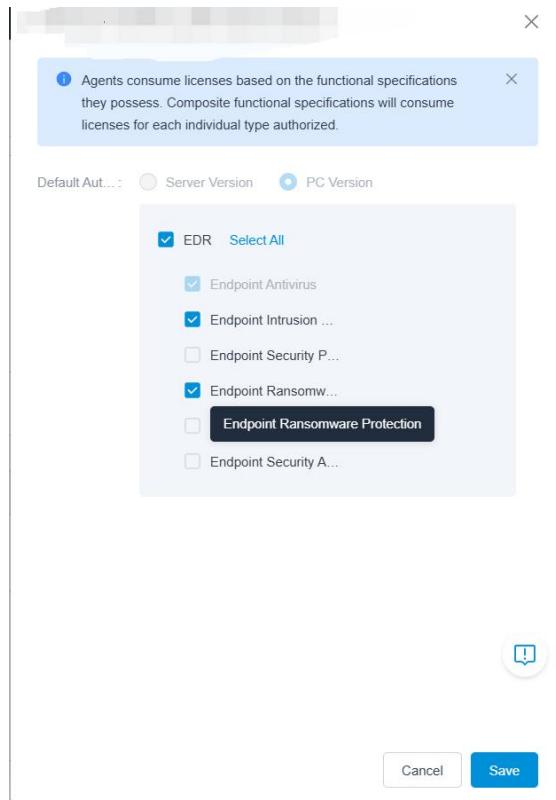
Method 2: Modify the agent authorization

After the agent is installed, you can also modify the authorization information, click "Ransom

Detection Configuration - Activate ransomware protection authorization - Go to Settings", enter the

"Agent Management - Running Monitor - License" Configuration page, and click [Configure

Authorization] to modify the authorization, as shown in the following figure:



5.1.4. Enable ransomware protection

On the detection configuration page, ransomware protection is not enabled in the default configuration.

- Newly installed hosts: If you want ransomware protection to be enabled on the newly installed hosts, modify the default detection configuration and enable ransomware protection.
- Enable ransomware protection only for specific hosts: If ransomware protection is still disabled in the default detection configuration, you can create a custom detection configuration and enable ransomware protection in the custom detection configuration.

We recommend that you turn on all switches in Ransomware Protection.

- Ransomware Bait protection, suspicious ransom behavior detection, and file extension detection: If this parameter is not enabled, the ransomware detection capability is affected.

Suspicious ransomware detection, which is only available on Windows devices, can detect typical ransomware behaviors such as ransomware viruses and deletion of volume shadows.

- Feature and AI Engine Detection: Qingteng integrates multiple virus engines and AI detection engines, which are enabled by default and cannot be disabled.
- Behavior Learning Model: monitors file behaviors (file read, file creation, file write, file rename, file deletion), processes that are not in the whitelist, and when prohibited operations are performed on the monitoring directory, alarms will be reported.
- Protection Directory: Automatically identifies and protects important directories.
- Whitelist: In the event of a false positive, users can whitelist files or processes.
- Automatic Response: If automatic response is not enabled, although the ransomware detection capability still exists, after the ransomware behavior is discovered, it cannot be stopped in time, resulting in all files still being encrypted or the shadow of the volume being deleted, making ransomware protection lose its core meaning.

Ransom Protection > Ransom Detection Configuration > Configuration Details

Linux-Server System Default Configuration

The screenshot shows the 'Ransom Protection' configuration page with the following sections:

- Ransomware Protection:** A summary section indicating a total of 9 devices unauthorized for ransomware protection. It includes links to 'Go to Configuration' and 'Driver Management'.
- Ransomware Bait Protection:** Enabled. Description: For devices with installed drivers, intelligently deploy bait files and monitor process operations on bait files to effectively identify ransomware.
- Feature and AI Engine Detection:** Opened. Description: Detection based on virus sample characteristics can accurately kill known ransomware; the AI engine can automatically complete deep analysis and feature extraction of samples to protect against unknown ransomware. It is recommended to install a local engine to timely scan and kill ransomware.
- File Extension Detection:** Disabled. Description: For devices with installed drivers, monitor file creation and renaming behaviors. If the file extension matches a known ransomware family-specific extension, it is suspected to be a ransomware attack. It includes a 'Driver Management' link.
- Behavior Learning Model:** Monitor file behavior (file read, file creation, file write, file rename, file delete). If a process not on the whitelist performs a prohibited action in the monitored directory, an alert will be triggered. Includes 'Behavior Learning Settings' and 'Model List' links.
- Protection Directory:** Automatically identify and protect critical directories (e.g., database directories), with support for custom directories. Includes a 'Protection Directory Configuration' link.
- Whitelist:** Users can customize the whitelist to avoid false positives. Includes a 'Configure detection whitelist' link.
- Automatic Response:** Not Enabled. Description: Automatically respond when ransomware is detected. Includes an 'Auto Response Setting' link.

5.1.5. Install the local engine

Although you can protect against ransomware without installing a local virus engine, we recommend that you install a local virus engine and ensure that it can be updated to the latest version in a timely manner.

Go to “Agent management - Integration Management - Anti-Virus Engines”, find the host you want to install, and click Install.

Agent management > Integration Management > Anti-Virus Engines

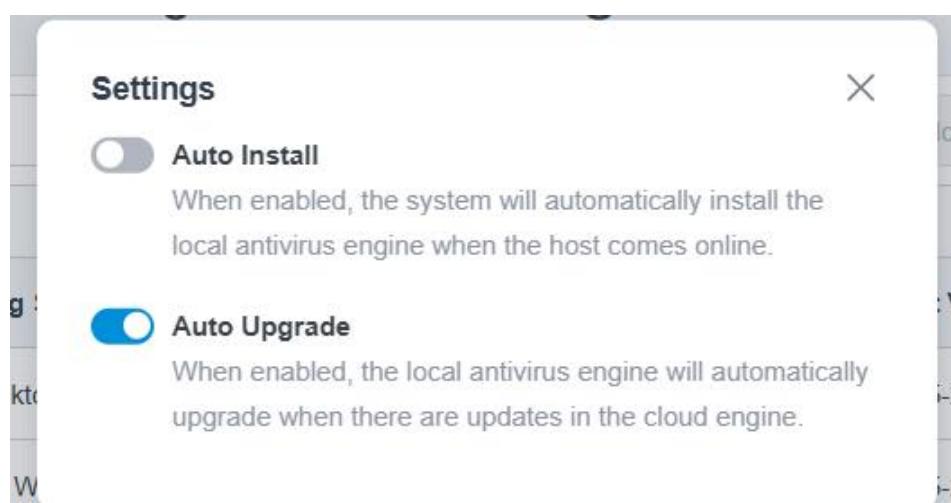
Anti-Virus Engines

The screenshot shows a table with the following data:

Total Hosts	Not Installed	Pending Upgrade	Latest Version	Installing	Upgrading
33	25	0	8	0	0

Below the table is a search bar labeled "Enter search term" and a toolbar with buttons for "More", "Upgrade", "Uninstall", "Settings", and "View Latest Virus Database Version". The main area displays a list of 33 items with columns: Host, Operating System, Host Type, Current Virus Database Version, Virus Definition Status, and Operation (with "Install", "Upgrade", and "Uninstall" buttons). Most hosts have the "latest version" checked, except for one which has a red exclamation mark.

Click Settings to turn on the automatic update switch to ensure that the local virus engine is updated to the latest version in a timely manner.



5.2. Alarm viewing

In Ransom Protection - Ransom Detection, you can view the detected ransomware alerts, including six types of alerts: Ransom Bait Capture | The ransom file suffix | Extortion of specific behaviors | Extortion Behavior Model | Ransomware known viruses | The ransom process starts.

Ransom Protection > Ransom Detection

Ransom Detection

Total 4 alarms		Select All	
<input type="checkbox"/>	Risk Level	<input type="checkbox"/> High Risk	Host IP
<input type="checkbox"/>	Description	<input type="checkbox"/>	Host Name
<input type="checkbox"/>	Alarm Type	<input type="checkbox"/>	Business Group
<input type="checkbox"/>	Platform Types		Last active Descending
<input type="checkbox"/>	Risk Level	<input type="checkbox"/> High Risk	<input type="checkbox"/> Select All
<input type="checkbox"/>	ID	<input type="checkbox"/>	Mark All
<input type="checkbox"/>	Rule ID	<input type="checkbox"/>	Export all
<input type="checkbox"/>	Annotation		
<input type="checkbox"/>	Detection Time	<input type="checkbox"/> 2025-07-02 14:57:47	Alarm Type
<input type="checkbox"/>		<input type="checkbox"/> 2025-07-02 14:57:47	Description
<input type="checkbox"/>			Affected Devices
<input type="checkbox"/>			Status
<input type="checkbox"/>	Risk Level	<input type="checkbox"/> High Risk	<input type="checkbox"/> Pending
<input type="checkbox"/>	ID	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Rule ID	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Annotation	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Detection Time	<input type="checkbox"/> 2025-07-02 14:12:05	Alarm Type
<input type="checkbox"/>		<input type="checkbox"/> 2025-07-02 14:54:40	Description
<input type="checkbox"/>			Affected Devices
<input type="checkbox"/>			Status
<input type="checkbox"/>	Risk Level	<input type="checkbox"/> High Risk	<input type="checkbox"/> Pending
<input type="checkbox"/>	ID	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Rule ID	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Annotation	<input type="checkbox"/>	<input type="checkbox"/>

Steps:

- Filter alarm data based on alarm type, risk level, alarm status, alarm time, and other conditions.
- Click View Alarm Details to view the details of the alarm.
 - Different ransomware alerts are displayed to facilitate users' research and judgment.
- Alarm markers:
 - Single mark: Click the drop-down list in Alarm Status to mark the alarm data as processing, confirmed, or ignored based on the actual analysis situation
 - Batch mark:
 - Select the list data and click "Batch Mark" to mark all the selected data in a

unified state. For alarms that have been marked as acknowledged, ignored, or in process, the alarm status will be overwritten after all alarms are marked.

- After filtering the list data, click "Mark All" to mark all the filtered results in a unified state. For alarms that have been marked as acknowledged, ignored, or in process, the alarm status will be overwritten after all alarms are marked.
- Data export: You can select and export lists in batches or export selected data.

In the Intrusion Detection - Alarm List, you can filter the alarms of ransomware-related alarm types or view ransomware alarms.

The screenshot shows the 'Intrusion Detection > Intrusion Detection > Detections' section. At the top, there are filters for 'Time Range: Last 7 Days', 'Risk Level: Critical Risk, High Risk, Medium Risk', and a search bar containing 'Alarm Type: Ransom bait capture, Ransom file extension, Ransom-specific behavior, Ransom behavior model, Ransomware known virus, Ransom process starts'. Below the search bar is a note: 'Please manually enter the content you want to inquire after the colon and press Enter to finish.' A red box highlights this search bar area. The main table has columns: Risk Level, Alarm Type, Affected Device Type, Status, and Time Range. The table shows 4 alarms under 'Ransomware known virus' for 'Host' devices, all in 'Pending' status. The 'Time Range' dropdown shows options like 'Today', 'Last 1 Hour', 'Last 1 Day', 'Last 7 Days', 'Last 30 Days', and 'Custom ...'. At the bottom, there are group by options ('All', 'Host', 'Container', 'Cluster'), a total count of 'Total 4 alarms', and buttons for 'Select All', 'Last active Descending', 'Mark All', 'Manual Scan', and 'Export'.

Risk Level	Alarm Type	Affected Device Type	Status	Time Range
Critical Risk	Ransomware known virus	Host	Pending	Today
High Risk	Web Backdoor	Container	Processing	Last 1 Hour
Medium Risk	Suspicious Process Parameters	Cluster	Confirmed	Last 1 Day
Low Risk	Memory-Resident Malware		Ignored	Last 7 Days
	Local Privilege Escalation			Last 30 Days
	Reverse Shell			Custom ...

5.3. Ransom Whitelist

When a false positive occurs, it can be whitened

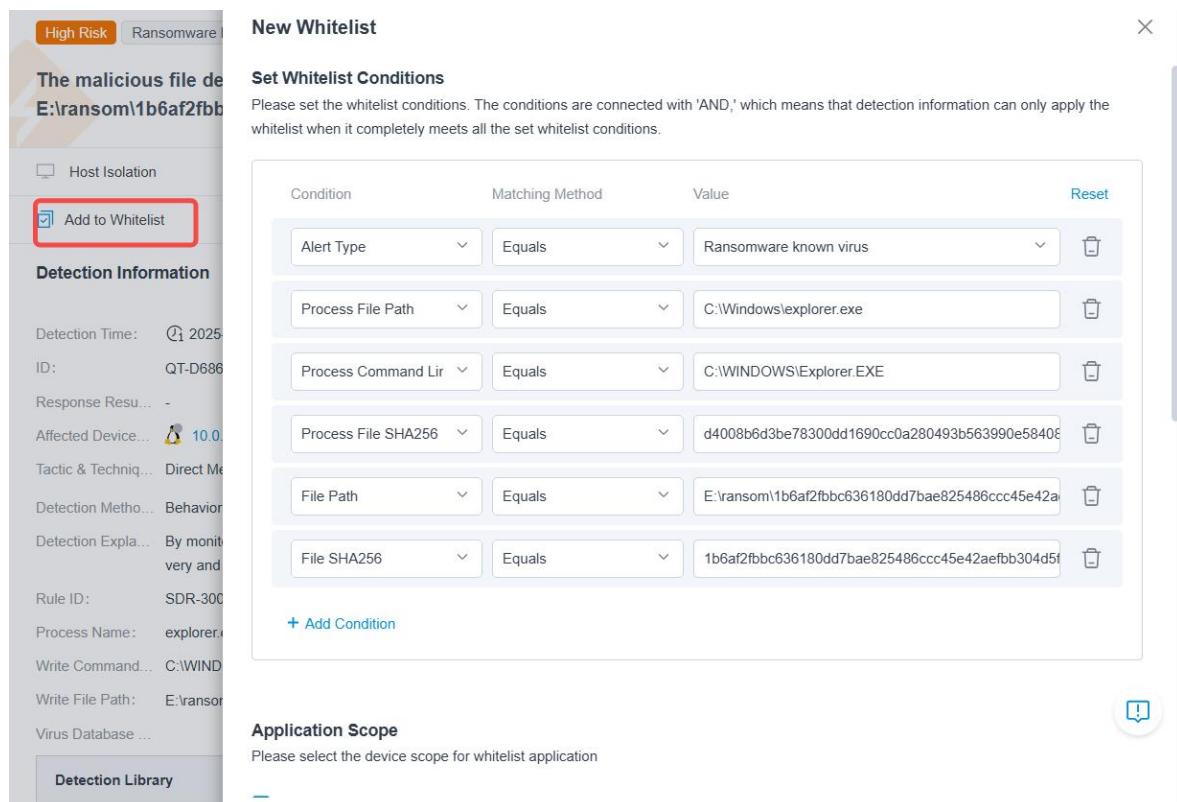
Steps:

- **Whitening conditions:** You can whiten the file according to conditions such as file SHA256/path or incoming file path/command line.

- Application scope:** You can select the device scope of the whitelist application, including hosts and containers.
- Scope of affected alarms:** You can select whether to affect the alarm records of the last 30 days. If you select Alarm that affects the last 30 days, the past alarm will be marked as whitened and removed from the alarm list.

5.3.1. Alarm whitening

In the Intrusion Detection or Ransom Protection alarm list, click Ransomware Alarm Details and click Add to Whitelist. The user can edit the whitening conditions, application scope, and affected alarm range. After saving, false alarms are automatically removed from the alarm list, and ransomware alarms are not generated for this process in the future.



The screenshot shows the 'New Whitelist' dialog box. At the top left, there are two buttons: 'High Risk' (orange) and 'Ransomware' (grey). Below these are sections for 'The malicious file de...' and 'E:\ransom\1b6af2fb...', 'Detection Information' (including Detection Time: 2025, ID: QT-D686, Response Result: -, Affected Device: 10.0, Tactic & Technique: Direct Me..., Detection Method: Behavior, Detection Explanation: By monitor..., Rule ID: SDR-300, Process Name: explorer.exe, Write Command Path: C:\WIND..., Write File Path: E:\ransom..., Virus Database: ...), and 'Detection Library'. A red box highlights the 'Add to Whitelist' button under 'Detection Information'. The main area is titled 'Set Whitelist Conditions' with the instruction: 'Please set the whitelist conditions. The conditions are connected with 'AND,' which means that detection information can only apply the whitelist when it completely meets all the set whitelist conditions.' It contains a table with columns 'Condition', 'Matching Method', and 'Value'. The table rows are:

Condition	Matching Method	Value	Reset
Alert Type	Equals	Ransomware known virus	
Process File Path	Equals	C:\Windows\explorer.exe	
Process Command Lin	Equals	C:\WINDOWS\Explorer.EXE	
Process File SHA256	Equals	d4008b6d3be78300dd1690cc0a280493b563990e5840e	
File Path	Equals	E:\ransom\1b6af2fb...6180dd7bae825486ccc45e42a...	
File SHA256	Equals	1b6af2fb...6180dd7bae825486ccc45e42aefbb304d5...	

At the bottom left is a blue '+ Add Condition' button. On the right side of the dialog box is a blue circular icon with a white exclamation mark.

5.3.2. Manual whitening

- On the Ransom Protection - Ransom Whitelist page, click [New] and select the whitelisting

conditions, application scope, and impact alarm scope.

New Whitelist

Set Whitelist Conditions

Please set the whitelist conditions. The conditions are connected with 'AND,' which means that detection information can only apply the whitelist when it completely meets all the set whitelist conditions.

Condition	Matching Method	Value	Reset
Process Command Line	Equals	Please fill in the condition value.	
Process File MD5	Equals	Please fill in the condition value.	
File MD5	Equals	Please fill in the condition value	

[+ Add Condition](#)

Application Scope

Please select the device scope for whitelist application

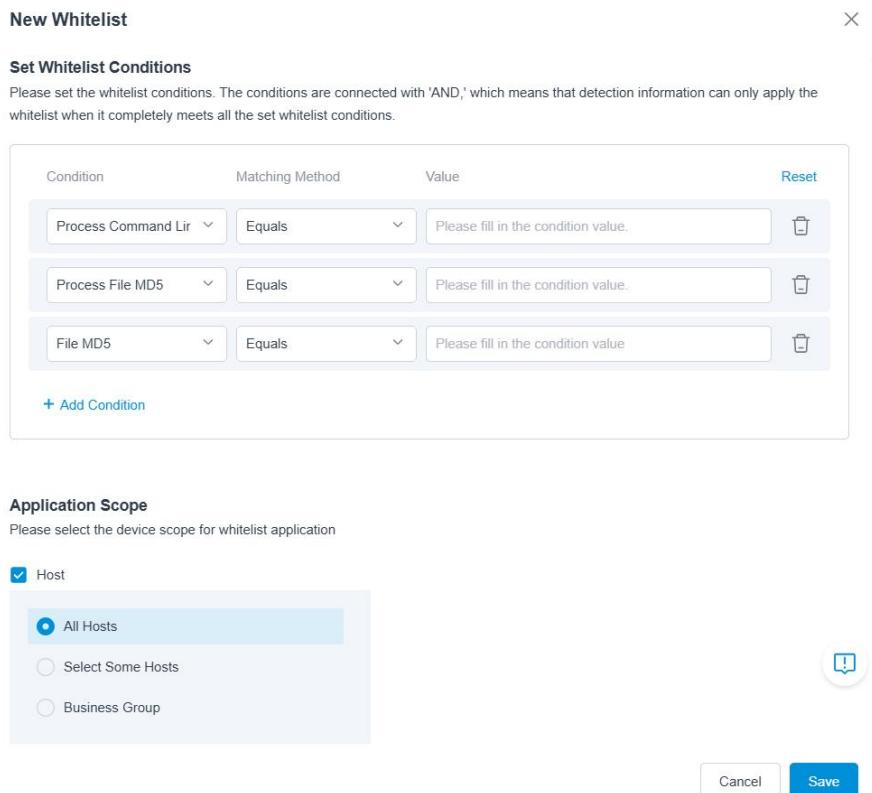
Host

All Hosts

Select Some Hosts

Business Group

[Cancel](#) [Save](#)



2. Enter the "Ransom Protection-Ransom Detection Configuration-Whitelist-Configure detection whitelist" page, click [New], and only select all sha256, path/directory and cmdline for whitelisting conditions, after saving, the system will automatically synchronize the detection whitelist to the Agent, and no ransomware alarm will be generated for this process in the future.

Create New Detection Whitelist

Set Whitelisting Conditions

Please set whitelist conditions and enter the type and corresponding value for the process file to be whitelisted.

sha256 Path/Directory cmdline

1 Please enter the full sha256 of the process file. Multiple values should be separated by newlines.

Value Type Path/Directory cmdline

1 items

All Hosts

Select Some Hosts

Business Group

Scope of affected alarms

Cancel Save

5.3.3. Whitelist List

The saved whitelist can be viewed in the whitelist list, and can be edited and deleted later.

Ransom Protection > Ransom Whitelist

Ransom Whitelist

Driver Detection Whitelist

The creation, modification, and deletion of whitelist rules are all asynchronous operations. It may take a long time for large data volumes. Please manually refresh the page after a while to get the latest data.

Please Enter Search Term

2 items

Whitelist Condition	Application Scope	Affected R...	Note	Update Time	Operation
[Redacted]	Container All Containers	0	-	2025-07-04 10:41:16	Edit Delete
[Redacted]	Host All Hosts	0	-	2025-07-03 15:42:37	Edit Delete

2 items

1 50 Item/Page

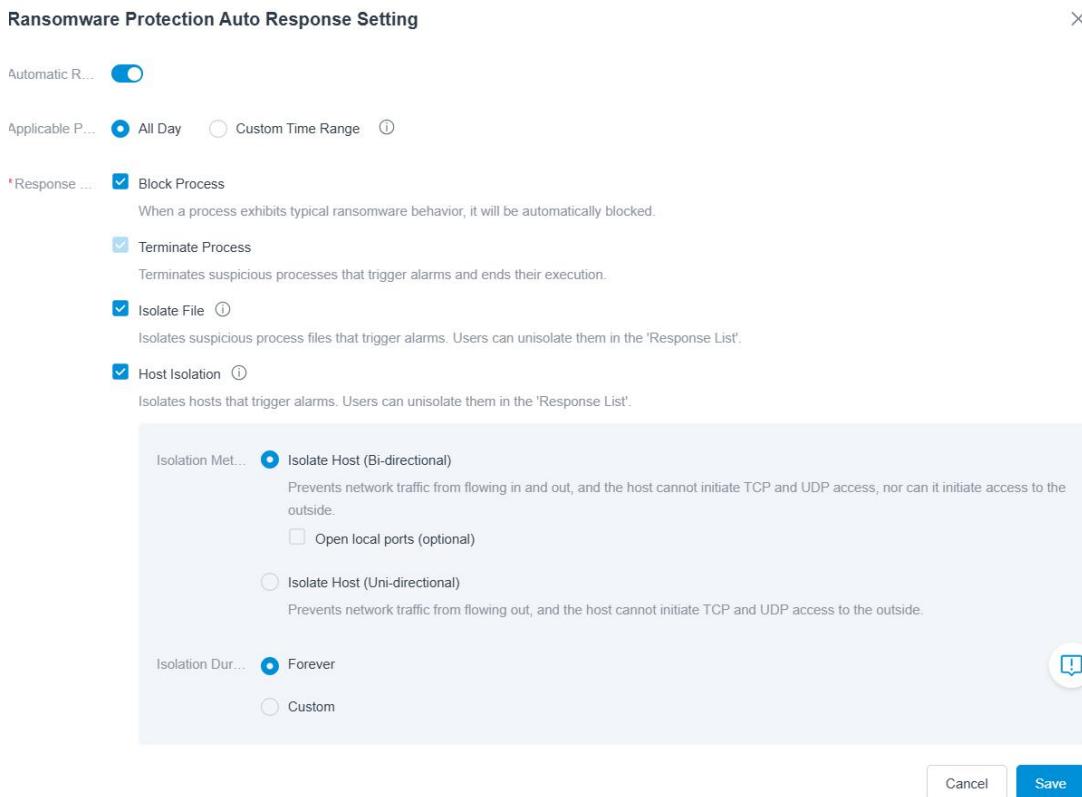
5.4. Alarm Response

5.4.1. Automatic Response

If automatic response is not enabled, although the ransomware detection capability still exists, after

the ransomware behavior is discovered, it cannot be prevented in time, resulting in all files still being encrypted or the volume shadow being deleted, making the core meaning of ransomware protection lost. For this reason, it is strongly recommended that you enable automatic responses in Ransomware Protection.

Steps: On the Ransom Detection Configuration page, open the detection configuration of Ransomware Protection, click **Auto Response Setting**, and set the required response method.



5.4.2. Manual response

On the Alarm Details page, you can manually respond to ransomware alarms by process response, file response, and host isolation

The screenshot shows a ransomware detection summary. At the top, there's a 'High Risk' status and a 'Ransomware known virus' alert. Below this is a blurred preview of the affected file. A navigation bar at the bottom includes 'Host Isolation' (which is highlighted with a red border), 'Process Response', 'File Response', and 'Pending'. There's also a 'Add to Whitelist' checkbox. A section titled 'Detection Information' is partially visible.

5.4.3. Response Logs

Whether it is an automatic response or a manual response, each response will be logged, and you can click "Ransomware Protection - Response List" to view the relevant response records

- Operation History: Record every response, whether successful or unsuccessful.
- Response List: Records the elements that were successfully responded, and can restore some of the responding elements. For example, quarantined files can be released from quarantine under the "Files" tab, or deleted completely.

The screenshot shows the 'Response List' page. At the top, there are tabs for 'Process', 'File', and 'Host Isolate', with 'Process' selected. A note says 'The process response list is used to display processes that have been terminated and automatically blocked.' Below is a search bar and a table with the following data:

Response Time	Process Name	Affected Devices	Disposal Mechanism	Response Met...	Operation
2025-05-09 16:53:35	bash(14680)	nginx	Automatic Respon...	Terminate Process	View Details Source
2025-05-09 14:54:59	bash(23083)	nginx	Automatic Respon...	Terminate Process	View Details Source
2025-05-09 14:52:51	bash(22103)	nginx	Automatic Respon...	Terminate Process	View Details Source
2025-05-09 14:52:15	bash(21759)	nginx	Automatic Respon...	Terminate Process	View Details Source

At the bottom, there are pagination controls and a '50 Item/Page' dropdown.

6. Risk discovery

As attackers' methods continue to change, the state of network security is becoming increasingly severe with the increase of security vulnerabilities. Traditional vulnerability scanners only perform periodic scans on a quarterly or annual basis, and new vulnerabilities can easily be exploited and invaded by hackers during the undetected period. Therefore, enterprises need to be able to achieve continuous risk monitoring and analysis products, which can transform passivity into proactivity, deeply discover internal exposed problems and risks, and continuously and effectively deal with risks, thereby increasing the attack threshold and reducing the repair window period. Risk discovery is committed to helping users accurately identify internal risks, assisting security teams in quickly locating issues and effectively resolving security risks, and providing detailed asset and risk information for analysis and response.

6.1. Risk Analysis

The risk analysis summarizes the latest risk results, providing users with a comprehensive perspective to view potential security risks. Users can flexibly select different objects and view the specific risk types corresponding to these objects.

6.1.1. Host risk

6.1.1.1. loophole

1、Page Display

The system supports vulnerability detection of applications running on the host. You can click on the highlighted "Detection Item Management" to view the details of the detection items.

- If you think certain detection items do not need to be detected, you can click  to close them.

General search: The system has set up a universal search box that supports unified retrieval of vulnerability information and asset information.

Quick screening: The system lists key risk screening items and values such as risk level, risk characteristics, asset category, etc., making it convenient for users to easily trigger result screening with one click.

List display: Analyzing vulnerabilities, you can choose different analysis perspectives, including all, aggregated by vulnerabilities, and aggregated by assets.

- All: Display all vulnerability data for all asset objects.
- Aggregation by vulnerability: Statistics are conducted from the vulnerability dimension, displaying relevant information about all vulnerabilities and the affected assets on the vulnerabilities.
- Aggregate by asset: Conduct statistics from the asset dimension to display the distribution of vulnerabilities on host objects.

steps:

- If you need to initiate vulnerability detection for host risks, you can choose full detection or targeted detection based on actual testing requirements:
 - To perform a full-volume scan, simply click the "Detection All" button.
 - To retest partial vulnerabilities from existing risk analysis results, switch the analysis perspective to the "Group by Vulnerability" view, select the target range of data, and then click the "Detection" button.
 - To retest partial hosts from existing risk analysis results, switch the analysis

perspective to the "Group by Host" view, select the target range of data, and then click the "Detection" button.

- To retest specific data from existing risk analysis results, click the "Detection" button in the operation bar corresponding to the relevant list data.
- When the host scope of the business under the user's data rights changes (e.g., adding or removing hosts), click the "Update Statistics" button to recalculate and recompile the results. A successful update will log the update time; in the event of a failure, a warning icon  will appear—hover your cursor over it to view the cause of the failure.
- For each vulnerability, you can see the corresponding affected assets. Click the highlighted host IP value, and the corresponding details page will pop up.
- Click the "View Details" button, and the detailed information of the vulnerability will pop up. You can view the description of the vulnerability, repair suggestions, and other information from it.
- If you think a certain vulnerability has little risk and does not affect system security, you can click the "Add to Whitelist" button individually or in batches to whitelist the vulnerability, so that these vulnerabilities will be ignored during the next scan.
- Click the "Whitelist Management" button, and you can enter the whitelist management page to view the whitelist, cancel whitelisting, and perform operations related to creating new whitelist rules.
- Click the "Execution Records" button, and you can view the detection history records and execution status of host risks - vulnerabilities within the past 180 days.
- The system supports exporting all vulnerabilities or selecting to export some of them.

The screenshot shows the Sentry CWPP interface. The left sidebar includes links for Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery, More (General, Tools, Messages), and a user account for admin. The main content area is titled 'Risk Discovery > Analysis > Host Risk' under 'Host Risk'. It features tabs for Vulnerability, Patch, and Weak Password. A 'Vulnerability List' table is displayed with columns: Severity (Critical, High, Medium, Low), Risk Features (hasRemoteExec, hasKernel, hasLocalPerm, hasExp, hasPoc), Asset Category (Linux, Windows), Detection Method (VersionComparison, Poc, Condition), and First discovery time (Within the last 1 day, Within the last 7 days, Within the last 30 days). Below the table are buttons for 'Add to whitelist', 'Update Statistics', and 'Detection All'. A detailed table below shows specific vulnerability entries with columns: ID, Severity, Vulnerability Name, Risk Features, Affected Assets, Business G..., First discovery ti., Operation. Two entries are shown: QTV-2024... (High, Linux kernel privilege...) and QTV-2024... (High, Apache HTTP Server ...).

Note:

- Switching the analysis perspective to vulnerability aggregation or asset aggregation, you can directly click on the small triangle icon in front of a single data or click on a single data to display the corresponding information of the vulnerability.
- The other operational procedures are the same as above.

2、Whitelist Management

steps:

- If you want to view the whitelist of host vulnerabilities, cancel whitelisting, or create new whitelist rules, you need to click the "Whitelist Management" button to enter the whitelist management page.
- The Precise Whitelist displays the result list of precisely whitelisting specific risk items. If you want to cancel whitelisting, you can directly click the "Cancel Whitelisting" button.
- If you need to create a whitelist rule for batch whitelisting based on conditions, you can enter the Fuzzy Whitelist Rule page.
 - Click "New Rule", and fill in relevant parameters, including conditions for different risk

characteristics, scope of application hosts, effective scope, rule description, and other information.

- For newly created whitelist rules, you can edit and delete them.
- After creation, you can click the highlighted number in the affected records to view the risk data specifically affected by the rule.

The screenshot shows the Sentry CWPP web interface. The top navigation bar includes links for Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery (which is selected), Compliance, and More. On the far right, there are links for General, Tools, 999 Messages, and a user account labeled 'admin'. The main content area has a left sidebar with categories like Analysis, Host Risk, Container Risk, Node Image Risk, Cluster Risk, Remediation History, Detection, and Library Query. The 'Analysis' section is expanded, showing 'Host Risk' as the active tab. Below this, under 'Host Risk', is a 'White List' section. Within 'White List', there are tabs for 'Vulnerability' (which is selected), Patch, and Weak Password. A sub-section titled 'Precise Whitelist' contains a note: 'This list shows the results of directly selecting specific risk items for precise whitelisting. To create whitelist rules for batch whitelisting based on conditions, please go to Fuzzy Whitelist Rules'. Below this is a search bar with placeholder text 'Please select filter content' and a 'Cancel Whitelisting' button. A table lists one item: 'QTV-2022-000004' (High risk, Linux polkit Local Privilege Escalation Vulnerability) associated with 'Affected Assets' (IP address 10.106.128.128) and 'Whitelist Time' (2025-08-01 17:38:38). The table has columns for ID, Risk, Affected Assets, Whitelist Time, and Operation. At the bottom of the table are buttons for 'Cancel Whitelisting' and '50 Item/Page'.

3、Detection Logic

The system supports vulnerability detection on hosts from different dimensions. You can click "Detection All" or check the data and then click "Detection" to directly initiate the detection.

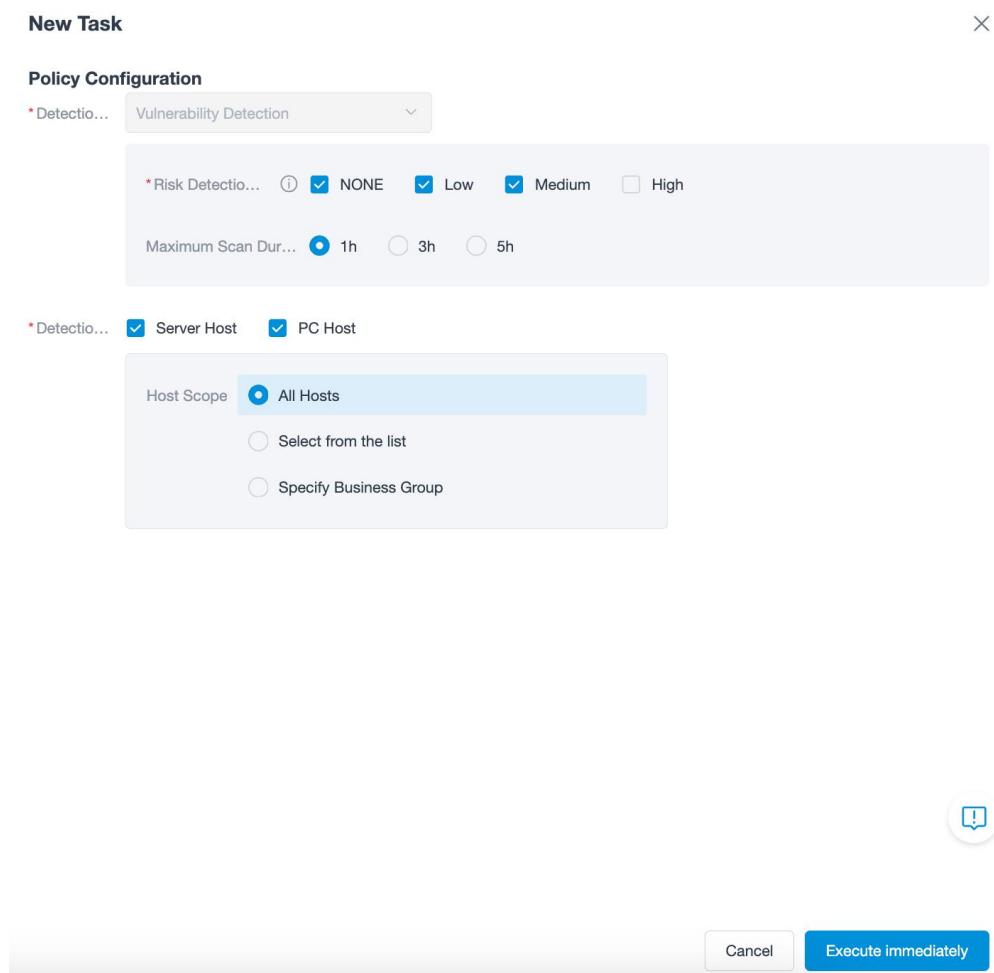
- (1) Detection All: By default, a full scan is initiated using the template policy "Vulnerability Scan".

You can select the host scanning scope, and the default setting covers all hosts.

steps:

- Click the "Detection All" button, and a page for creating a new task will pop up.
- The detection policy is, by default, the template policy - Vulnerability Detection.
- By default, Risk Detection Settings are set to NONE, Low and Medium , and High is not detected by default. You can check or uncheck the detection risks according to your detection needs. It should be specially noted that the detection risk here refers to the potential impact that may occur when using POC scripts for detection. Therefore, the detection risk settings selected here will affect the detection items included when executing the task.

- The Maximum scan Duration is 1 hour by default. If the detection task is not completed within the set duration, a timeout will occur. You can select the maximum scanning duration according to the estimated time.
- The Detection Scope covers all hosts of Server and PC by default. You can make a selection according to the host scope you need to detect.
- After confirming that the above information has been filled in completely, click "Execute Immediately" to issue the vulnerability detection for the hosts.



(2) Detection: Used to initiate targeted retests.

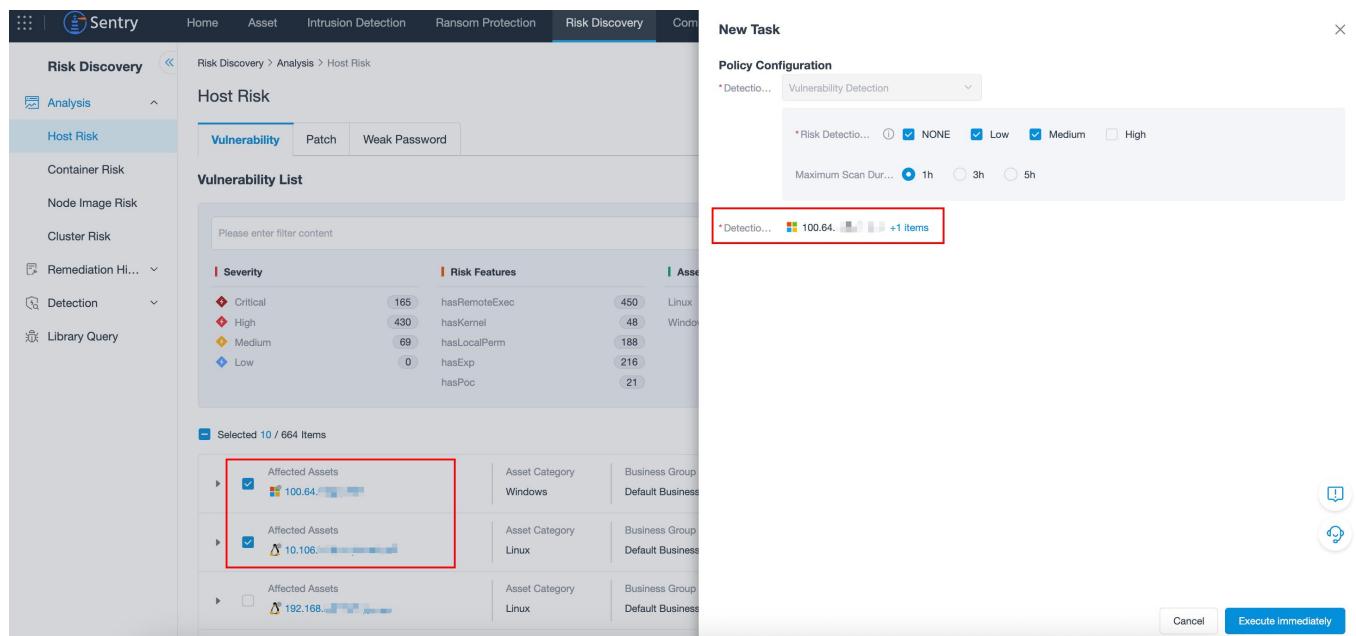
Scenario 1: Initiate a retest for specific hosts in existing risk analysis results

steps:

- Switch the analysis perspective to the "Group by Host" view, check the data and click the

"Detection" button, and a page for creating a new task will pop up.

- The detection policy is, by default, the template policy - Vulnerability Detection.
- By default, Risk Detection Settings are set to NONE, Low and Medium , and High is not detected by default. You can check or uncheck the detection risks according to your detection needs. It should be specially noted that the detection risk here refers to the potential impact that may occur when using POC scripts for detection. Therefore, the detection risk settings selected here will affect the detection items included when executing the task.
- The Maximum scan Duration is 1 hour by default. If the detection task is not completed within the set duration, a timeout will occur. You can select the maximum scanning duration according to the estimated time.
- The detection scope is the host information you have checked and cannot be modified.
- After confirming that the above information has been filled in completely, click "Execute Immediately" to issue the vulnerability detection for the hosts.



Scenario 2: Initiate a retest for specific vulnerabilities in existing risk analysis results

steps:

- Switch the analysis perspective to the "Group by Vulnerability" view, or in Detection Items, check the data and click the "Detection" button, and a page for creating a new task will pop up.
- The scope of detection items is the checked vulnerabilities. If there is a high - risk detection risk for a detection item, a prompt will appear: There is a high risk in the vulnerability detection items. Please confirm whether to initiate the detection! If you think some detection items do not need to be detected, you can remove them individually or in batches.
- The Maximum scan Duration is 1 hour by default. If the detection task is not completed within the set duration, a timeout will occur. You can select the maximum scanning duration according to the estimated time.
- The Detection Scope covers all hosts of Server and PC by default. You can make a selection according to the host scope you need to detect.
- After confirming that the above information has been filled in completely, click "Execute Immediately" to issue the vulnerability detection for the hosts.

The screenshot shows the Sentry CWPP interface with the 'Risk Discovery' tab selected. On the left, a sidebar menu includes 'Analysis', 'Host Risk', 'Container Risk', 'Node Image Risk', 'Cluster Risk', 'Remediation History', 'Detection', and 'Library Query'. The main area displays 'Host Risk' analysis, specifically the 'Vulnerability' tab under 'Analysis'. A 'Vulnerability List' table shows various vulnerabilities with columns for ID, Severity (Critical, High, Medium, Low), Risk Features (e.g., hasRemoteExec, hasKernel, hasLocalPerm, hasExp, hasPoc), and Assets (Linux, Windows). Below this is a table showing 'Selected 8 / 664 Items' with columns for ID, Severity, Vulnerability Name, and Description. Two specific items are highlighted with red boxes: 'XStream Security Vulnerability (CVE-2021-21350)' (Severity: Critical) and 'Spring Framework path traversal vulnerability (CVE-2024-028...)' (Severity: High). A 'New Task' dialog box is overlaid on the screen. It contains a 'Testing Items' section with a table showing the selected items and their details. It also includes fields for 'Maximum Scan Duration' (set to 1h), 'Detection Scope' (selected 'Server Host'), and 'Host Scope' (selected 'All Hosts'). At the bottom right of the dialog are 'Cancel' and 'Execute Immediately' buttons.

Scenario 3: Initiate a retest for specific data in existing risk analysis results

steps:

- Click the "Detection" button in the operation bar corresponding to the relevant list data; a new task page will pop up.
- The detection items will be automatically populated with the vulnerability detection items corresponding to the data, and the detection scope will be automatically populated with the host information corresponding to the data.
- The default maximum scan duration is 1 hour. If the detection task is not completed within the set duration, a timeout will occur. You can select the maximum scan duration based on your estimated time.
- After confirming and filling in the above information, click "Execute Immediately" to initiate the vulnerability detection for the host.

The screenshot shows the Sentry CWPP Risk Discovery interface. On the left, there's a sidebar with navigation links: Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery (which is selected), More, General, Tools, Messages (with 99+ notifications), and a user account for admin. The main area is titled 'Host Risk' under 'Risk Discovery > Analysis > Host Risk'. It has tabs for 'Vulnerability' (selected), Patch, and Weak Password. Below is a 'Vulnerability List' table with columns: Severity, Risk Features, Asset Category, Detection Method, and First discovery time. The table shows data for Critical, High, Medium, and Low severity vulnerabilities across Linux and Windows assets. At the bottom, there are buttons for 'Add to whitelist', 'Update Statistics', 'Detection All', and a table toolbar. The 'Operation' column in the table has a red box around it, and a red arrow points from the text 'A red arrow points to the "Detection" button in the table header of the vulnerability list.' to the 'Detection' button in the table header.

ID	Severity	Vulnerability Name	Risk Features	Affected Assets	Business G...	First discovery ti...	Operation
QTV-2024...	High	Linux kernel privilege...	hasExp has... +1	192.168.1.100	Default Busin...	2025-12-05 10:41:00	Detection View Details Add
QTV-2024...	High	Apache HTTP Server ...	hasRemoteExec	192.168.1.100	Default Busin...	2025-12-05 10:41:00	Detection View Details Add

New Task

X

Testing Items

1 items			
Detection Item Name	Vulnerability Type	Detection Method	Risk Detection
Linux kernel privilege esca...	Permission and Acces...	VersionComparison	NONE

Maximum Sca... 1h 3h 5h**Detection Scope***Detection Sc...  192.168.1.100

Cancel

Execute immediately

Instructions:

- After a detection task is initiated, it will be added to the queue by trigger time to wait for detection. Each queue allows a maximum of 10 pending tasks. If there are more than 10 pending tasks in the queue when a user creates a new task, task creation will be blocked, and a prompt will appear: "Too many pending tasks in the queue. Please try again later."
- Once detection is completed, click the "Execution Records" button to view historical execution records from the past 180 days. The page will redirect to Risk Discovery > Detection > Execution Records, and the detection type will be automatically populated as "Host Risk_Vulnerability".

Task Trigger ...	Task Name	Task Type	Policy	Detection Object	Detection T...	Task start time	Operation
2025-12-10 19:04:00	2	Custom	Vulnerability d...	Server	Host Risk_Vul...	2025-12-10 19:04:00	End Task View Failed Item
2025-12-10 18:56:00	Vulnerability d...	System Presen...	Vulnerability d...	Server	Host Risk_Vul...	2025-12-10 19:15:43	End Task View Failed Item
2025-12-10 18:48:00	Vulnerability d...	System Presen...	Vulnerability d...	Server	Host Risk_Vul...	2025-12-10 18:48:00	End Task View Failed Item
2025-12-10 18:40:00	1	Custom	Vulnerability d...	Server	Host Risk_Vul...	2025-12-10 19:07:52	End Task View Failed Item
2025-12-10 18:32:00	1	Custom	Vulnerability d...	Server	Host Risk_Vul...	2025-12-10 18:32:00	End Task View Failed Item
2025-12-10 18:24:00	2	Custom	Vulnerability d...	Server	Host Risk_Vul...	2025-12-10 18:55:31	End Task View Failed Item

6.1.1.2. patch

1、Page Display

A patch is a file containing repair code or data that provides a solution for fixing related vulnerabilities. By installing patches, you can prevent potential security threats and ensure that the system can operate normally.

List display: Analyze patches, you can choose different analysis perspectives, including all, aggregate by patch, and aggregate by asset.

- All: Display all patch data for all asset objects.
- Aggregation by patch: Conduct statistics from the patch dimension, displaying relevant information of all patches and the status of affected assets on the patches.
- Aggregate by asset: Conduct statistics from the asset dimension to display the distribution of patches on host objects.
- The other operational procedures are the same as above.

steps:

- If you need to initiate patch detection for host risks, you can choose full detection or targeted

detection based on actual testing requirements:

- To perform full-volume detection, simply click the "Detection All" button.
- To retest specific hosts from existing risk analysis results, switch the analysis perspective to the "Group by Host" view, select the target range of data, and then click the "Detection" button.
- When the host scope of the business group under the user's data rights changes (e.g., adding or removing hosts), click the "Update Statistics" button to recalculate and recompile the results. Each successful update will log the update time; if the update fails, a warning icon will be displayed—hover your cursor over it to view the failure reason.
- For each patch, you can see the corresponding affected assets. Click the highlighted host IP value, and the corresponding details page will pop up.
- Click the "View Details" button, and the detailed information of the patch will pop up. You can view the description of the patch, verification information, and other details from it.
- If you think a certain patch has little risk and does not affect system security, you can click the "Add to Whitelist" button individually or in batches to whitelist the patch, so that these patches will be ignored during the next scan.
- Click the "Whitelist Management" button, and you can enter the whitelist management page to view the whitelist, cancel whitelisting, and perform operations related to creating new whitelist rules.
- Click the "Execution Records" button, and you can view the detection history records and execution status of host risks - patches within the past 180 days.
- The system supports exporting all patches or selecting to export some of them.

Severity	Risk Features	Asset Category	Business Impact	First discovery time
Critical	hasRemoteExec	Linux	Unspecified	Within the last 1 day
High	hasKernel	Windows	Yes	Within the last 7 days
Medium	hasLocalPerm		No	Within the last 30 days
Low	hasExp			
	hasPoc			

ID	Severity	Patch...	Risk Features	Affected Assets	Business G...	Business...	First discover	Operation
a24f18ff-6...	Critical	2024-11 ...	hasKernel	100.64	Default Busin...	Unspecified	2025-12-16	View Details Add to whi...
00b3356d...	Critical	2024-08 ...	hasKernel	100.64	Default Busin...	Unspecified	2025-12-16	View Details Add to whi...

2、Whitelist Management

steps:

- If you want to view the whitelist of host patches, cancel whitelisting, or create new whitelist rules, you need to click the "Whitelist Management" button to enter the whitelist management page.
- The Precise Whitelist displays the result list of precisely whitelisting specific risk items. If you want to cancel whitelisting, you can directly click the "Cancel Whitelisting" button.
- If you need to create a whitelist rule for batch whitelisting based on conditions, you can enter the Fuzzy Whitelist Rule page.
 - Click "New Rule", and fill in relevant parameters, including conditions for different risk characteristics, scope of application hosts, effective scope, rule description, and other information.
 - For newly created whitelist rules, you can edit and delete them.
 - After creation, you can click the highlighted number in the affected records to view the risk data specifically affected by the rule.

3、Detection Logic

The system supports patch detection on hosts from different dimensions. You can click "Detection All" or check the data and then click "Detection" to directly initiate the detection.

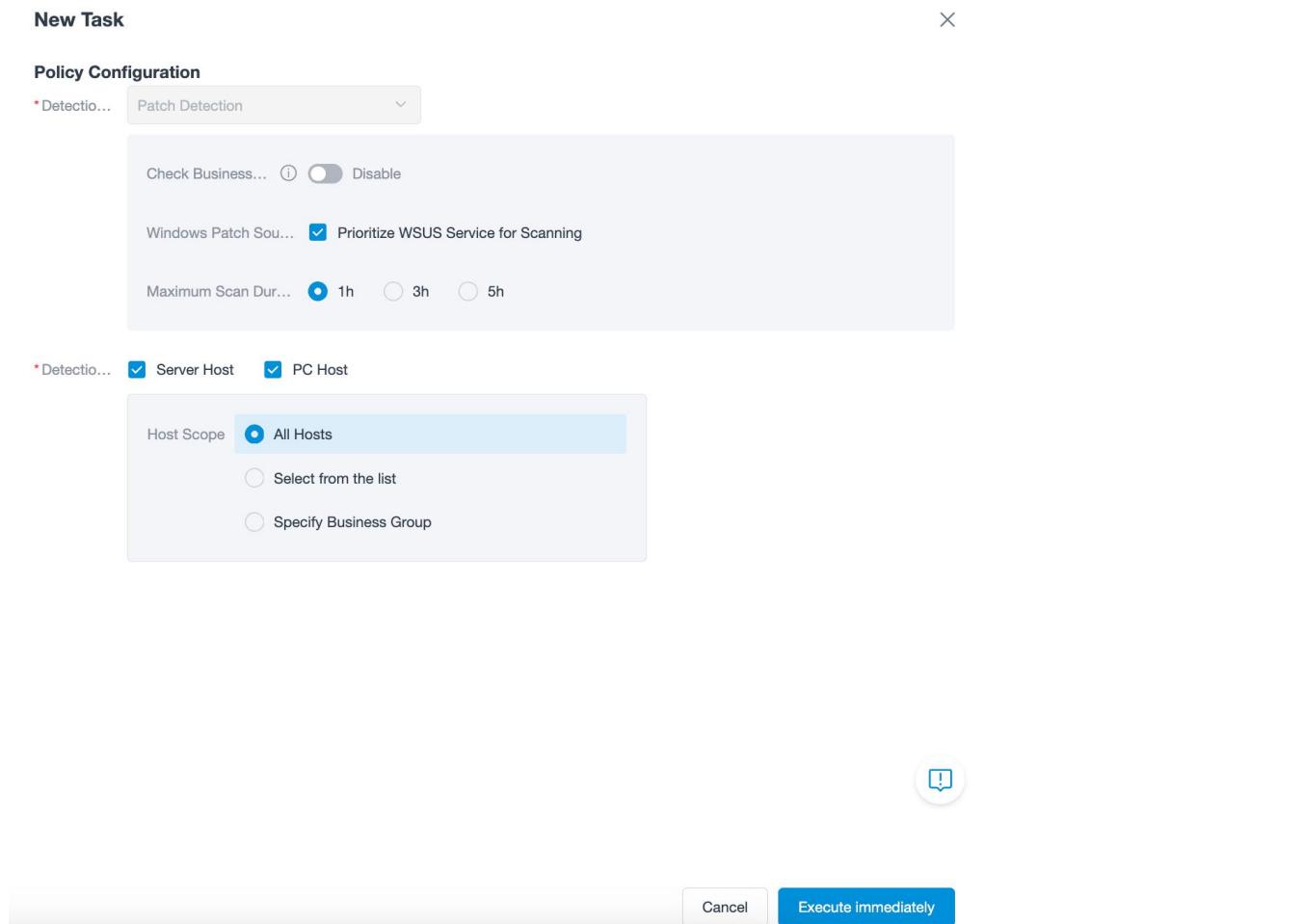
(1) Detection All: A full-volume detection is initiated by default using the template policy "Patch Detection". You can select the host detection scope, and the default setting covers all hosts. steps:

- Click the "Detection All" button, and a page for creating a new task will pop up.
- The detection policy is, by default, the template policy - Patch Detection.
- Set the switch for checking the business impact of Linux patch risks. It is turned off by default.

You can manually turn it on. After turning it on, the business impact of the Linux patch risk items found in this detection task will be checked.

- The Maximum Scan Duration is 1 hour by default. If the detection task is not completed within the set duration, a timeout will occur. You can select the Maximum Scan Duration according to the estimated time.
- The Detection Scope covers all hosts of Server and PC by default. You can make a selection according to the host scope you need to detect.
- After confirming that the above information has been filled in completely, click "Execute"

"Immediately" to issue the patch detection for the hosts.



(2) Detection: Used to initiate targeted retests for specific hosts in existing risk analysis results.

steps:

- Switch the analysis perspective to the "Group by Host" view, select the relevant data, and click the "Detection" button. A new task page will pop up.
- The detection policy is, by default, the template policy - Patch Detection.
- Set the switch for the business impact of Linux patch risks, which is turned off by default. You can manually turn it on. After turning it on, the business impact of the Linux patch risk items found in this detection task will be checked.
- The Maximum Scan Duration is 1 hour by default. If the detection task is not completed within the set duration, a timeout will occur. You can select the Maximum Scan Duration according to

the estimated time.

- The Detection Scope is the checked host information and cannot be modified.
- After confirming that the above information has been filled in completely, click "Execute Immediately" to issue the patch detection for the hosts.

The screenshot shows the Sentry CWPP interface for Risk Discovery. The left sidebar includes options like Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery, and more. The main area is titled 'Host Risk' and has tabs for 'Vulnerability', 'Patch' (which is selected), and 'Weak Password'. Below these tabs is a 'Patch List' table with columns for Severity, Risk Features, and Assets. A red box highlights the 'Affected Assets' section, which lists two hosts: 10.106.1.1 and 10.106.1.2. To the right, there's a 'New Task' configuration window for 'Patch Detection'. It includes fields for 'Check Business...', 'Windows Patch Sou...', 'Maximum Scan Dur...', and a dropdown for 'Detectio...'. At the bottom right of the task window are 'Cancel' and 'Execute Immediately' buttons. The 'Affected Assets' section is also highlighted with a red box.

Instructions:

- After a detection task is initiated, it will be added to the queue by trigger time to wait for detection. Each queue allows a maximum of 10 pending tasks. If there are more than 10 pending tasks in the queue when a user creates a new task, task creation will be blocked, and a prompt will appear: "Too many pending tasks in the queue. Please try again later."
- After the detection is completed, you can click "Execution Records" to view the historical execution records within the past 180 days. The page will jump to Risk Discovery > Detection > Execution Records, and the detection type will default to "Host Risk_Patch".

Task Trigger ...	Task Name	Task Type	Policy	Detection Object	Detection T...	Task start time	Operation
2025-12-24 09:30:01	PC-202...	Custom	Patch Detection	PC	Host Risk_Pat...	2025-12-24 09:30:36	End Task View Failed Item
2025-12-24 09:30:00	Patch-PC	System Prese...	Patch Detection	PC	Host Risk_Pat...	2025-12-24 09:30:00	End Task View Failed Item
2025-12-24 03:30:00	Patch	System Prese...	Patch Detection	Server	Host Risk_Pat...	2025-12-24 03:30:00	End Task View Failed Item
2025-12-23 09:30:00	Patch-PC	System Prese...	Patch Detection	PC	Host Risk_Pat...	2025-12-23 09:30:19	End Task View Failed Item
2025-12-23 09:30:00	PC-202...	Custom	Patch Detection	PC	Host Risk_Pat...	2025-12-23 09:30:00	End Task View Failed Item
2025-12-23 03:30:00	Patch	System Prese...	Patch Detection	Server	Host Risk_Pat...	2025-12-23 03:30:00	End Task View Failed Item

6.1.1.3. Weak password

1、Page Display

Detect weak password situations in various applications on the host. Click on the highlighted 'View supported detection application' to display the names of supported apps.

List display: Analyzing weak passwords, you can choose different analysis perspectives, including aggregation by application and aggregation by asset.

- Aggregation by application: Statistically display all affected applications and corresponding weak password related information from the application dimension.
- Aggregate by asset: Conduct statistics from the asset dimension to display the distribution of weak passwords on host objects.

steps:

- If you need to initiate weak password detection for host risks, you can choose full detection or targeted detection based on actual testing requirements:
 - To perform full-volume detection, simply click the "Detection All" button.
 - To retest specific applications from existing risk analysis results, switch the analysis

perspective to the "Group by Application" view, select the target range of data, and then click the "Detection" button.

- To retest specific hosts from existing risk analysis results, switch the analysis perspective to the "Group by Host" view, select the target range of data, and then click the "Detection" button.
- To retest specific data from existing risk analysis results, click the "Detection" button in the operation bar corresponding to the relevant list data.
- When the host scope of the business group under the user's data rights changes (e.g., adding or removing hosts), click the "Update Statistics" button to recalculate and recompile the results. Each successful update will log the update time; if the update fails, a warning icon will be displayed—hover your cursor over it to view the failure reason.
- Click on a single piece of data or the small triangle icon in front of the data to expand the corresponding information.
- You can click "Display" to determine whether the password value is displayed as plain text or cipher text.
- If you want to put a collection of common, simple passwords that are easy to guess or crack into a dictionary, you can click the "Dictionary" button.
- If you think a certain account weak password has little risk and does not affect system security, you can click the "Add to Whitelist" button individually or in batches to whitelist the weak password, so that these weak passwords will be ignored during the next scan.
- Click the "Whitelist Management" button, and you can enter the whitelist management page to view the whitelist, cancel whitelisting, and perform operations related to creating new whitelist rules.

- Click the "Execution Records" button, and you can view the detection history records and execution status of host risks - weak passwords within the past 180 days.
- The system supports batch exporting of weak passwords or selecting to export some of them.

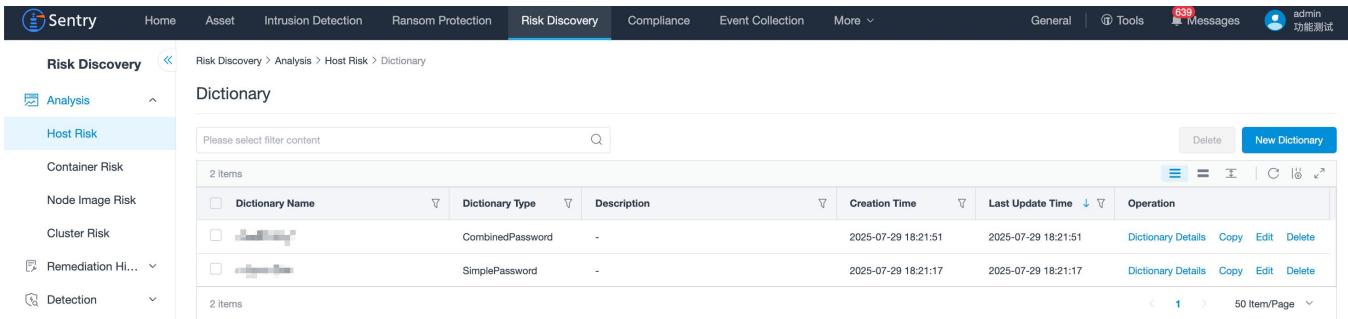
Asset Category	Affected Application	Count
Linux	CouchDB	1
Linux	MySQL	1
Linux	OpenLDAP	1
Linux	PostgreSQL	3
Windows	SSH	58

2、Dictionary management:

steps:

- If you want to build a list (i.e. dictionary) containing common, simple, or easily guessed passwords for quick detection and identification of weak passwords you have set to improve account security, you can click the "Dictionary" button.
- Then click on "New Dictionary" to create a new dictionary. You can manually input it or import it directly. Among them:
 - The dictionary categories are divided into simple passwords and combination passwords.
 - Simple Password:** A simple password dictionary that checks if your password is set to any password in the dictionary. If it is set, it is considered a weak password.
 - Combination Password:** A combination password dictionary that combines password features for weak password detection.

- Click  to view the descriptions of two dictionary categories.
- For newly created dictionaries, you can view the dictionary details and perform operations such as copying, editing, and deleting.



Dictionary Name	Dictionary Type	Description	Creation Time	Last Update Time	Operation
[REDACTED]	CombinedPassword	-	2025-07-29 18:21:51	2025-07-29 18:21:51	Dictionary Details Copy Edit Delete
[REDACTED]	SimplePassword	-	2025-07-29 18:21:17	2025-07-29 18:21:17	Dictionary Details Copy Edit Delete

3、White list management:

steps:

- If you want to view the whitelist list of host vulnerabilities, patches, and weak passwords, cancel whitelisting, or create new whitelist rules, you need to click the "Whitelist Management" button to enter the whitelist management page.
- The precise whitelist displays a list of results for accurately whitelisting specific risk items. If you want to cancel the whitelisting, you can directly click the "Cancel Whitelisting" button.
- If you need to create a whitelist rule for batch whitelisting based on conditions, you can enter the fuzzy whitelist rule page.
 - Click on 'New Rule' and fill in relevant parameters, including different risk characteristic conditions, application host scope, effective scope, rule description, and other information.
 - For newly created whitelist rules, you can edit and delete them.
 - After creation, you can click on the highlighted number of the affected record to view the specific risk data affected by the rule.

The screenshot shows the Sentry CWPP interface. The top navigation bar includes Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery (selected), Compliance, and More. On the right, there are General, Tools, 999+ Messages, and a user account for admin. The main area is titled 'Risk Discovery > Analysis > Host Risk > White List'. The left sidebar has sections for Host Risk (selected), Container Risk, Node Image Risk, Cluster Risk, Remediation History, Detection, and Library Query. The 'Host Risk' section has tabs for Vulnerability, Patch, and Weak Password (selected). Below this is a 'Precise Whitelist' section with a note about creating rules based on conditions. A search bar says 'Please select filter content'. A table lists one item: 'test1' with 'Empty passwords' type, 'SSH' affected application, and a whitelist time of '2025-11-19 09:48:53'. Buttons for 'Cancel Whitelisting' and 'Precise Whitelist' are visible.

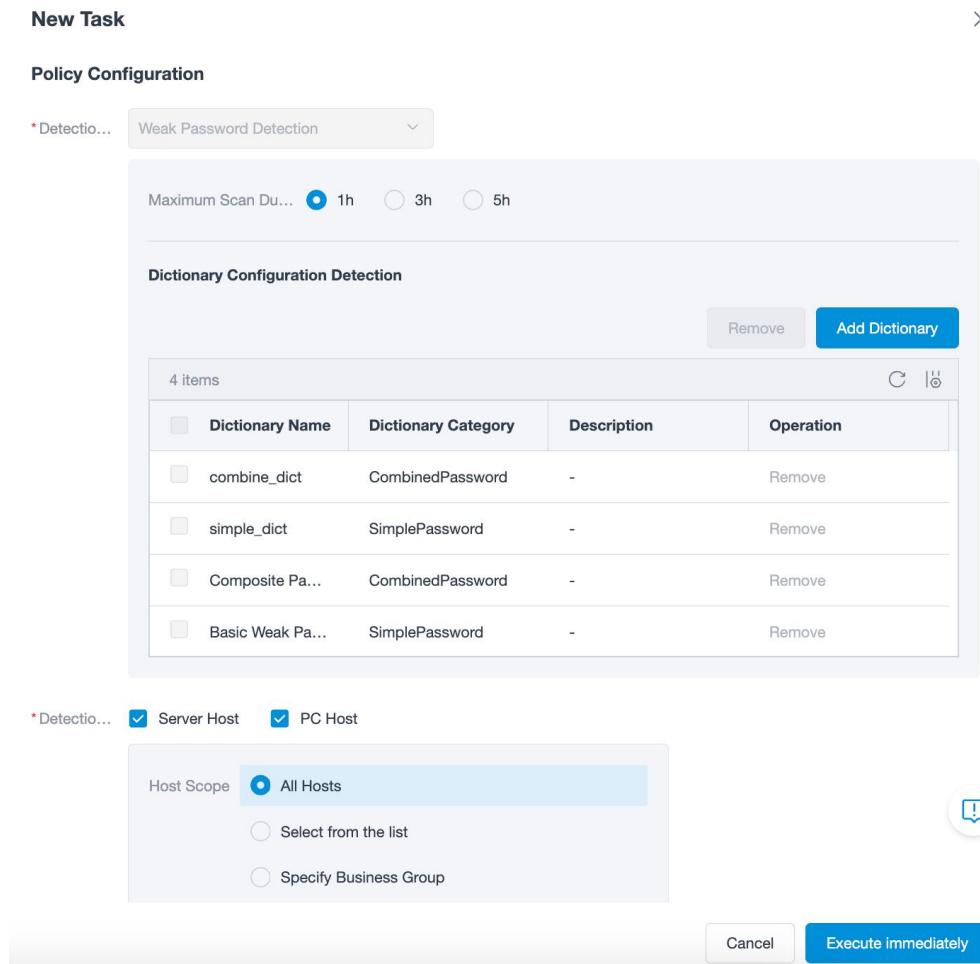
4、Detection Logic

The system supports weak password detection on hosts from different dimensions. You can click "Detection All" or check the data and then click "Detection" to directly initiate the detection.

(1) Detection All: A full-volume detection is initiated by default using the template policy "Weak Password Detection". You can select the host detection scope, and the default setting covers all hosts.

steps:

- Click the "Detection All" button, and a page for creating a new task will pop up.
- The detection policy is, by default, the template policy - Weak Password Detection.
- The Maximum Scan Duration is 1 hour by default. If the detection task is not completed within the set duration, a timeout will occur. You can select the Maximum Scan Duration according to the estimated time.
- The Dictionary Configuration Detection is, by default, the weak password dictionary preset by Qingteng. You can add a custom dictionary.
- The Detection Scope covers all hosts of Server and PC by default. You can make a selection according to the host scope you need to detect.
- After confirming that the above information has been filled in completely, click "Execute Immediately" to issue the weak password detection for the hosts.



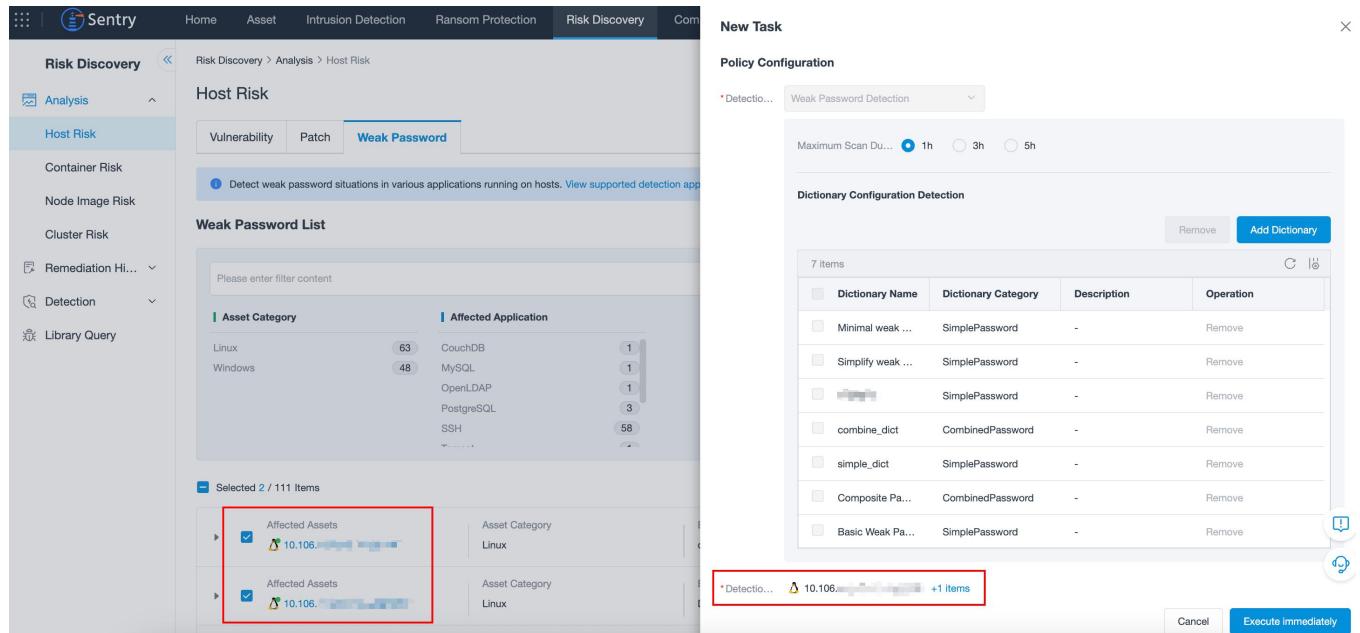
(2) Detection: Used to initiate targeted retests.

Scenario 1: Initiate a retest for specific hosts in existing risk analysis results

steps:

- Switch the analysis perspective to the "Group by Host" view, select the relevant data, and click the "Detection" button. A new task page will pop up.
- The detection policy is, by default, the template policy - Weak Password Detection.
- The Maximum Scan Duration is 1 hour by default. If the detection task is not completed within the set duration, a timeout will occur. You can select the Maximum Scan Duration according to the estimated time.
- The Dictionary Configuration Detection is, by default, the weak password dictionary preset by Qingteng. You can add a custom dictionary.

- The Detection Scope is the checked host information and cannot be modified.
- After confirming that the above information has been filled in completely, click "Execute Immediately" to issue the weak password detection for the hosts.



Scenario 2: Initiate a retest for specific applications in existing risk analysis results

steps:

- Switch the analysis perspective to the "Group by Application" view, select the relevant data, and click the "Detection" button. A new task page will pop up.
- The scope of detection items is the checked applications. If you think some applications do not need to be detected, you can remove them individually or in batches.
- The Maximum Scan Duration is 1 hour by default. If the detection task is not completed within the set duration, a timeout will occur. You can select the Maximum Scan Duration according to the estimated time.
- The Dictionary Configuration Detection is, by default, the weak password dictionary preset by Qingteng. You can add a custom dictionary.
- The Detection Scope covers all hosts of Server and PC by default. You can make a selection

according to the host scope you need to detect.

- After confirming that the above information has been filled in completely, click "Execute Immediately" to issue the weak password detection for the hosts.

The screenshot shows the Sentry CWPP Risk Discovery interface. The 'Weak Password' tab is selected. In the 'Testing Items' section, there are two items: 'CouchDB' (Linux Application) and 'PostgreSQL' (Linux Application). In the 'Affected Applications' section, 'CouchDB' and 'PostgreSQL' are selected. The 'Dictionary Configuration Detection' section shows several preset dictionaries like 'Minimal weak pass...', 'Simplify weak pass...', etc.

Scenario 3: Initiate a retest for specific data in existing risk analysis results

steps:

- Click the "Detection" button in the operation bar corresponding to the relevant list data; a new task page will pop up.
- The detection items will be automatically populated with the application corresponding to the data, and the detection scope will be automatically populated with the host information corresponding to the data.
- The default maximum scan duration is 1 hour. If the detection task is not completed within the set duration, a timeout will occur. You can select the maximum scan duration based on your estimated time.
- The detection dictionary is configured with Qingteng's preset weak password dictionary by default, and you can add a custom dictionary.
- After confirming and filling in the above information, click "Execute Immediately" to initiate

the weak password detection for the host.

The screenshot shows the Sentry CWPP interface. The top navigation bar includes Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery (selected), More, General, Tools (with 99+ messages), and a user account for admin. The left sidebar has sections for Risk Discovery, Analysis (Host Risk selected), Host Risk, Container Risk, Node Image Risk, Cluster Risk, Remediation History, Detection, and Library Query. The main content area is titled 'Host Risk' and 'Weak Password'. It shows a sub-section 'Weak Password List' with a search bar and filter options (Total 74 items, Group by Application Items, Updated on 2025-12-24 11:27:38). Below this is a table with columns: Affected Assets, Asset Category, Business Group, Account Name, Password Value, First discovery time, and Operation. A single row is shown: 'Affected Assets' is 192.168.1.100, 'Asset Category' is Linux, 'Business Group' is Default Business Group, 'Account Name' is admin, 'Password Value' is 123***, 'First discovery time' is 2025-12-11 20:04:56, and 'Operation' has a red box around it. A red arrow points to the 'Detection' button in the 'Operation' column.

New Task

Testing Items

1 items	
Application Name	Application Type
Zookeeper	Linux Application +1 items

Maximum Sca... 1h 3h 5h

Dictionary Configuration Detection

7 items			
Dictionary Name	Dictionary Category	Description	Operation
Minimal weak pass...	SimplePassword	Applications suitable for ...	Remove
Simplify weak pass...	SimplePassword	Applications applicable fo...	Remove

Detection Scope

* Detection Sc... 192.168.1.100

Instructions:

- After a detection task is initiated, it will be added to the queue by trigger time to wait for detection. Each queue allows a maximum of 10 pending tasks. If there are more than 10 pending tasks in the queue when a user creates a new task, task creation will be blocked, and

a prompt will appear: "Too many pending tasks in the queue. Please try again later."

- After the detection is completed, you can click "Execution Records" to view the historical execution records within the past 180 days. The page will jump to Risk Discovery > Detection > Execution Records, and the detection type will default to "Host Risk_Weak Password".

Task Trigger ...	Task Name	Task Type	Policy	Detection Object	Detection T...	Task start time	Operation
2025-12-24 11:24:00	Weak Password	System Prese...	Weak Passwo...	Server	Host Risk_We...	2025-12-24 11:24:00	End Task View Failed Item
2025-12-24 04:00:00	[REDACTED]-2025...	Custom	Weak Passwo...	Server	Host Risk_We...	2025-12-24 04:00:01	End Task View Failed Item
2025-12-23 11:24:00	Weak Password	System Prese...	Weak Passwo...	Server	Host Risk_We...	2025-12-23 11:24:00	End Task View Failed Item
2025-12-23 04:00:00	[REDACTED]-2025...	Custom	Weak Passwo...	Server	Host Risk_We...	2025-12-23 04:00:01	End Task View Failed Item
2025-12-22 11:24:00	Weak Password	System Prese...	Weak Passwo...	Server	Host Risk_We...	2025-12-22 11:24:00	End Task View Failed Item
2025-12-22 04:00:00	[REDACTED]-2025...	Custom	Weak Passwo...	Server	Host Risk_We...	2025-12-22 04:00:01	End Task View Failed Item

6.1.2. Container risk

6.1.2.1. loophole

1、Page Display

The system supports vulnerability detection for applications running on containers. You can click the "Detection Items" to view the details of the detection items. Among them:

If you think certain detection items do not need to be detected, you can click to close them.

List display: For the filtered vulnerabilities, you can choose different analysis perspectives, including aggregation by vulnerability and aggregation by image.

- Aggregation by vulnerability: Statistics are conducted from the vulnerability dimension,

displaying relevant information about all vulnerabilities and the affected images on the vulnerabilities.

- Aggregation by image: Conduct statistics from the image dimension, displaying relevant information of all images and the distribution of vulnerabilities on the images.

steps:

- If you need to initiate vulnerability detection for container risks, you can choose full detection or targeted detection based on actual testing requirements:
 - To perform full-volume detection, simply click the "Detection All" button.
 - To retest specific vulnerabilities from existing risk analysis results, switch the analysis perspective to the "Group by Vulnerability" view, select the target range of data, and then click the "Detection" button.
- When the host scope of the business group under the user's data rights changes (e.g., adding or removing hosts), click the "Update Statistics" button to recalculate and recompile the results. Each successful update will log the update time; if the update fails, a warning icon will be displayed—hover your cursor over it to view the failure reason.
- Click the small triangle icon in front of a single data entry or directly click on the data entry to display the corresponding information of the vulnerability, including the affected images, associated containers, etc.
- Click the highlighted "View Details" to pop up the detailed information of the vulnerability, including vulnerability description, repair suggestions, scanning information, etc.
- If you think a certain vulnerability has little risk and does not affect system security, you can click the "Add to Whitelist" button individually or in batches to whitelist the vulnerability, so that these vulnerabilities will be ignored during the next scan.

- To view the whitelist, cancel whitelisting, or create new whitelist rules, you can click the "Whitelist Management" button to enter the whitelist management page for relevant operations.
- Click the "Execution Records" button, and you can view the detection history and execution status of Container Risk - Vulnerability from the past 180 days.
- The system supports exporting all vulnerabilities or selecting to export some of them.

ID	Severity	Vulnerability Name	Risk Features	Affected A...	Detection Method	Number of...
QTV-2021...	High	XStream <=1.4.17 Deserialization Remote Code ...	hasRemoteExec	XStream	VersionComparison	1
QTV-2022...	Critical	PostgreSQL JDBC Driver Remote Code Executi...	hasRemoteExec	PostgreS...	VersionComparison	1

2. Whitelist Management

steps:

- If you want to view the whitelist of container vulnerabilities, cancel whitelisting, or create new whitelist rules, you need to click the "Whitelist Management" button to enter the whitelist management page.
- The Precise Whitelist displays the result list of precisely whitelisting specific risk items. If you want to cancel whitelisting, you can directly click the "Cancel Whitelisting" button.
- If you need to create a whitelist rule for batch whitelisting based on conditions, you can enter the Fuzzy Whitelist Rule page.

- Click "Create Rule" and fill in relevant parameters, including conditions for different risk characteristics, application scope, effective scope, rule description, and other information.
- For newly created whitelist rules, you can edit and delete them.
- After creation, you can click the highlighted number in the affected records to view the risk data specifically affected by the rule.

The screenshot shows the Sentry CWPP interface. The top navigation bar includes Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery (selected), Compliance, More, General, Tools, Messages (99+), and admin. The left sidebar has sections for Analysis, Host Risk, Container Risk (selected), Node Image Risk, Cluster Risk, Remediation History, Detection, and Library Query. The main content area is titled 'White List' under 'Vulnerability'. It displays a table with two items:

ID	Risk	Affected Assets	Whitelist Time	Operation
QTV-2024-002197	High	runc Container Escape Vulnerability (CVE-202...	2025-08-18 12:07:32	Cancel Whitelisting
QTV-2024-007234	High	Spring Security authentication bypass vulnera...	2025-08-01 16:19:57	Cancel Whitelisting

3、Detection Logic

The system supports vulnerability detection on containers from different dimensions. You can click "Detection All" or check the data and then click "Detection" to directly initiate the detection.

(1) Detection All: By default, it triggers a full scan for the template policy Vulnerability Detection.

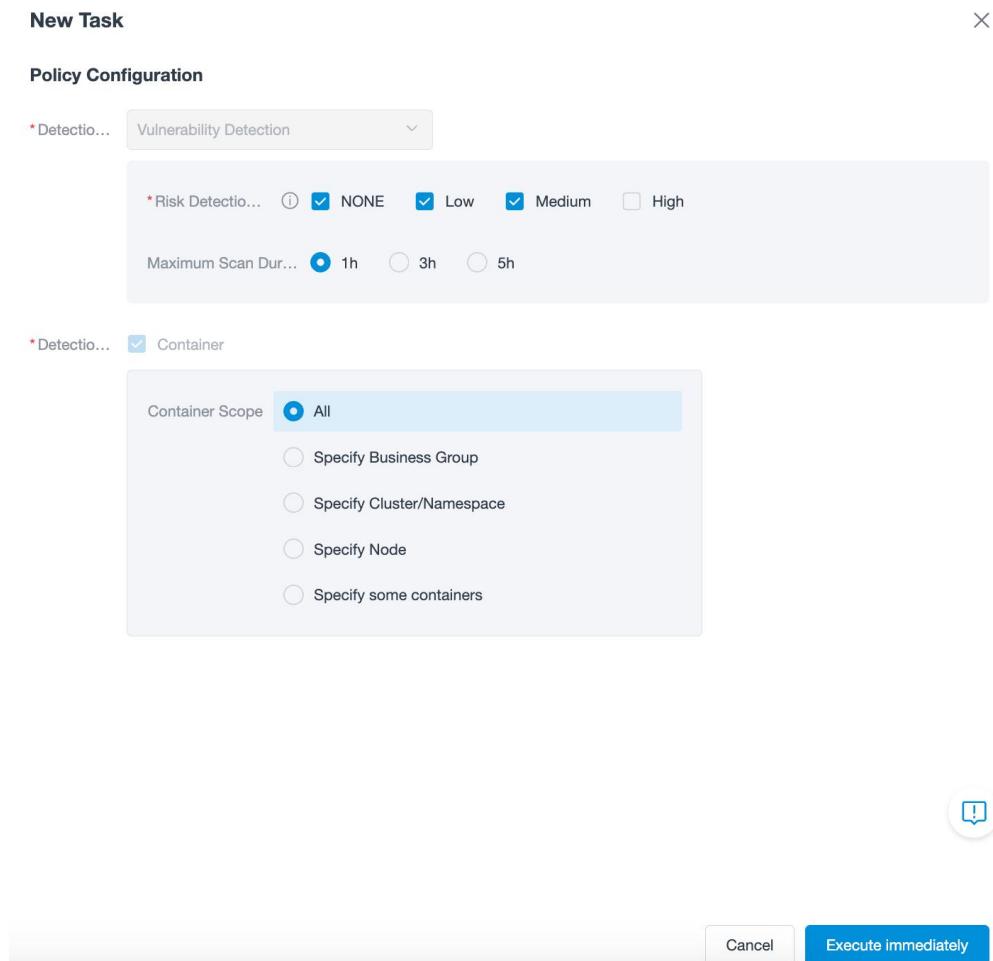
You can select the container scan scope, which defaults to all containers.

steps:

- Click the "Detection All" button, and a page for creating a new task will pop up.
- The detection policy is, by default, the template policy - Vulnerability Detection.
- By default, the detection risks are set to no risk, low risk, and medium risk, and high risk is not detected by default. You can check or uncheck the detection risks according to your detection needs. It should be specially noted that the detection risk here refers to the potential impact that may occur when using POC scripts for detection. Therefore, the detection risk settings

selected here will affect the detection items included when executing the task.

- The maximum scanning duration is 1 hour by default. If the detection task is not completed within the set duration, a timeout will occur. You can select the maximum scanning duration according to the estimated time.
- The detection scope covers all containers by default. You can make a selection according to the container scope you need to detect.
- After confirming that the above information has been filled in completely, click "Execute Immediately" to issue the vulnerability detection for the containers



(2) Detection: Used to initiate targeted retests for specific vulnerabilities in existing risk analysis results.

steps:

- Switch the analysis perspective to the "Group by Vulnerability" view, or in the detection item management interface, select the relevant data and click the "Detection" button. A new task page will pop up.
- The scope of detection items is the checked vulnerabilities. If there is a high - risk detection risk for a detection item, a prompt will appear: There is a high risk in the vulnerability detection items. Please confirm whether to initiate the detection! If you think some detection items do not need to be detected, you can remove them individually or in batches.
- The maximum scanning duration is 1 hour by default. If the detection task is not completed within the set duration, a timeout will occur. You can select the maximum scanning duration according to the estimated time.
- The detection scope covers all containers by default. You can make a selection according to the container scope you need to detect.
- After confirming that the above information has been filled in completely, click "Execute Immediately" to issue the vulnerability detection for the containers.

The screenshot shows the Sentry CWPP interface with the 'Risk Discovery' tab selected. In the 'Container Risk' section, under the 'Vulnerability' tab, two vulnerabilities are selected: 'Redis' (High severity) and 'glibc Buffer Overflow' (Critical severity). These are highlighted with a red border. The 'New Task' dialog box is open, showing the 'Testing Items' section with the selected items listed. The 'Detection Scope' section shows 'Container' selected. The 'Operation' section includes fields for 'Detection Method' (VersionComparison), 'Risk Detection' (NONE), and 'Operation' (Remove). The 'Maximum Scan Duration' is set to 1 hour. At the bottom right of the dialog box are 'Cancel' and 'Execute immediately' buttons.

Instructions:

- After a detection task is initiated, it will be added to the queue by trigger time to wait for detection. Each queue allows a maximum of 10 pending tasks. If there are more than 10 pending tasks in the queue when a user creates a new task, task creation will be blocked, and a prompt will appear: "Too many pending tasks in the queue. Please try again later."
- After the detection is completed, you can click the "Execution Records" button to view the historical execution records within the past 180 days. The page will jump to Risk Discovery > Detection > Execution Records, and the detection type will default to "Container Risk_Vulnerability".

Detection ID	Detection Type	Detection Object	Start Executed	Execution Status	Total Time	Execution Result	Operation
[REDACTED]	Container Risk_Vulnerability	Container	2025-07-30 1...	Completed	23 seconds	Successful: 10 Failed: 1	View Failed Items
[REDACTED]	Container Risk_Vulnerability	Container	2025-07-30 1...	Completed	3 minutes 1 s...	Successful: 1 Failed: 0	View Failed Items
[REDACTED]	Container Risk_Vulnerability	Container	2025-07-30 1...	Completed	3 minutes 3 s...	Successful: 2 Failed: 0	View Failed Items
[REDACTED]	Container Risk_Vulnerability	Container	2025-07-30 1...	Completed	6 minutes 35 ...	Successful: 8 Failed: 1	View Failed Items
[REDACTED]	Container Risk_Vulnerability	Container	2025-07-24 1...	Completed	48 seconds	Successful: 1 Failed: 0	View Failed Items
[REDACTED]	Container Risk_Vulnerability	Container	2025-07-24 1...	Completed	12 minutes 50...	Successful: 0 Failed: 0	View Failed Items
[REDACTED]	Container Risk_Vulnerability	Container	2025-07-22 1...	Timeout	1 hours 0 min...	Successful: 0 Failed: 9	View Failed Items

6.1.2.2. Weak password

1、Page Display

The system supports weak password detection for applications running in the container. Clicking on the highlighted "View Applications Supporting Detection" will display the names of the supported applications.

List display: Analyzing weak passwords, you can choose different analysis perspectives, including aggregation by application and aggregation by container.

- Aggregation by application: Statistically display all affected applications and corresponding

weak password related information from the application dimension.

- Aggregate by container: Conduct statistics from the container dimension, displaying relevant information of all containers and the corresponding weak password situations on the containers.

steps:

- If you want to initiate weak password detection for container risks, you can choose full detection or targeted detection based on your actual testing needs:
 - To perform a full detection, simply click the "Detection All" button.
 - To re-test some applications that already have risk analysis results, switch the analysis view to the "Group by Application" view, select the target scope data, then click the "Detection" button.
- When the host scope of the business group in the user's data permissions changes (e.g., adding or removing hosts), you can click the "Update Statistics" button to recalculate and re-statistics the results. Each successful update will record the update time; if the update fails, a warning icon  will appear, and you can hover over the icon to view the failure reason.
- Click the small triangle icon in front of a single data entry or directly click on the single data entry to display the corresponding information of the aggregated data.
- To choose whether the password value is displayed as plain text or cipher text, you can click the "Password Display" button.
- If you want to put a collection of common, simple passwords that are easy to guess or crack into a dictionary, you can click the "Dictionary Management" button.
- If you think a weak password of a certain account has little risk and does not affect system security, you can click the "Add to Whitelist" button individually or in batches to whitelist the

weak password, so that these weak passwords will be ignored during the next scan.

- To view the whitelist, cancel whitelisting, or create new whitelist rules, you can click the "Whitelist Management" button to enter the whitelist management page for relevant operations.
- Click the "Execution Records" button, and you can view the detection history and execution status of container risk - weak password detection within the past 180 days.
- The system supports batch exporting of weak passwords or selecting to export some of them.

The screenshot shows the Sentry CWPP web interface. The top navigation bar includes links for Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery (which is highlighted in blue), Compliance, Event Collection, More, General, Tools, Messages (with a red notification badge), and a user account for admin. On the left, there's a sidebar with sections like Analysis, Host Risk, Container Risk (selected and highlighted in blue), Node Image Risk, Cluster Risk, Remediation History, Detection, and Library Query. The main content area is titled 'Container Risk' under 'Analysis > Container Risk'. It has tabs for 'Vulnerability' and 'Weak Password' (which is selected and highlighted in blue). A note says 'Perform weak password detection on applications running in containers. View supported detection applications'. Below this is a 'Weak Password List' section with a search bar and a 'Collapse' button. It shows a table with columns for 'Affected Application' and 'Weak Password Type'. The table data is as follows:

Affected Application	Weak Password Type	Count
MySQL	Empty passwords	2
SSH	Weak password by default	0
Zookeeper	The password is the same as the user...	2
	Common weak passwords	3

At the bottom of the list, there are buttons for 'Total 7 Items', 'Analysis Perspective: Group by Application 3', 'Updated on 2025-12-24 11:22:38', 'Display' (with a dropdown menu), and actions like 'Add to whitelist', 'Export', 'Detection', 'Export All', 'Update Statistics', and 'Detection All'.

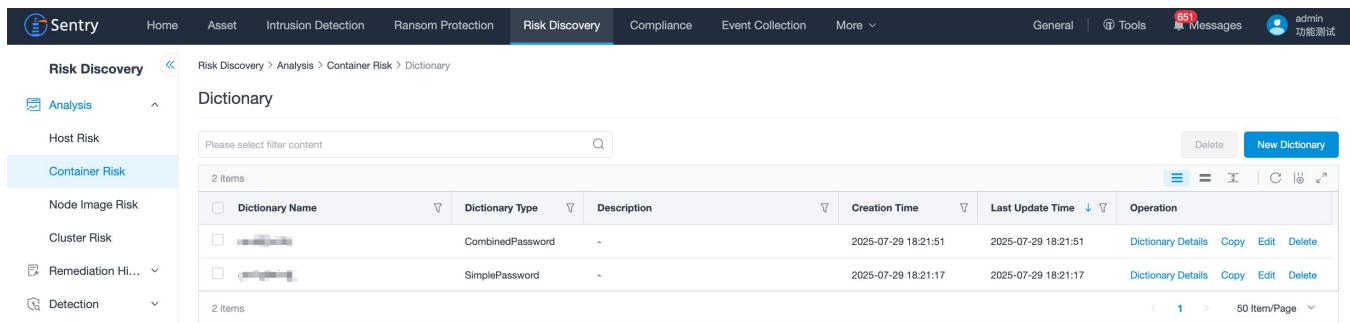
2. Dictionary Management

steps:

- If you want to build a list (i.e., a dictionary) containing common, simple, or easily guessable passwords for quickly detecting and identifying the weak passwords you set to improve account security, you can click the "Dictionary Management" button.
- Then click "Create New Dictionary" to create a new dictionary. You can manually enter passwords or directly import them. Among them:
 - Dictionary categories are divided into simple passwords and combined passwords.
 - Simple passwords: The simple password dictionary checks whether your password is

set as any password in this password dictionary. If so, it is determined as a weak password.

- Combined passwords: The combined password dictionary combines password features for weak password detection.
- Click the  button, and you can view the descriptions of the two dictionary categories.
- For the newly created dictionary, you can view the dictionary details and also perform operations such as copying, editing, and deleting.



Dictionary Name	Dictionary Type	Description	Creation Time	Last Update Time	Operation
[REDACTED]	CombinedPassword	-	2025-07-29 18:21:51	2025-07-29 18:21:51	Dictionary Details Copy Edit Delete
[REDACTED]	SimplePassword	-	2025-07-29 18:21:17	2025-07-29 18:21:17	Dictionary Details Copy Edit Delete

3、Whitelist Management

steps:

- If you want to view the whitelist of weak passwords for containers, cancel whitelisting, or create new whitelist rules, you need to click the "Whitelist Management" button to enter the whitelist management page.
- The Precision Whitelist displays the result list of precisely whitelisting specific risk items. If you want to cancel whitelisting, you can directly click the "Cancel Whitelisting" button.
- If you need to create a whitelist rule for batch whitelisting based on conditions, you can enter the Fuzzy Whitelist Rule page.
 - Click "Create Rule" and fill in relevant parameters, including conditions for different risk characteristics, application scope, effective scope, rule description, and other

information.

- For newly created whitelist rules, you can edit and delete them
- After creation, you can click the highlighted number in the affected records to view the risk data specifically affected by the rule.

Account name	Weak Password Type	Affected Applications	Whitelist Time	Operation
kingbase	Common weak passwords	SSH	2025-11-22 16:03:28	Cancel Whitelisting

4、Detection Logic

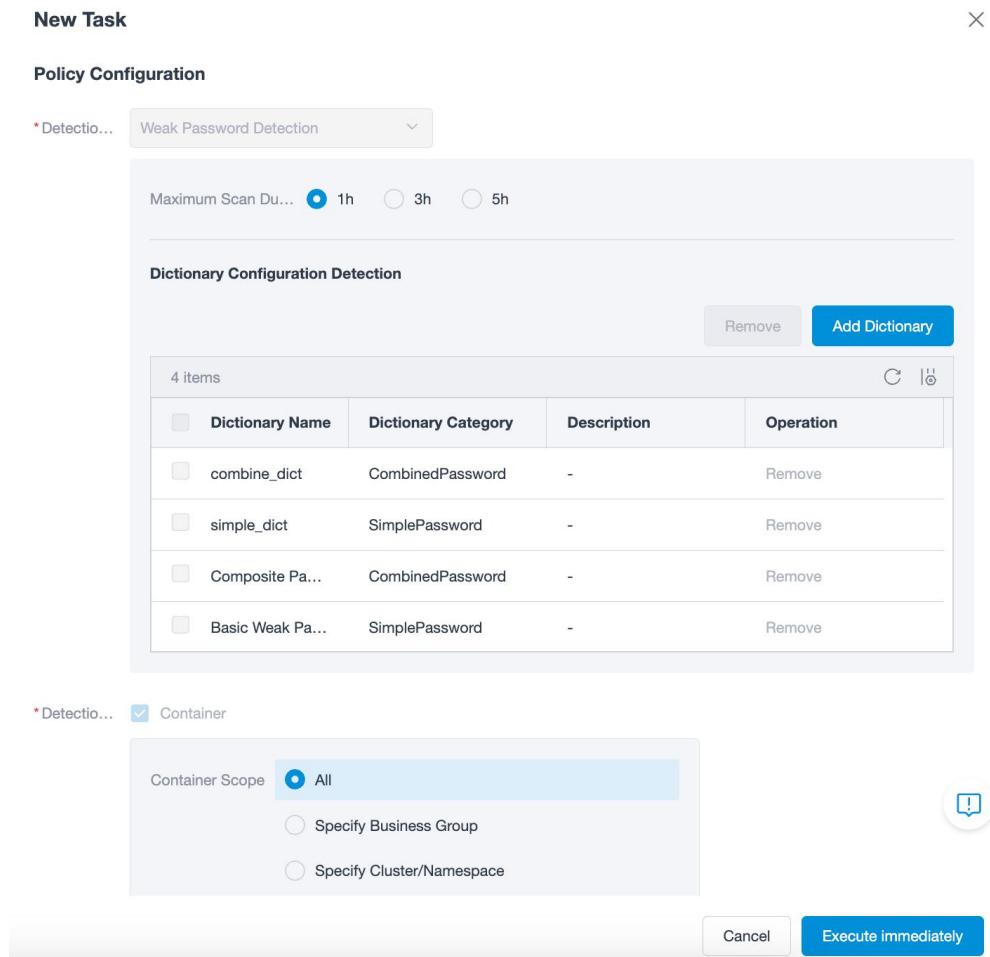
The system supports weak password detection on containers from different dimensions. You can click "Detection All" or check the data and then click "Detection" to directly initiate the detection.

(1) Detection All: By default, it initiates a comprehensive detection for the template policy "Weak Password Detection". You can select the container detection scope, and by default, it covers all containers.

steps:

- Click the "Detection All" button, and a page for creating a new task will pop up.
- The detection policy is, by default, the template policy - Weak Password Detection.
- The maximum scanning duration is 1 hour by default. If the detection task is not completed within the set duration, a timeout will occur. You can select the maximum scanning duration according to the estimated time.
- The detection dictionary configuration is, by default, the weak password dictionary preset by Qingteng. You can add a custom dictionary.

- The detection scope covers all containers by default. You can make a selection according to the container scope you need to detect.
- After confirming that the above information has been filled in completely, click "Execute Immediately" to issue the weak password detection for the containers.



(2) Detection: Used to initiate targeted retests for specific applications in existing risk analysis results.

steps:

- Switch the analysis perspective to the "Group by Application" view, tick the data and click the "Detection" button to bring up the new task creation page.
- The scope of detection items is the checked applications. If you think some applications do not need to be detected, you can remove them individually or in batches.

- The maximum scanning duration is 1 hour by default. If the detection task is not completed within the set duration, a timeout will occur. You can select the maximum scanning duration according to the estimated time.
- The detection dictionary configuration is, by default, the weak password dictionary preset by Qingteng. You can add a custom dictionary.
- The detection scope covers all containers by default. You can make a selection according to the container scope you need to detect.
- After confirming that the above information has been filled in completely, click "Execute Immediately" to issue the weak password detection for the containers.

The screenshot shows the Sentry CWPP web interface. On the left, there's a sidebar with various navigation options like Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery, Analysis, Host Risk, Container Risk, Node Image Risk, Cluster Risk, Remediation History, Detection, and Library Query. The 'Container Risk' section is currently selected.

In the main area, under 'Analysis', the 'Weak Password' tab is active. It displays a 'Weak Password List' with a table showing affected applications (Jenkins, KingbaseES, MySQL, PostgreSQL, Redis) and weak password types (Empty passwords, Weak password by default, The password is the same as the user name, Common weak passwords). A red box highlights the 'Affected Applications' section where Jenkins and KingbaseES are listed.

A modal window titled 'New Task' is open on the right. It has two tabs: 'Testing Items' and 'Dictionary Configuration Detection'. The 'Testing Items' tab shows a table with two items: KingbaseES (Linux Application) and Jenkins (Linux Application). The 'Dictionary Configuration Detection' tab shows a table with seven items, each corresponding to a different dictionary name and category. At the bottom of the modal, there are buttons for 'Cancel' and 'Execute immediately'.

Instructions:

- After a detection task is initiated, it will be added to the queue by trigger time to wait for detection. Each queue allows a maximum of 10 pending tasks. If there are more than 10 pending tasks in the queue when a user creates a new task, task creation will be blocked, and a prompt will appear: "Too many pending tasks in the queue. Please try again later."
- After the detection is completed, you can click "Execution Records" to view the historical

execution records within the past 180 days. The page will jump to Risk Discovery > Detection > Execution Records, and the detection type will default to "Container Risk_Weak Password".

Task Trigger ...	Task Name	Task Type	Policy	Detection Object	Detection T...	Task start time	Operation
2025-12-24 11:22:00	container wea...	System Prese...	Weak Passwo...	Container	Container Ris...	2025-12-24 11:22:00	End Task View Failed Item
2025-12-23 11:22:00	container wea...	System Prese...	Weak Passwo...	Container	Container Ris...	2025-12-23 11:22:00	End Task View Failed Item
2025-12-22 11:22:00	container wea...	System Prese...	Weak Passwo...	Container	Container Ris...	2025-12-22 11:22:00	End Task View Failed Item
2025-12-21 11:22:00	container wea...	System Prese...	Weak Passwo...	Container	Container Ris...	2025-12-21 11:22:00	End Task View Failed Item
2025-12-20 11:22:00	container wea...	System Prese...	Weak Passwo...	Container	Container Ris...	2025-12-20 11:22:00	End Task View Failed Item
2025-12-19 11:22:00	container wea...	System Prese...	Weak Passwo...	Container	Container Ris...	2025-12-19 11:22:00	End Task View Failed Item

6.1.3. Cluster Risk

6.1.3.1. Page Display

Cluster security supports risk inspection of the container runtime environment. You can click the highlighted "Risk Item Management" to view the details of risk items. Among them:

- You can click the / button to customize the enabling/disabling of risk items. You can also check data to enable or disable in batches.
- Click the "View Details" button to pop up the detailed information of the risk item. You can view the description of the risk, repair suggestions, and other information from it.

General search: The system has a general search box that supports unified retrieval of risk information and asset information.

Quick screening: The system lists key risk filtering options and values such as risk level, risk characteristics, risk item category, and inspection node type, facilitating users to click with one key to

quickly trigger result filtering.

List display: When analyzing vulnerabilities, you can choose different analysis perspectives, including aggregation by vulnerability and aggregation by host. Statistics are made from the vulnerability dimension to display relevant information of all vulnerabilities and the situation of assets affected by vulnerabilities.

- **Group by vulnerability:** Statistics are made from the vulnerability dimension to display relevant information of all vulnerabilities and the situation of assets affected by vulnerabilities.
- **Group by host:** Statistics are made from the asset dimension to display the distribution of vulnerabilities on host objects.

steps:

- If you want to initiate vulnerability detection for cluster risks, you can choose full detection or targeted detection based on your actual testing needs:
 - To perform a full detection, simply click the "Detection All" button.
 - To initiate retesting for some hosts with existing risk analysis results: switch the analysis perspective to the "Group by Host" view, select the target range of data, and then click the "Detection" button.
- When the host scope of the business under the user's data rights changes (e.g., adding or removing hosts), click the "Update Statistics" button to recalculate and recompile the results.
A successful update will log the update time; in the event of a failure, a warning icon  will appear—hover your cursor over it to view the cause of the failure.
- For each vulnerability, the corresponding affected assets can be seen. Click the highlighted host IP value to pop up the corresponding details page.

- Click the "View Details" button to pop up the detailed information of the vulnerability. You can view the description, repair suggestions and other information of the vulnerability from it.
- If you think a certain vulnerability has little risk and does not affect system security, you can click the "Add to Whitelist" button individually or in batches to whitelist the vulnerability so that these vulnerabilities can be ignored during the next scan.
- Click the "Whitelist Management" button, and you can enter the whitelist management page to view the whitelist list, cancel whitelisting, and perform operations related to creating new whitelist rules.
- Click the "Execution Records" button, and you can view the detection history records and execution status of cluster risks within nearly 180 days.
- The system supports exporting all vulnerabilities or selecting part of them for export.

Cluster Risk							
Please enter filter content Collapse ^							
Severity		Risk Features		Risk Item Category		Check Node Type	
◆ Critical	◆ High	◆ Medium	◆ Low	1 hasRemoteExec	4 hasKernel	0 KBS	0 TARGET_ALL
				10 hasLocalPerm	0 hasExp	0 Docker	17 TARGET_MASTER
				6 hasPoc	0	0 TARGET_NODE	0

Total 17 items | Analysis Perspective: Group by Vulnerability 8 items | Updated on 2025-12-09 15:46:24 | Add to whitelist | Export | Export All | Update Statistics | Detection All

Severity	Risk item name	Risk Type	Risk Item Category	Check Node Type	Risk Features	Affected Clu...	Affected No...
Critical	Docker privilege bypass vulnerability (CVE-....)	HTTP Request	Docker	TARGET_ALL	hasRemoteExec	0	1
High	runc privilege escalation vulnerability (CVE-....)	Path Traversal	Docker	TARGET_ALL	-	0	3
High	runc Container Escape Vulnerability (CVE-2....)	Permission and Acces...	Docker	TARGET_ALL	-	0	3
High	Containerd Security Feature Bypass Vulner...	Permission and Acces...	Docker	TARGET_ALL	hasLocalPerm	0	3

Note:

- When the analysis perspective is switched to aggregation by vulnerability or aggregation by host, you can directly click the small triangle icon in front of a single data item to display the information corresponding to the vulnerability or the host.
- The other operational procedures are the same as above.

6.1.3.2. Whitelist Management

steps:

- If you want to view the whitelist of cluster risks, cancel whitelisting, or create new whitelist rules, you need to click the "Whitelist Management" button to enter the whitelist management page.
- The Precision Whitelist displays the result list of precisely whitelisting specific risk items. If you want to cancel whitelisting, you can directly click the "Cancel Whitelisting" button.
- If you need to create a whitelist rule for batch whitelisting based on conditions, you can enter the Fuzzy Whitelist Rule page.
 - Click "Create Rule" and fill in relevant parameters, including conditions for different risk characteristics, application host scope, effective scope, rule description, and other information.
 - For newly created whitelist rules, you can edit and delete them.
 - After creation, you can click the highlighted number in the affected records to view the risk data specifically affected by the rule.

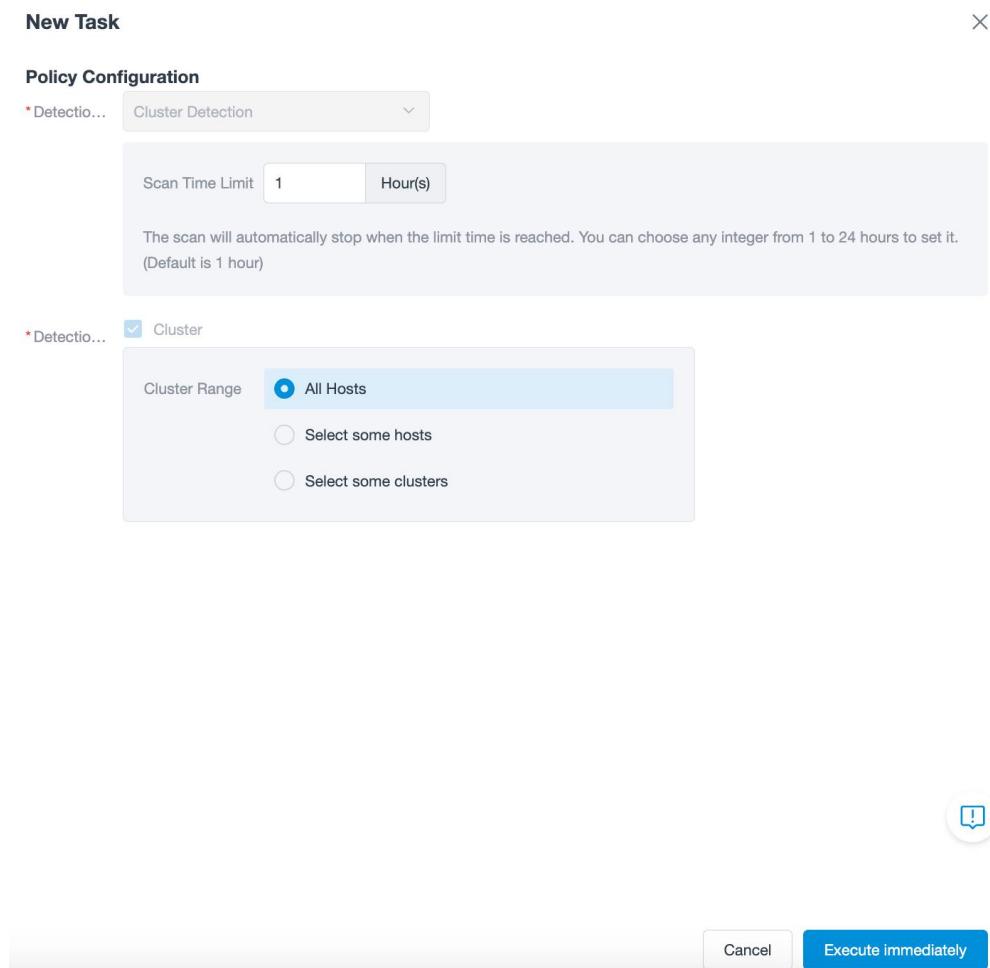
ID	Risk	Affected nodes	Affected Clusters	Whitelist Time	Operation
QTV-2024-023334	Critical	Docker privilege bypass...	10.1.1.1	2025-09-11 10:53:56	Cancel Whitelisting

6.1.3.3. Detection Logic

(1) Detection All: By default, it initiates a comprehensive detection for the template policy "Cluster Detection". You can select the cluster detection scope, and by default, it covers all hosts.

steps:

- Click the "Detection All" button, and a page for creating a new task will pop up.
- The detection policy is, by default, the template policy - Cluster Detection.
- The default scanning time limit is 1 hour. If the detection task is not completed within the set time, a timeout will occur. You can select any integer from 1 hour to 24 hours for setting.
- The detection scope covers all hosts by default. You can make a selection according to the cluster scope you need to detect.
- After confirming that the above information has been filled in completely, click "Execute Immediately" to issue the cluster detection.



(2) Detection: Initiate retesting for some hosts with existing risk analysis results.

steps:

- Switch the analysis perspective to the "Group by Host" view, select the data, and click the "Detection" button to bring up the new task creation page.
- The default detection strategy is the template strategy - cluster detection.
- The default maximum scanning duration is 1 hour. If the detection task is not completed within the set duration, a timeout will occur. You can select the maximum scanning duration based on the estimated time.
- The detection scope is the selected host information and cannot be modified.
- After confirming that the above information is filled in, click "Execute immediately" to issue the cluster detection for the host.

The screenshot shows the 'New Task' dialog box in the Sentry CWPP interface. The 'Policy Configuration' section has 'Cluster Detection' selected. The 'Scan Time Limit' is set to 1 Hour(s). The 'Affected Assets' section is highlighted with a red box, showing two entries: '192.168.1.10' and '192.168.1.11'. The 'Execute immediately' button is at the bottom right.

Instructions:

- After a detection task is initiated, it will be added to the queue by trigger time to wait for detection. Each queue allows a maximum of 10 pending tasks. If there are more than 10 pending tasks in the queue when a user creates a new task, task creation will be blocked, and a prompt will appear: "Too many pending tasks in the queue. Please try again later."
- After the detection is completed, you can click "Execution Records" to view the historical

execution records within the past 180 days. The page will jump to Risk Discovery > Detection > Execution Records, and the detection type will default to "Cluster Risk".

Task Trigger	Task Name	Task Type	Policy	Detection Object	Detection Type	Task start time	Operation
2025-12-09 15:20:28	1765...	Quick Scan	-	Cluster	Cluster Risk	2025-12-09 15	End Task View Failed Item
2025-12-05 11:53:00	Cluster Risk	System Prese...	Cluster Risk	Cluster	Cluster Risk	2025-12-05 11	End Task View Failed Item
2025-12-05 11:52:00	Cluster Risk	System Prese...	Cluster Risk	Cluster	Cluster Risk	2025-12-05 11	End Task View Failed Item
2025-12-05 11:51:00	Cluster Risk	System Prese...	Cluster Risk	Cluster	Cluster Risk	2025-12-05 11	End Task View Failed Item
2025-12-05 11:50:00	Cluster Risk	System Prese...	Cluster Risk	Cluster	Cluster Risk	2025-12-05 11	End Task View Failed Item
2025-12-05 11:48:00	Cluster Risk	System Prese...	Cluster Risk	Cluster	Cluster Risk	2025-12-05 11	End Task View Failed Item

6.1.4. Node Image risk

6.1.4.1. Image Overview

6.1.4.1.1. Image rule settings

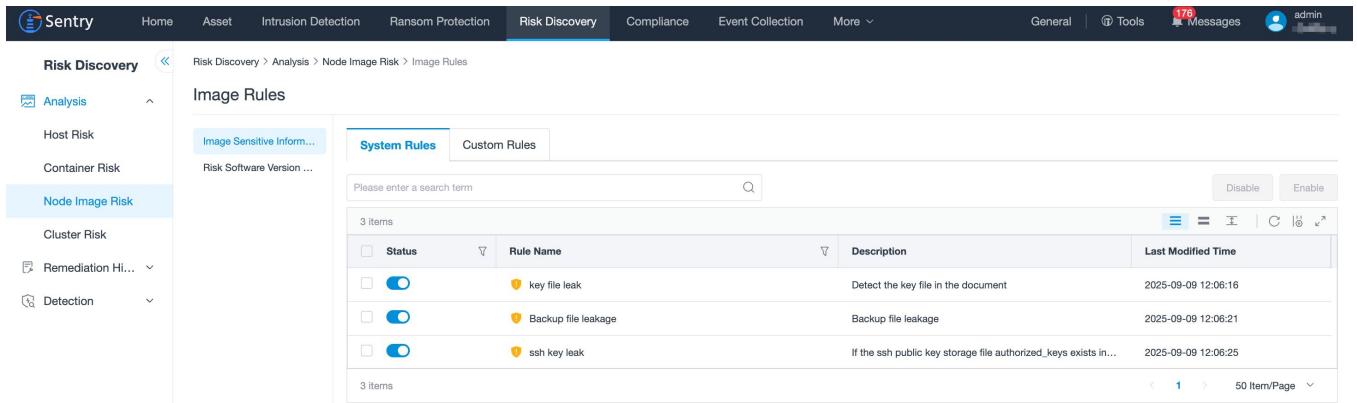
This feature includes the setting of sensitive information, basic images, and risk software version detection rules.

1、Image sensitive information: supports system rules for viewing suspicious operations and sensitive information in mirror scanning, and can control the opening and closing of rules; And support custom detection rules.

steps:

- Click on "Configuration Management" in the upper right corner of the image overview page and select "Image Rule Settings".

- You can click  to turn on/off the preset rules.
- Click the New Rule button under the Custom Rules tab, enter the matching criteria, and complete the rule settings.



Status	Rule Name	Description	Last Modified Time
	key file leak	Detect the key file in the document	2025-09-09 12:06:16
	Backup file leakage	Backup file leakage	2025-09-09 12:06:21
	ssh key leak	If the ssh public key storage file authorized_keys exists in...	2025-09-09 12:06:25

New Rule

Basic Information

Status: Enable

* Rule Name: Please enter a name within 30 characters

* Severity: Please select the risk level

Description: Please enter a description

Rule Detection

To match files in the image, enter a regular expression following the PCRE specification
 Each rule can match up to 100 files per image. Multiple rules are separated by line breaks

* Matching....:

1 Example:
 Match files with a suffix of .php, the expression is \.php\$
 Match files with the filename containing virus, the expression is virus or .virus.*



2、Set risk software version: Support setting risk version blacklists and whitelists for software, so that the latest risk version installation packages and risk software version information can be discovered during image scanning.

steps:

- Firstly, to customize the application, click on the "New Application" button in the custom application management and enter the name of the application to be detected.
- Then click on 'New Rule', select the application and set the risk version information for the application.
- Rules that have been created can be modified and deleted.

The screenshot shows the Sentry CWPP web interface. The top navigation bar includes links for Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery (which is highlighted), Compliance, Event Collection, and More. On the far right, there are links for General, Tools, 178 Messages, and a user account for admin. The main content area is titled 'Risk Discovery > Analysis > Node Image Risk > Image Rules'. A sidebar on the left lists categories: Analysis, Host Risk, Container Risk, Node Image Risk (which is selected and highlighted in blue), Cluster Risk, Remediation History, and Detection. The main panel displays a table titled 'Image Rules' with two entries:

Application Name	Rule Type	Operator	Version	Add Time	Modified Time	Operation
gmp	BlackListRule	equal	1:6.1.2-10.el8	2025-09-10 11:39:40	2025-09-10 11:39:40	Modify Delete
python	BlackListRule	greater than	1.0	2025-09-10 11:38:22	2025-09-10 11:38:22	Modify Delete

The screenshot shows a modal dialog titled 'Custom Application Management'. It contains a search bar labeled 'Please select filter content' and a 'New' button. Below the search bar is a table with two items:

Application Name
gmp
python

At the bottom of the dialog are navigation buttons for page 1 of 1, a '50 Item/Page' dropdown, and a close button (X).

New Rule X

Set Application and Version Information

* Select A... :

Rule Type: Whitelist Rules (Safe Version Range) Blacklist Rules (Risk Version Range)

* Operator:

* Version:



Note:

After adding, deleting, and modifying software version rules, it is necessary to re execute the scanning and detection task.

6.1.4.1.2. Whitelist Management

This function is divided into risk whitelist and image whitelist.

steps:

- If you want to view the list of node image risks that have been added to the whitelist or cancel the whitelisting, you need to click the "Whitelist Management" button to enter the whitelist management page.
- The risk whitelist includes all risk types of node images (security patches, application vulnerabilities, sensitive information, malicious viruses, webshells, and risky software versions), and displays the result list of specific risk content and whitelisting in terms of

application scope. If you want to cancel the whitelisting, you can directly click the "Remove" button.

- The image whitelist displays the result list of specific images added to the whitelist, and all risks of the image will be whitelisted. If you want to cancel the whitelisting, you can directly click the "Remove" button.

Whitelist N...	Risk Type	Risk Content	Application Scope	Reason for Whit...	Creation Time	Creator	Operation
webshell...	WebShell	bca3a'	All Images	-	2025-09-10 18:10:28	admin	Remove

6.1.4.1.3. Image Overview List

1、Page Display

The system supports risk detection for node images, including risks such as security patches, application vulnerabilities, WebShell, malicious viruses, and sensitive information. Click the highlighted "Supported Node Types for Detection" to view the supported nodes.

General search: The system is equipped with a general search box, supporting unified retrieval of asset information, risk information, and detection status.

Quick screening: The system arranges two key filtering options, detection status and security issues, along with their filtering values, facilitating users to click with one key to quickly trigger result filtering.

steps:

- For each mirror, you can see the corresponding security issues. Click on the highlighted mirror name, and the page will jump to the detailed page of that mirror.

- If you want to get the latest node mirror asset results, you can click the "Update" button to trigger it manually, and the node mirror data detected by the App will be synchronized.
- If you need to perform risk detection, you can click "Full Detection". In the pop-up detection interface, fill in the relevant policy configuration and select the execution scope. You can also perform risk detection on a single mirror or batch mirrors. Click the "Detect" button in the operation bar or select mirrors in batch and click the "Detect" button. Fill in the relevant policy configuration in the pop-up detection interface.
- If you think a single mirror or batch mirrors have no major risks and do not affect system security, you can click the "Add to Whitelist" button in the operation bar or select mirrors in batch and click the "Add to Whitelist" button to whitelist the mirrors, so that the risks on these mirrors will be ignored during the next scan.
- For each mirror, you can see the corresponding security issues. Click on the highlighted mirror name, and the page will jump to the detailed page of that mirror, including mirror overview, security patches, application vulnerabilities, webshell, malicious viruses, sensitive information, layer files and installation packages. You can click on different tabs to view the detailed information of the corresponding mirror or risk information. Among them:
 - You can click the mirror overview tab to view the basic information of the mirror. There are also risk items existing on the mirror, and the system has given repair suggestions. You can refer to and copy the commands for repair.
 - If you want to re-detect this mirror, you can click the "Re-detect" button in the upper right corner.
 - If you think this mirror has no major risks and does not affect system security, you can click the "Add to Whitelist" button in the upper right corner to whitelist

the mirror, so that the risk on this mirror will be ignored during the next scan.

- If you want to export the scan report of this mirror, click the "Export" button to select the export type. Considering the file size and performance issues, the installation package is not selected by default. So if necessary, please select it yourself. After determining the export type, click the "Confirm" button to export the mirror scan report.
- You can click on different tabs such as security patches/application vulnerabilities/Webshell/malicious viruses/sensitive information to view the risks existing in the mirror, and click the "View Details" button to pop up the detailed information of the risk.
 - If there is a webshell or malicious virus, you can also click the "Download File" button on the risk details page to download the file to the local for viewing and repair.
 - If you think a certain risk does not affect system security, you can click the "Add to Whitelist" button and select the application scope to whitelist the risk, so that these risks will be ignored during the next scan.
- You can click the layer file tab to view all layer file information of the mirror and the risk items existing on the layer files. Click the "View Details" button to pop up the basic information and detailed list of risk items of the layer file.
- You can click the installation package tab to view all installation package information of the mirror and the vulnerabilities existing in the installation package. Click the "View" button to pop up the basic information of the installation package. If the vulnerability distribution is safe, there is no data in the vulnerability detailed list.

- In the vulnerability list, if you think a certain risk does not affect the installation package and system security, you can click the "Add to Whitelist" button to whitelist the risk in all mirrors, so that these risks will be ignored during the next scan.

The screenshot shows the Sentry CWPP interface for 'Node Image Risk'. The left sidebar has 'Node Image Risk' selected. The main area shows a summary of detected issues:

Detection Status	Count	Security Issues	Count
Unspecified	0	Application Vulnerability	181
Completed	561	Sensitive Information	58
Error	423	Security Patch	126
		Risk Software Version Detection	88
		Virus	2

Below this is a table of 984 scanned images:

Image	Image Size	Running Containers	Related Images	Security Issues	Last Detection Time	Detection S...	Operation
registry: [REDACTED]	91.05MB	0	1	✓	2025-10-24 12:03:08	Completed	Detection Add to whitelist
registry: [REDACTED]	91.06MB	1	1	✓	2025-10-24 12:03:07	Completed	Detection Add to whitelist
registry: [REDACTED]	187.35MB	2	2	✓	2025-10-24 12:03:19	Completed	Detection Add to whitelist

The screenshot shows the 'Image Details' page for a Docker image. The left sidebar has 'Node Image Risk' selected. The main area shows basic information about the image:

Basic Information	Associated assets
Image ID: 30195ab... Operate...: alpine:3.21.3 CPU a...: amd64 Image ...: 217.66MB Create...: 2025-10-22 02:47:17	Running cont...: 0 Associated n...: 1 Environment ...: PATH=/go...

Repair Suggestions:

```

1 # [Poc] Add the following instruction to the Dockerfile to rebuild the image and fix the security vulnerability. If the installation package fails to upgrade, please try to upgrade to the latest version.
2 npm install ...

```

2、Detection Logic

Detection All: By default, detection is initiated for the template policy "Node Image Risk". You can select the detection scope of node images, and the default is all hosts. steps:

- Click the "Detection All" button to pop up the new task page.

- The default detection strategy is the template strategy - Node Image Risk.
- The default selected detection risk types are security patches, application vulnerabilities, sensitive information, and risky software versions.
- The running status check is enabled by default, and only the images of running containers are scanned.
- The default scanning time limit is 1 hour. If the detection is not completed within the set time, a timeout will occur. You can set any integer from 1 hour to 24 hours.
- The default detection scope is all hosts, and you can select according to the scope of node images that need to be detected.
- After confirming that the above information is filled in, click the "Execute Immediately" button to issue the detection.

New Task

Policy Configuration

Node Image Risk



* Risk Type Det... Security Patch Application Vulnerability WebShell Virus
 Sensitive Information Risk Software Version Detection

If not checked, this risk of node images will not be detected (at least one detection item must be checked)

Running Status... Enable

Enable to scan only the images of running containers, otherwise scan all node images

Scan Time Limit Hour(s)

The scan will automatically stop when the limit time is reached. You can choose any integer from 1 to 24 hours to set it. (Default is 1 hour)

* Detectio...



Node Image

- Node Image ... All Hosts
 Select some hosts
 Select cluster/namespace
 Specify Business Group



Detection: Detection can be initiated from the image dimension.

steps:

- Click the "Detection" button in the operation bar or select multiple images and click the "Detection" button to pop up the new task page.
- The default detection strategy is the template strategy - Node Image Risk.
- The default selected detection risk types are security patches, application vulnerabilities, sensitive information, and risky software versions.
- The default scanning time limit is 1 hour. If the detection is not completed within the set time, a timeout will occur. You can set any integer from 1 hour to 24 hours.
- The detection scope is the selected image information and cannot be modified.
- After confirming that the above information is filled in, click the "Execute Immediately" button to issue the detection.

New Task

X

Policy Configuration

* Detectio...

Node Image Risk

- * Risk Type Det... Security Patch Application Vulnerability WebShell Virus
 Sensitive Information Risk Software Version Detection

If not checked, this risk of node images will not be detected (at least one detection item must be checked)

Scan Time Limit

1

Hour(s)

The scan will automatically stop when the limit time is reached. You can choose any integer from 1 to 24 hours to set it. (Default is 1 hour)

* Detectio...

registry



Cancel

Execute immediately

Instructions:

- Whether it is a system preset task or a manually initiated detection task, if any of the detection risk types such as Security Patches, Application Vulnerabilities, or Risky Software Versions is selected, the node images and the inventory of image installation packages will be automatically synchronized before risk detection.
- All issued detection tasks will enter the queue to wait for detection. You can click the "Mirror task queue" button in the upper right corner of the page or the "Mirror task queue" button in the floating ball to jump to the mirror task queue page and view the execution status and results of all tasks. For details, please refer to 1.1.1.4.

6.1.4.1.4. Mirror task queue

This function allows you to view the execution status and results of all tasks for node mirror risk detection and node mirror data update.

Statistical Cards: Three statistical dashboards are set up for successful task execution, failed task execution, and pending task execution, allowing you to **直观地** (intuitively) see the total number of tasks in different states.

General Search: The system has set up a general search box, which supports unified retrieval by task trigger time, task trigger type, task type, task start time, and task status.

Steps:

- Whether initiated manually or as a system preset scheduled task, they will all enter the mirror task queue for queuing after execution and be executed in sequence.
- You can click the "End Task" button for a task being scanned to manually terminate the task. If there are pending tasks in the queue, the next task scan will be delayed after termination.
- You can click the "Re-execute" button for successful or failed tasks, which will re-update/scan the node mirror according to the original configuration of the task. Each re-executed task will generate a new record.
- You can click the highlighted number in the execution result to view the details of the runtime mirror scan result in the pop-up page, mainly including the name of the mirror scanned in the task, detection status, latest detection time, and task duration.

Task Trigger Time	Execution Range	Task Trigger	Task Type	Task start time	Task Duration	Task Status	Execution ...	Operation
2025-10-24 12:00:05	All Hosts	Automatic	Node image risk scan	2025-10-24 12:03:01	-	Running	982 / 984	End Task
2025-10-24 07:59:59	All Hosts	Automatic	Node image risk scan	2025-10-24 08:02:00	4 hours 1 min...	Failed	984 / 984	Re-execute
2025-10-24 03:59:59	All Hosts	Automatic	Node image risk scan	2025-10-24 04:01:00	4 hours 1 min...	Failed	984 / 984	Re-execute
2025-10-24 00:00:06	All Hosts	Automatic	Node image risk scan	2025-10-24 00:00:10	4 hours 0 min...	Failed	990 / 990	Re-execute
2025-10-23 19:59:59	All Hosts	Automatic	Node image risk scan	2025-10-23 19:59:59	4 hours 0 min...	Failed	990 / 990	Re-execute
2025-10-23 18:34:30	All Hosts	Manual	Node image risk scan	2025-10-23 18:39:01	3 minutes 59 ...	Failed	971 / 971	Re-execute
2025-10-23 16:00:05	All Hosts	Automatic	Node image risk scan	2025-10-23 16:24:00	2 hours 15 mi...	Failed	971 / 971	Re-execute
2025-10-23 12:00:09	All Hosts	Automatic	Node image risk scan	2025-10-23 12:23:00	4 hours 1 min...	Failed	971 / 971	Re-execute
2025-10-23 08:00:06	All Hosts	Automatic	Node image risk scan	2025-10-23 08:22:00	4 hours 1 min...	Failed	1032 / 1032	Re-execute

Runtime Image Scan Result Details

Image Name	Detection Status	Last Detection Time	Task Duration
registry	Success	2025-10-21 19:14:03	0 seconds
registry	Success	2025-10-21 19:13:43	0 seconds
registry	Success	2025-10-21 19:13:43	0 seconds
registry	Success	2025-10-21 19:13:43	0 seconds
registry	Success	2025-10-21 19:13:43	0 seconds
registry	Success	2025-10-21 19:13:43	0 seconds
registry	Success	2025-10-21 19:13:43	0 seconds

Instructions:

- Tasks preset by the system are not allowed to be re-executed.
- Only 50 tasks can be added to the queue at a time. Exceeding tasks will not be added to the queue and will not be detected.

6.1.4.2. Security Patches

The system supports the detection of security patches on node images and displays all detected patch-related information and the situation of affected images from the perspective of risk analysis.

steps:

- The list displays patch - related information, including Severity, Patch Name, Risk Features, Number of Affected Images, etc.
- If you want to obtain the latest risk detection results, you can click the "Update" button to update the list and recalculate the number of affected images.
- Click "View Details" to pop up the detailed information of the patch, including description, repair suggestions, reference information, etc.
- If you think a certain patch has little risk and does not affect system security, you can click the "Add to Whitelist" button individually or in batches to whitelist all images of the patch, so that these patches can be ignored during the next scan.
- The system supports exporting all or part of the risk data in the list.
- For each patch, the number of affected images can be seen. Click the highlighted number of images to pop up the detailed page of the affected image list. Among them:
 - The list displays image information such as Image, Image Size, Related Images, and Build Time.
 - Click the highlighted image name, and the page will jump to the detailed page of the image.
 - You can click the "Add to Whitelist" button to whitelist the image so that the risks on these images can be ignored during the next scan.

ID	Severity	Patch Name	Risk Features	Number of Aff...	Operation
QT012022022742	Critical	Debian CVE-2022-31813 : apache2 - security update	-	0 1	View Details Add to whitelist
QT012024000399	Critical	Debian dla-3710 : hyperv-daemons - security update	hasRemoteExec hasExp	0 1	View Details Add to whitelist
QT012022022667	Critical	Debian CVE-2022-23943 : apache2 - security update	-	0 1	View Details Add to whitelist

6.1.4.3. Application Vulnerabilities

The system supports the detection of application vulnerabilities on node images and displays all detected vulnerability - related information and the situation of affected images from the perspective of risk analysis.

steps:

- The list displays vulnerability - related information, including Severity, Vulnerability Name, Risk Features, Number of Affected Images, etc.
- If you want to obtain the latest risk detection results, you can click the "Update" button to update the list and recalculate the number of affected images.
- Click "View Details" to pop up the detailed information of the vulnerability, including Description, Repair Suggestions, Reference Information, etc.
- If you think a certain vulnerability has little risk and does not affect system security, you can click the "Add to Whitelist" button individually or in batches to whitelist all images of the vulnerability, so that these vulnerabilities can be ignored during the next scan.

- The system supports exporting all or part of the risk data in the list.
- For each vulnerability, the number of affected images can be seen. Click the highlighted number of images to pop up the detailed page of the affected image list. Among them:
 - The list displays image information such as Image, Image Size, Related Images, and Build Time.
 - Click the highlighted image name, and the page will jump to the detailed page of the image.
 - You can click the "Add to Whitelist" button to whitelist the image so that the risks on these images can be ignored during the next scan.

The screenshot shows two main sections of the Sentry CWPP interface:

Node Image Risk - Application Vulnerabilities

ID	Severity	Vulnerability Name	Release Time	Risk Features	Number of Affected Images	Operation
QTV-2021-009920	Critical	Rust rand_core	2021-02-17 00:00:00	hasRemoteExec	1	View Details Add to whitelist
QTV-2021-010567	Critical	Rust 资源管理器	2021-03-05 00:00:00	hasRemoteExec	1	View Details Add to whitelist
QTV-2022-000098	Critical	Spring Boot Admin SPE	2022-12-09 00:00:00	hasRemoteExec	1	View Details Add to whitelist
QTV-2023-066301	Critical	Hutool	2023-09-08 00:00:00	hasRemoteExec	1	View Details Add to whitelist

Affected Image List

Image	Image Size	Related Images	Build Time	Operation
alpine	470.8MB	1	2023-06-16 23:36:32	Add to whitelist

6.1.4.4. Webshell

The system supports the detection of webshell on node images and displays all detected webshell-related file information and the situation of affected images from the perspective of risk analysis.

steps:

- The list displays the file path (path within the image) that matches the rule, file MD5, Hit Backdoor Type, Number of Affected Images, etc.
- If you want to obtain the latest risk detection results, you can click the "Update" button to update the list and recalculate the number of affected images.
- Click "View Details" to pop up the basic information of the file and the details of the matching rule, including detection description, handling suggestions, etc.
- If you think a certain risk does not affect system security, you can click the "Add to Whitelist" button individually or in batches to whitelist all images of the risk, so that these risks can be ignored during the next scan.
- The system supports exporting all or part of the risk data in the list.
- For each risk, the number of affected images can be seen. Click the highlighted number of images to pop up the detailed page of the affected image list. Among them:
 - The list displays image information such as Image, Image Size, Related Images, and Build Time.
 - Click the highlighted image name, and the page will jump to the detailed page of the image.
 - You can click the "Add to Whitelist" button to whitelist the image so that the risks on these images can be ignored during the next scan.

Severity	File	SHA256	Hit Backdoor Type	Number of Affected Images	Operation
Critical	/var/www/html/index.html	26b2f...	HashCompare	00 1	View Details Add to whitelst
Critical	/var/www/html/index.html	4a4d...	HashCompare	00 1	View Details Add to whitelst
Critical	/root/apache-tomcat-8.5.24/webapp...	5161e...	ThunderFire	00 1	View Details Add to whitelst
Critical	/root/apache-tomcat-8.5.24/webapp...	b55e5...	ThunderFire	00 1	View Details Add to whitelst
Critical	/root/apache-tomcat-8.5.24/webapp...	bdb5d...	ThunderFire	00 1	View Details Add to whitelst

Image	Image Size	Related Images	Build Time	Operation
registry	678.83MB	1	2018-10-13 01:49:01	Add to whitelist

6.1.4.5. Malicious Virus

The system supports the detection of malicious viruses on node images and displays all detected malicious virus - related file information and the situation of affected images from the perspective of risk analysis.

steps:

- The list displays the file path (path within the image) that matches the virus detection library, file MD5, Hit Backdoor Type, Number of Affected Images, etc.
- If you want to obtain the latest risk detection results, you can click the "Update" button to update the list and recalculate the number of affected images.
- Click "View Details" to pop up the basic information and detection details of the file, including the detection library, repair methods, virus library version, etc.
- If you think a certain risk does not affect system security, you can click the "Add to Whitelist" button individually or in batches to whitelist all images of the risk, so that these risks can be ignored during the next scan.
- The system supports exporting all or part of the risk data in the list.
- For each risk, the number of affected images can be seen. Click the highlighted number of images to pop up the detailed page of the affected image list. Among them:
 - The list displays image information such as Image, Image Size, Related Images, and

Build Time.

- Click the highlighted image name, and the page will jump to the detailed page of the image.
- You can click the "Add to Whitelist" button to whitelist the image so that the risks on these images can be ignored during the next scan.

The screenshot shows the Sentry CWPP interface with the 'Risk Discovery' tab selected. Under 'Analysis', 'Node Image Risk' is chosen. The main panel displays a table titled 'Malicious Virus' with four items. Each item includes columns for Severity (all marked as Critical), File path, SHA256 hash, Hit Detection Library (JMav or Avira), Number of Affected Images (1), and Operation buttons for 'View Details' and 'Add to whitelist'. A sidebar on the left lists other risk categories like Host Risk, Container Risk, Cluster Risk, Remediation History, Detection, and Library Query.

Severity	File	SHA256	Hit Detection Library	Number of Affected Images	Operation
Critical	/home/[REDACTED]	dadd0c[REDACTED]	JMav	00 1	View Details Add to whitelist
Critical	/image/[REDACTED]	9a10e[REDACTED]	Avira	00 1	View Details Add to whitelist
Critical	/image/[REDACTED]	4b6232[REDACTED]	Avira	+1 items	View Details Add to whitelist
Critical	/image/[REDACTED]	11edf[REDACTED]	Avira	+1 items	View Details Add to whitelist

This screenshot shows the same interface but with the 'Affected Image List' tab selected. It displays a single item: 'registry.[REDACTED]' with a size of 1.26GB, one related image, and a build time of 2024-07-18 16:48:42. There is also a note indicating the list can only display up to 1000 items.

Image	Image Size	Related Images	Build Time	Operation
registry.[REDACTED]	1.26GB	00 1	2024-07-18 16:48:42	Add to whitelist

6.1.4.6. Sensitive Information

The system supports the detection of sensitive information on node images and displays all detected sensitive information - related data and the situation of affected images from the perspective of risk analysis.

steps:

- The list displays sensitive information - related details, including Severity, Rule Name, Number of Affected Images, etc.

- If you want to obtain the latest risk detection results, you can click the "Update" button to update the list and recalculate the number of affected images.
- If you think a certain risk does not affect system security, you can click the "Add to Whitelist" button individually or in batches to whitelist all images of the risk, so that these risks can be ignored during the next scan.
- The system supports exporting all or part of the risk data in the list.
- For each piece of sensitive information, the number of affected images can be seen. Click the highlighted number of images to pop up the detailed page of the affected image list. Among them:
 - The list displays image information such as Image, Image Size, Related Images, and Build Time.
 - Click the highlighted image name, and the page will jump to the detailed page of the image.
 - You can click the "Add to Whitelist" button to whitelist the image so that the risks on these images can be ignored during the next scan.

The screenshot shows the Sentry CWPP interface for Risk Discovery, specifically the Node Image Risk section. The top navigation bar includes Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery (which is selected), Compliance, Event Collection, and More. On the right, there are links for General, Tools, Messages, and a user account labeled 'admin 功能测试'. A circular badge in the top right corner indicates '1 Image task'.

The main content area is titled 'Node Image Risk' and shows a table with the following data:

Severity	Rule Name	Type	Description	Number of Affected Images	Operation
Medium	ssh key leak	SystemRule	If the ssh public key storage file auth...	12	Add to whiteli
Medium	key file leak	SystemRule	Detect the key file in the document	18	Add to whiteli
Medium	Backup file leakage	SystemRule	Backup file leakage	50	Add to whiteli

At the bottom of the table, it says '3 items'. To the right, there are buttons for 'Last Updated At' (2025-10-24 08:00:02), 'Update', and 'Add to whitelist'. There is also a '50 Item/Page' dropdown menu.

Image	Image Size	Related Images	Build Time	Operation
registry...	719.12MB	1	2025-07-02 11:21:54	Add to whitelist
registry...	367.79MB	1	2024-03-25 11:11:48	Add to whitelist
registry...	691.05MB	1	2024-12-30 14:42:10	Add to whitelist
registry...	784.4MB	1	2023-07-31 10:46:21	Add to whitelist
registry...	691.05MB	1	2024-12-29 17:52:05	Add to whitelist
registry...	303.07MB	1	2024-12-30 14:41:50	Add to whitelist
registry...	303.07MB	1	2024-12-29 17:51:46	Add to whitelist
registry...	303.07MB	1	2024-12-29 17:51:46	Add to whitelist
registry...	303.07MB	1	2024-12-29 17:51:46	Add to whitelist
registry...	303.07MB	1	2024-12-29 17:51:46	Add to whitelist
registry...	303.07MB	1	2024-12-29 17:51:46	Add to whitelist
registry...	303.07MB	1	2024-12-29 17:51:46	Add to whitelist
registry...	303.07MB	1	2024-12-29 17:51:46	Add to whitelist
registry...	303.07MB	1	2024-12-29 17:51:46	Add to whitelist
registry...	303.07MB	1	2024-12-29 17:51:46	Add to whitelist

6.1.4.7. Package Risk

The system supports risk software version and patch vulnerability detection for the installation packages of node images. On the function page, you can view the basic information of installation packages with risky software versions or patch vulnerabilities, associated images, and vulnerability distribution.

steps:

- Since the detection of risky software versions depends on the detection strategy configured by the system, you need to go to Image Rule Settings - Risk Software Version function to set it before detection.
- If you want to get the latest risk detection results, you can click the "Update" button to update the list and recalculate the number of associated images.
- You can view the associated images for each installation package. Click the highlighted number of images to pop up the detailed page of the affected image list. Among them:
 - The list displays image information such as the highlighted image name, image size, associated images, and build time.
 - Click the highlighted image name, and the page will jump to the detailed page of the image.

- If there are patch vulnerabilities in the installation package, you can view them in the vulnerability distribution column. When the mouse hovers over it, the specific risk level and the number of patch vulnerabilities will be displayed. Click the "View" button to pop up the vulnerability list. Among them:
 - The list displays vulnerability name, risk characteristics, and release time.
 - You can click the "Add to Whitelist" button to whitelist the risk items, so that these risks will be ignored in the next scan.

The screenshots illustrate the Node Image Risk analysis feature in the Sentry CWPP Risk Discovery module. The first screenshot shows the main Node Image Risk page with a table of packages and their risk levels. The second screenshot shows the Affected Image List, which lists images and their details. The third screenshot shows the Vulnerability List for the libde265-0 package, displaying specific vulnerabilities and their details.

Screenshot 1: Node Image Risk Analysis

Package Name	Image	Version	Related Images	Vulnerability Distribution	Operation
apache2-utils	OS	2.4.38-3+deb10u4	0/0	4 (Red) 2 (Yellow) 0 (Green)	View
libde265-0	OS	1.0.3-1+b1	0/0	0 (Green) 4 (Yellow) 0 (Blue)	View
commons-fileupload:commons-fileupload	JAVA	1.4	0/0	0 (Green) 1 (Yellow) 0 (Blue)	View
libgs9-common	OS	9.27-dfsg-2+deb10u4	0/0	1 (Red) 2 (Yellow) 0 (Green)	View
org.springframework.cloud:spring-cloud-openfeign-core	JAVA	3.0.3	0/0	0 (Green) 1 (Yellow) 0 (Blue)	View

Screenshot 2: Affected Image List

Image	Image Size	Related Images	Build Time
registry/	525.17MB	0/0	2021-07-21 07:21:01

Screenshot 3: Vulnerability List

Vulnerability Name	Risk Features	Release Time	Operation
Debian DLA-3676-1 ...	hasRemoteExec +1 items	2023-11-30 00:00:00	Add to whitelist
Debian DLA-3352-1 ...	hasRemoteExec +1 items	2023-03-05 00:00:00	Add to whitelist
Debian DLA-3280-1 ...	hasRemoteExec +1 items	2023-01-24 00:00:00	Add to whitelist
Debian DLA-3240-1 ...	hasRemoteExec +1 items	2022-12-15 00:00:00	Add to whitelist

6.2. Remediation History

6.2.1. Host Remediation History

6.2.1.1. Vulnerability

This list displays the vulnerability remediation history records of the host.

steps:

- For each vulnerability, you can view the corresponding affected assets. Click the highlighted host IP value, and the corresponding details page will pop up.
- Click the "View Details" button, and the detailed information of the vulnerability will pop up. You can view the description, remediation suggestions, remediation information and other details of the vulnerability from it.
- The system supports batch export of remediated vulnerabilities.

Risk Discovery > Remediation History > Host Remediation History

Host Remediation History

Vulnerability	Linux, patch	Windows, patch	Weak Password												
Please select filter content															
344 items															
Severity	Vulnerability Name	Risk Features	Affected nodes	Business Group	MTTR	Repair time	Operation								
Critical	BES AppServer remote command ex...	hasRemoteExec	10.106.110.182 k8s-01	dxh-out	2025-06-13 04:42:04	15 days 3 minutes	View Details								
Critical	BES AppServer remote command ex...	hasRemoteExec	10.106.110.182 k8s-01	dxh-out	2025-06-13 04:41:59	15 days 3 minutes	View Details								
High	BES AppServer Spark protocol deser...	hasRemoteExec	10.106.110.182 k8s-01	dxh-out	2025-06-13 04:41:41	15 days 6 minutes	View Details								
High	Spring Framework path traversal vul...	hasRemoteExec	10.106.110.182 k8s-01	dxh-out	2025-06-13 04:00:29	15 days 1 minutes	View Details								

6.2.1.2. Linux,patch

This list displays the installation history records of Linux patches for the host.

steps:

- For each patch, you can view the corresponding affected assets. Click the highlighted host IP value, and the corresponding details page will pop up.
- Click the "View Details" button, and the detailed information of the patch will pop up. You can

view the description, remediation suggestions, remediation commands and other information of the patch from it.

- The system supports batch export of installed patches.

Risk Discovery > Remediation History > Host Remediation History

Host Remediation History

Vulnerability	Linux, patch	Windows, patch	Weak Password	
Please select filter content <input type="text"/> <input type="button" value="Search"/>				
314 items				
Severity	Patch Name	Risk Features	Affected nodes	Business Group
High	CentOS 8 : krb5 (CESA-20...	hasRemoteExec	192.168.21.146 localhost.localdomain	[REDACTED]
High	CentOS 8 : krb5 (CESA-20...	hasExp hasRemoteE...	192.168.21.146 localhost.localdomain	[REDACTED]
High	CentOS 8 : openssl (CESA...	hasExp hasRemoteE...	192.168.21.146 localhost.localdomain	[REDACTED]
Medium	CentOS 8 : openssl (CESA...	hasRemoteExec	192.168.21.146 localhost.localdomain	[REDACTED]

6.2.1.3. Windows,patch

This list displays the patch installation records of Windows hosts. It fetches the latest data from the local daily at a scheduled time and supports manual updates.

steps:

- If you need to view the currently latest Windows patch installation records, click the "Update" button to obtain the latest data in real time.
- For each patch, you can see the corresponding affected assets. Click the highlighted host IP value to pop up the corresponding details page.
- The system supports batch export of the installed patches.

Risk Discovery > Remediation History > Host Remediation History					General	Tools	Messages	admin				
Host Remediation History					Container Remediation							
Vulnerability	Linux, patch	Windows, patch	Weak Password		Patch installation...							
● This list displays the patch installation records of Windows and hosts, and retrieves the latest data from the local system on a daily basis. It supports manual updates <input type="button" value="Update"/>												
Please select filter content <input type="text"/> <input type="button" value="Search"/>												
199 items					Operation							
Patch Name	Affected nodes	Business Group	Patch installatio...									
Microsoft Defender Antivirus	10.106.129.46 DESKTOP-TDNHHKD	[REDACTED]	2025-07-03 15:23:27		<input type="button" value="View Details"/>							
Microsoft Defender Antivirus	10.106.144.139 DESKTOP-BG0M8VJ	Default Business Group	2025-07-03 10:04:38		<input type="button" value="View Details"/>							
Microsoft Defender Antivirus	10.106.107.109 WIN11	Default Business Group	2025-07-03 08:52:09		<input type="button" value="View Details"/>							
Microsoft Defender Antivirus	100.64.1.108 DONGXIAOHUI-WINDOWSPC	dxb	2025-07-03 01:53:25		<input type="button" value="View Details"/>							
Microsoft Defender Antivirus	192.170.30.136 WIN-AJ67ET5T9IV	Default Business Group	2025-06-30 04:10:50		<input type="button" value="View Details"/>							
Windows Server 2008 R2 x64 Edition	10.106.110.74 WIN-48UNCO96JAE	Default Business Group	2025-06-24 11:24:31		<input type="button" value="View Details"/>							

6.2.1.4. Weak Password

This list shows the repair history records of weak passwords of the host.

steps:

- Displayed from the host dimension, you can view the affected applications and account names. Click the highlighted host IP value to pop up the corresponding details page.
- Click the "View Details" button to pop up the detailed information of the weak password of this host. You can view the basic information, repair information, and details of the weak password from it.
- The system supports batch export of the repaired weak passwords.

The screenshot shows the Sentry CWPP interface under the Risk Discovery tab, specifically the Host Remediation History section. The 'Weak Password' tab is selected. A table displays 68 items of repair history, with columns for Host, Affected Applications, Account name, Weak Password Type, MTTR, Repair time, and Operation. Each row includes a checkbox and a 'View Details' link. The data in the table is as follows:

Host	Affected Applications	Account name	Weak Password Type	MTTR	Repair time	Operation	
172.16.12.184 QT-PC	system	Guest	Disabled	Empty passwords	2025-07-03 10:00:04	1 minutes	View Details
172.16.12.184 QT-PC	system	Administrator	Disabled	Empty passwords	2025-07-03 10:00:04	1 minutes	View Details
10.106.107.109 WIN11	system	Guest	Disabled	Empty passwords	2025-07-03 10:00:04	1 minutes	View Details
10.106.107.109 WIN11	system	DefaultAccount	Disabled	Empty passwords	2025-07-03 10:00:04	1 minutes	View Details
10.106.107.109 WIN11	system	Administrator	Disabled	Empty passwords	2025-07-03 10:00:04	1 minutes	View Details
172.16.21.127 DESKTOP-QPC3G5L	system	qingteng	Active	The password is the same as the username	2025-07-03 10:00:03	1 minutes	View Details
172.16.21.127 DESKTOP-QPC3G5L	system	Guest	Disabled	Empty passwords	2025-07-03 10:00:03	1 minutes	View Details

6.2.2. Container Remediation History

This list displays the container weak password recovery history.

steps:

- Displayed from the container dimension, you can view the host where the container is located, the associated image, the affected applications, account names, etc. Click the highlighted data to pop up the corresponding details page.
- Click the "View Details" button to pop up the detailed information of the weak password of this container. You can view the basic information, repair information, and details of the weak

password from it.

- The system supports batch export of the repaired weak passwords.

Container	Contain...	Host location	Image	Cluster Names...	Affected ...	Acco...	Account St...	Weak Pass...	MTTR	Operation
sshd	-	10.106.121.14 k8s-node1	registry.qingteng.cn/4.0-test-vuls/sshd:weak...	-	SSH	test	Active	Common wea...	2025-06-25 16:00:00	View Details
k8s_ssh_depl...	-	10.106.110.182 k8s-01	sha256:cde878dabdb59098313a29a81a348...	default-d3fe32a28...	SSH	haha	Active	Common wea...	2025-04-25 10:00:00	View Details
k8s_ssh_depl...	-	10.106.110.182 k8s-01	sha256:cde878dabdb59098313a29a81a348...	182dih default	SSH	test	Active	Common wea...	2025-04-22 18:00:00	View Details
k8s_ssh_depl...	-	10.106.110.182 k8s-01	sha256:cde878dabdb59098313a29a81a348...	182dih default	SSH	momo	Active	Common wea...	2025-04-22 18:00:00	View Details
k8s_ssh_depl...	-	10.106.110.182 k8s-01	sha256:cde878dabdb59098313a29a81a348...	182dih default	SSH	lily	Active	Common wea...	2025-04-22 18:00:00	View Details
vigilant_mirza...	-	10.106.110.182 k8s-01	registry.qingteng.cn/hivetest/ctn-wpd-redis:4	-	Redis	-	Unknown	Common wea...	2025-04-22 16:00:00	View Details
vigilant_mirza...	-	10.106.110.182 k8s-01	registry.qingteng.cn/hivetest/ctn-wpd-redis:4	-	Redis	-	Unknown	Common wea...	2025-04-22 16:00:00	View Details
practical_noel...	-	172.16.22.86 host2286	registry.qingteng.cn/hivetest/ctn_detect_rbc...	-	SSH	test	Active	Common wea...	2025-04-22 16:00:00	View Details
practical_noel...	-	172.16.22.86 host2286	registry.qingteng.cn/hivetest/ctn_detect_rbc...	-	SSH	test	Active	Common wea...	2025-04-22 16:00:00	View Details
vigilant_mirza...	-	10.106.110.182 k8s-01	registry.qingteng.cn/hivetest/ctn-wpd-redis:4	-	Redis	-	Unknown	Common wea...	2025-04-22 15:00:00	View Details
vigilant_mirza...	-	10.106.110.182 k8s-01	registry.qingteng.cn/hivetest/ctn-wpd-redis:4	-	Redis	-	Unknown	Common wea...	2025-04-22 15:00:00	View Details
practical_noel	-	172.16.22.86 host2286	registry.qingteng.cn/hivetest/ctn_detect_rbc...	-	SSH	test	Active	Common wea...	2025-04-21 19:00:00	View Details

6.2.3. Cluster Remediation History

This list displays the remediation history records of the cluster.

steps:

- For each risk item, you can see the corresponding node and the cluster it belongs to. Click the highlighted position to pop up the corresponding details page.
- Click the "View Details" button to pop up the detailed information of the risk item. You can view the description, repair suggestions, repair information, and other information of the risk item from it.
- The system supports batch export of the repaired risk items.

Severity	Risk item name	Risk Features	Node	Belonging cluster	MTTR	Repair time	Operation
Medium	Calico Input Validation Vulnerability (C...)	hasRemoteExec	10.106.110.181 node181	default-8a006d5e25349163	2025-06-26 05:30:04	5 days	View Details
Medium	Containerd resource management erro...	hasRemoteExec	10.106.107.178 ids-performance	default-c45ae7f136226674	2025-05-21 05:30:10	23 days	View Details
Critical	Containerd Denial of Service vulnerabil...	-	10.106.107.178 ids-performance	default-c45ae7f136226674	2025-05-21 05:30:10	23 days	View Details
Medium	Containerd resource management erro...	-	10.106.107.178 ids-performance	default-c45ae7f136226674	2025-05-21 05:30:10	23 days	View Details
High	Containerd Information Disclosure Vuln...	hasRemoteExec	10.106.107.178 ids-performance	default-c45ae7f136226674	2025-05-21 05:30:10	23 days	View Details
High	Docker runc Container Escape Vulnerab...	hasRemoteExec	10.106.107.178 ids-performance	default-c45ae7f136226674	2025-05-21 05:30:10	23 days	View Details
Medium	Docker containerd Container Escape V... ...er...	hasPoc	10.106.107.178 ids-performance	default-c45ae7f136226674	2025-05-21 05:30:10	23 days	View Details

6.3. Risk Detection

The system supports periodic risk detection for hosts, containers, clusters, and node mirror objects. It allows users to view historical execution records to promptly identify and report various risk issues such as vulnerabilities, patches, and weak passwords. Moreover, it enables users to flexibly configure detection policies and detection tasks according to different business requirements.

6.3.1. Task List

Detection tasks include system - preset periodic detection, that is, performing a global risk scan on user assets periodically to achieve continuous detection and discovery of asset risk issues. At the same time, you can also flexibly customize detection tasks.

6.3.1.1. Custom

You can customize the selection of the execution cycle, detection strategy, and detection scope to perform irregular and personalized scans on assets.

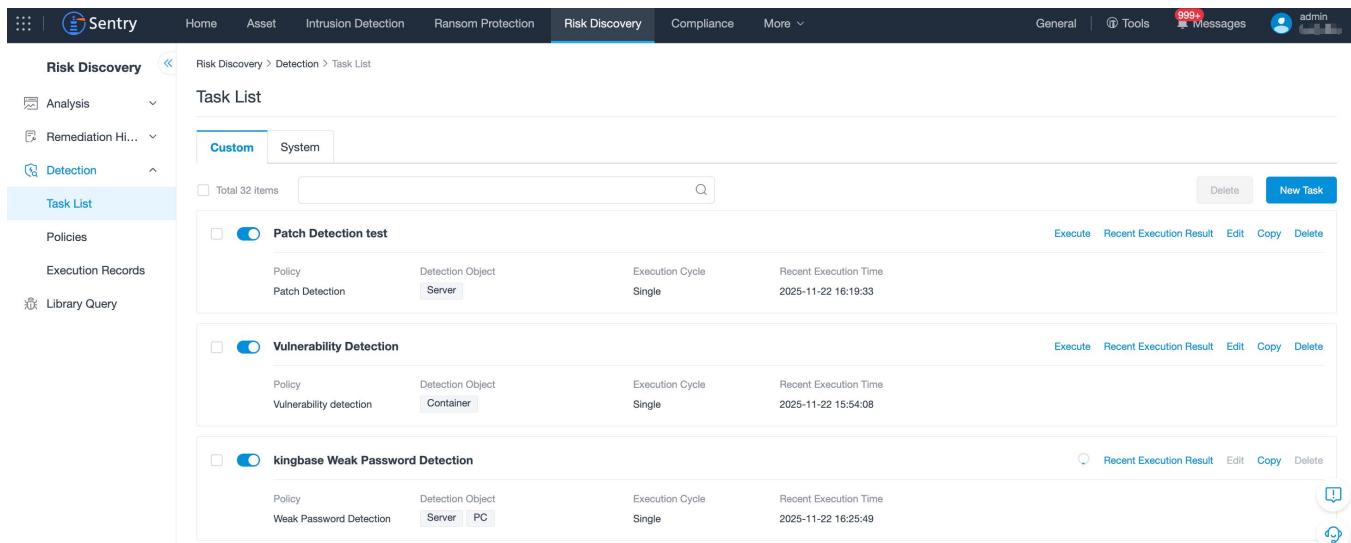
General Search: The system has set up a general search box, which supports unified retrieval of task status, task name, detection strategy, detection object, execution cycle, creation time, and latest execution time.

Page Display: Displayed in the form of tasks, each task displays one piece of data, including the task

name, strategy, detection object, execution cycle, and latest execution time.

steps:

- Click the "New Task" button on the custom task page, enter basic information, and select strategy configuration.
- For all custom tasks, you can edit, copy, delete the task, and view the latest execution result of the task by clicking buttons.
- You can click any one of them to view the details of the task.
- If you want to execute a certain task immediately, you can also directly click the "Execute" button.
- Click the  button, and you can switch the on/off status of the task by yourself.



The screenshot shows the Sentry CWPP interface with the Risk Discovery tab selected. On the left, there's a sidebar with categories like Analysis, Remediation History, Detection, Task List (which is currently selected), Policies, Execution Records, and Library Query. The main area is titled 'Task List' and shows three entries:

Task Name	Policy	Detection Object	Execution Cycle	Recent Execution Time	Action Buttons
Patch Detection test	Patch Detection	Server	Single	2025-11-22 16:19:33	Execute Recent Execution Result Edit Copy Delete
Vulnerability Detection	Vulnerability detection	Container	Single	2025-11-22 15:54:08	Execute Recent Execution Result Edit Copy Delete
kingbase Weak Password Detection	Weak Password Detection	Server / PC	Single	2025-11-22 16:25:49	Recent Execution Result Edit Copy Delete

New Task

New Task

Basic Information

* Task N... : Please enter the name of the risk detectio

Task Des...: Please enter a description

Execution...: Once Daily Weekly Expression

Task Sta...: Enable

Policy Configuration

* Detecti... : Please select



Select the detection strategy first for advanced configuration



Cancel

Save

Save and Execute

- Task Name: Fill in manually.
- Task Description: Fill in manually.
- Execution Cycle: Select One - time/Daily/Weekly/Expression.
 - Daily: Need to select the start time.

Execution...: Once Daily Weekly Expression

Start Time 00:00

-

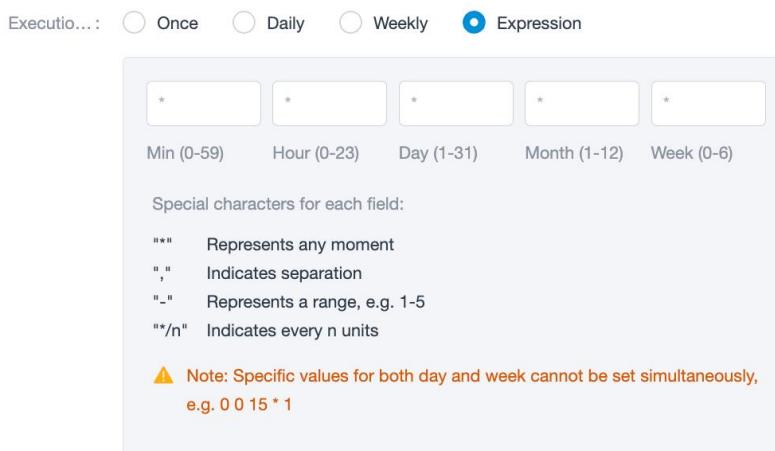
- Weekly: Need to select the date and start time.

Execution...: Once Daily Weekly Expression

Sun Mon Tues Wed Thur Fri Sat

Start Time 00:00

- - Expression: Need to fill in a custom cycle.



- Task Status: Select On/Off.
- Detection Strategy: Weak Password Detection/Vulnerability Detection/Patch Detection/Cluster Risk.
- Detection Scope: Select according to the detection scope supported by the detection strategy.

Instructions:

- Maximum Scanning Duration: Controls the upper limit of the execution time for detection tasks. If the actual detection time exceeds the maximum scanning duration, the task scanning will time out. The task execution result will only update the data of the completed scanning part, and the unscanned data will not be updated.
- Creating custom tasks for node image risks is not supported.
- After a task is dispatched, the "Execute" button remains in a loading state, and consecutive task dispatches are not allowed until the previous task is completed.
- Custom tasks are not subject to the limit of a maximum of 10 tasks in the execution queue.

Latest Execution Results

The interface mainly consists of four parts: Basic Information, Execution Status, Execution Results,

and Result List.

- **Basic Information:** Task name, creation time, latest execution time, inspection duration, execution status, detection scope
- **Execution Status:** Displays the execution results of the latest execution record of the task, including the number of successful, failed, and offline hosts. If there are failures, you can view the failure list. Weak password detection will have an additional account scanning progress, and you can view the details of the weak password scanning progress. Click the “Execution Records” button to view the historical execution records of the task within the past 180 days.
- **Execution Results:** Displays the latest detection results of the task, summarized by critical, high, medium, and low risks. Weak password detection is an exception, which displays the account status of the latest execution results of the task, summarized by enabled, disabled, and unknown.
- **Result List:** Displays the detailed list of the results of this task scan.

(1) Vulnerability Detection

The screenshot shows the Sentry CWPP Risk Discovery interface. The main title is "Vulnerability Detection-2025-11-22 15:54:08-Execution Result". The "Task List" tab is selected in the sidebar. The "Execution Result" section shows the following summary:

Success	Failure	Number of Offline Hosts	Critical	High	Medium	Low
16	0	29	54	209	56	1

The "Vulnerability List" section displays a table with 320 items. The columns include ID, Severity, Vulnerability Name, Risk Features, Affected Apps, Detection Method, and Number of A... . Some rows are highlighted with blue borders. The first few rows are:

ID	Severity	Vulnerability Name	Risk Features	Affected Apps	Detection Method	Number of A...
QTV-2021-00...	Critical	Grafana Authentication Bypass Vulnerability (CVE-2021-...)	hasRemoteExec	Grafana	VersionComparison	1
QTV-2022-03...	High	Nginx ngx_mp4_module buffer overflow vulnerabilit...	-	Nginx	VersionComparison	10
QTV-2021-00...	High	XStream <=1.4.17 Deserialization Remote Code Executio...	hasRemoteExec	XStream	VersionComparison	2
QTV-2023-00...	High	Tomcat Injection Vulnerability (CVE-2022-45143)	hasRemoteExec	Tomcat	VersionComparison	1

(2) Patch Detection

Risk Discovery

Patch Detection test-2025-11-22 16:19:33-Execution Result

Basic Information

- Creation Time: 2025-11-22 16:19:35
- Recent Execution Time: 2025-11-22 16:19:33
- Inspection Duration: 24 seconds
- Execution Status: Completed
- Detection Scope: Server

Execution Environment		Execution Result					
Success	Failure	Number of Offline Hosts		Critical	High	Medium	Low
27	0	60		377	1822	842	65

Patch List

ID	Severity	Patch Name	Risk Features	Affected Assets	Business Group	Business Status	First discovery time	Operation
4861ab0d...	Critical	2025-04 Cum...	hasKernel	172.16...	Default Business G...	Unspecified	2025-11-21 18:54:06	View Details
QT01202...	High	CentOS 8 : les...	-	192.16...	Default Business G...	No	2025-07-29 16:16:00	View Details
QT01202...	Medium	CentOS 8 : sa...	hasRemoteExec	192.16...	Default Business G...	No	2025-07-29 16:16:00	View Details
QT01202...	High	CentOS 8 : ed...	hasExp	192.16...	Default Business G...	No	2025-11-01 03:30:14	View Details

(3) Cluster Risk

Risk Discovery

dxtest-2025-07-31 09:35:57-Execution Result

Basic Information

- Creation Time: 2025-07-22 18:41:42
- Recent Execution Time: 2025-07-31 09:35:57
- Inspection Duration: 15 seconds
- Execution Status: Completed
- Detection Scope: All Hosts

Execution Environment		Execution Result					
Success	Failure	Number of Offline Hosts		Critical	High	Medium	Low
9	1	11		7	25	17	0

Cluster Risk List

Total 49 Items	Severity	Risk item name	Risk Type	Risk Item Category	Check Node Type	Risk Features	Affected Clusters	Affected Nodes
49	High	Docker runc Container Escape Vulnerability...	Privilege Escalation	Docker	TARGET_ALL	hasRemoteExec	0	2
49	High	runc privilege escalation vulnerability (CVE-...)	Path Traversal	Docker	TARGET_ALL	-	0	1
49	Critical	Docker privilege bypass vulnerability (CVE-...)	HTTP Request/Respon...	Docker	TARGET_ALL	hasRemoteExec	1	2
49	High	Kubernetes API Server SSRF Vulnerability (...)	Server-Side Request F...	K8S	TARGET_MASTER	hasRemoteExec	1	1
49	Medium	Kubernetes kubectl cp Directory Traversal V...	Path Traversal	K8S	TARGET_ALL	hasRemoteExec	1	2

(4) Weak Password Detection

The screenshot shows the Sentry CWPP Risk Discovery interface. The main title is "kingbase Weak Password Detection-2025-11-22 16:25:49-Execution Result". Below it, the "Basic Information" section shows creation time (2025-10-20 14:30:54), recent execution time (2025-11-22 16:25:49), inspection duration (43 seconds), and execution status (Completed). The "Execution Environment" section displays success (30), failure (0), number of offline hosts (78), account scanning progress (100%), disabled (12), active (41), and undefined (1). The "Execution Result" section shows a table with three items: OpenLDAP (1 weak password), system (23 weak passwords), and SSH (30 weak passwords). The "Weak Password List" section provides a detailed view of these findings.

Affected Applications	Number of Weak Passwords
OpenLDAP	1
system	23
SSH	30

6.3.1.2. System

Periodic detection preset by the system. The detection objects include PC hosts, Server hosts, containers, images, and clusters. The detection strategies are template strategies (vulnerability detection, patch detection, weak password detection, node image risk, cluster risk).

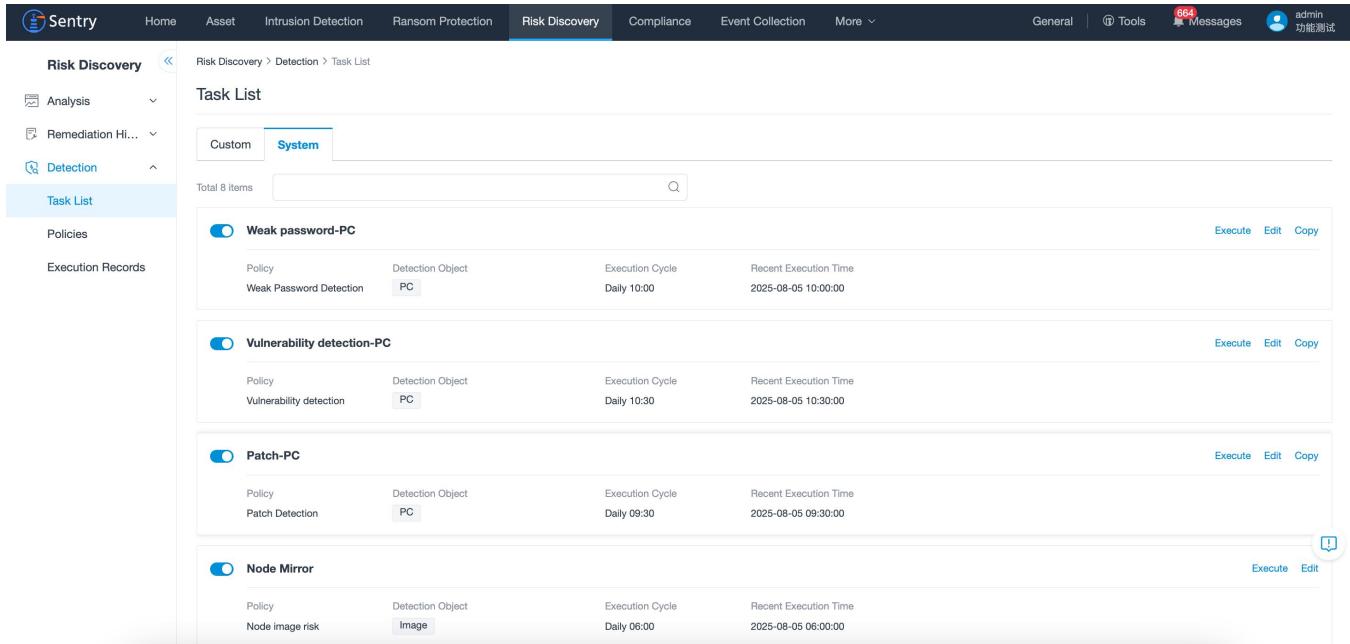
General Search: The system has set up a general search box, which supports unified retrieval of task status, task name, detection strategy, detection object, execution cycle, creation time, and latest execution time.

Page Display: Displayed in the form of tasks, each task displays one piece of data, including the task name, strategy, detection object, execution cycle, and latest execution time.

steps:

- You can click any one of them to view the task details and execution records.
- For the preset tasks of vulnerability detection, patch detection, weak password detection, and cluster risk, you can edit and copy the tasks by clicking buttons. For the preset tasks of node image risk, you can only edit the tasks by clicking buttons.
- If you want to execute a certain task immediately, you can directly click the "Execute" button.

- Click the  button, and you can switch the on/off status of the strategy by yourself.



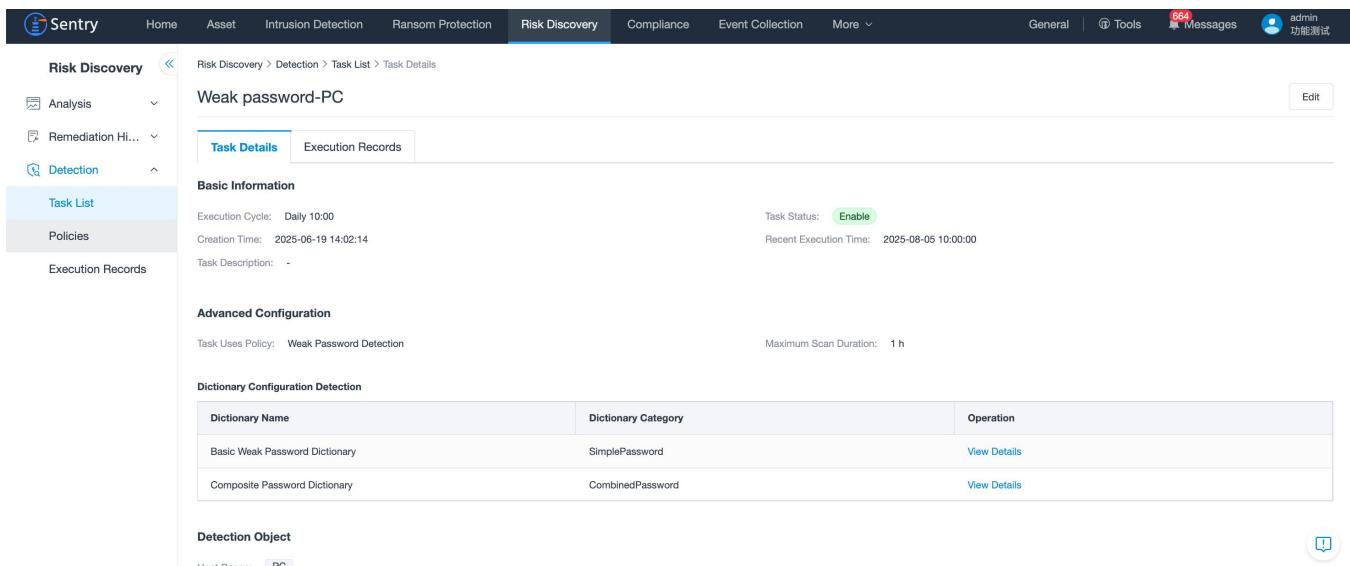
The screenshot shows the Sentry CWPP interface under the Risk Discovery tab. On the left sidebar, the 'Task List' option is selected. The main area displays a 'Task List' with four entries:

- Weak password-PC**: Policy: Weak Password Detection, Detection Object: PC, Execution Cycle: Daily 10:00, Recent Execution Time: 2025-08-05 10:00:00. Buttons: Execute, Edit, Copy.
- Vulnerability detection-PC**: Policy: Vulnerability detection, Detection Object: PC, Execution Cycle: Daily 10:30, Recent Execution Time: 2025-08-05 10:30:00. Buttons: Execute, Edit, Copy.
- Patch-PC**: Policy: Patch Detection, Detection Object: PC, Execution Cycle: Daily 09:30, Recent Execution Time: 2025-08-05 09:30:00. Buttons: Execute, Edit, Copy.
- Node Mirror**: Policy: Node image risk, Detection Object: Image, Execution Cycle: Daily 06:00, Recent Execution Time: 2025-08-05 06:00:00. Buttons: Execute, Edit.

Instructions:

- Only users with the admin role have editing permissions for the system's scheduled tasks.
- After a task is dispatched, the "Execute" button remains in a loading state, and consecutive task dispatches are not allowed until the previous task is completed.
- Scheduled tasks are exempt from the limit of a maximum of 10 pending tasks in the queue.

Task Details



The screenshot shows the Sentry CWPP interface under the Risk Discovery tab, specifically for the 'Weak password-PC' task. The left sidebar shows the 'Task List' option is selected. The main area displays 'Task Details' for the 'Weak password-PC' task:

Basic Information

Execution Cycle:	Daily 10:00	Task Status:	Enable
Creation Time:	2025-06-19 14:02:14	Recent Execution Time:	2025-08-05 10:00:00
Task Description:	-		

Advanced Configuration

Task Uses Policy:	Weak Password Detection	Maximum Scan Duration:	1 h
-------------------	-------------------------	------------------------	-----

Dictionary Configuration Detection

Dictionary Name	Dictionary Category	Operation
Basic Weak Password Dictionary	SimplePassword	View Details
Composite Password Dictionary	CombinedPassword	View Details

Detection Object

Host Range:	PC
-------------	----

Execution Records

The screenshot shows the Sentry CWPP Risk Discovery interface. On the left, there's a sidebar with navigation links: Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery (which is selected), More, General, Tools, Messages (with 999+ notifications), and a user profile for admin. The main area is titled "Risk Discovery > Detection > Task List > Task Details" for a "container vulnerability". It has tabs for "Task Details" and "Execution Records" (which is currently selected). A search bar says "Please select filter content" with a magnifying glass icon. Below is a table with 30 items, each row representing a task execution. The columns are: Task Trigger ..., Task Name, Task Type, Policy, Detection Object, Detection T..., Task start time, and Operation. The rows show various dates from December 16 to 24, 2025, with "container vulnerability" as the task name and "Container" as the detection object. Each row has a small edit icon (pencil) and a delete icon (trash can).

Task Trigger ...	Task Name	Task Type	Policy	Detection Object	Detection T...	Task start time	Operation
2025-12-24 04:40:00	container vulnerability	System Pres...	Vulnerability d...	Container	Container Ris...	2025-12-24 04:40:00	End Task View Failed Item
2025-12-23 04:40:00	container vulnerability	System Pres...	Vulnerability d...	Container	Container Ris...	2025-12-23 04:40:00	End Task View Failed Item
2025-12-22 04:40:00	container vulnerability	System Pres...	Vulnerability d...	Container	Container Ris...	2025-12-22 04:40:00	End Task View Failed Item
2025-12-21 04:40:00	container vulnerability	System Pres...	Vulnerability d...	Container	Container Ris...	2025-12-21 04:40:00	End Task View Failed Item
2025-12-20 04:40:00	container vulnerability	System Pres...	Vulnerability d...	Container	Container Ris...	2025-12-20 04:40:00	End Task View Failed Item
2025-12-19 04:40:00	container vulnerability	System Pres...	Vulnerability d...	Container	Container Ris...	2025-12-19 04:40:00	End Task View Failed Item
2025-12-18 04:40:00	container vulnerability	System Pres...	Vulnerability d...	Container	Container Ris...	2025-12-18 04:40:00	End Task View Failed Item
2025-12-17 04:40:00	container vulnerability	System Pres...	Vulnerability d...	Container	Container Ris...	2025-12-17 04:40:00	End Task View Failed Item
2025-12-16 04:40:00	container vulnerability	System Pres...	Vulnerability d...	Container	Container Ris...	2025-12-16 04:46:31	End Task View Failed Item

6.3.2. Policies

The system has preset various types of risk detection template policies, including cluster risk, patch detection, vulnerability detection, and weak password detection.

It also supports users to select different detection rule contents to build custom detection policy templates according to business needs. Among them:

- Custom policies only support two policy types: vulnerability and weak password.
- Vulnerability detection supports custom selection of detection items.
- Weak password detection supports custom selection of applications.

steps:

- On the policy management page, click "Add Custom Policy", select the policy type, and add detection items.
- For an existing custom policy, if you want to edit it, click the button.
- For an existing custom policy, if you want to delete it, click the button.
- For both template policies and custom policies, you can quickly create a new detection task

for the policy by clicking the "New Task" button on the corresponding policy.

New Custom Policy

(1) Vulnerabilities: Select Detection Items

The screenshot shows a modal dialog titled "Add Detection Item". On the left, there's a sidebar with fields for "Policy Name" (Please enter the name), "Policy Description" (Please enter the description), and "Policy Type" (radio buttons for POC and WeakPassword, with POC selected). Below these is a "Detection Strategy Configuration" section with a "Detection Items" tab selected. The main area contains a table titled "Add Detection Item" with the following columns: "Detection Item Name", "Vulnerability Type", "Detection Method", and "Vulnerability Reference". A search bar at the top of the table says "Please select filter content". The table lists 990 items, with the first few entries being:

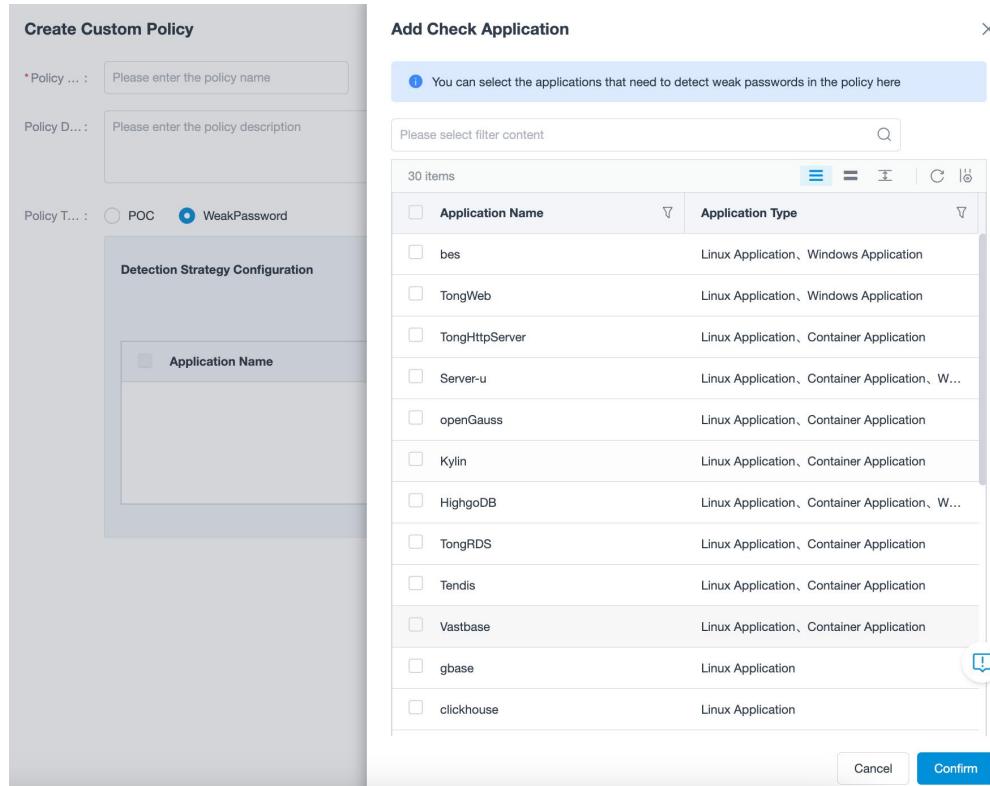
Detection Item Name	Vulnerability Type	Detection Method	Vulnerability Reference
Vite [REDACTED]	Sens... +1	VersionCompar...	2025-03-24
Oracle WebLogic Server [REDACTED]	Permission a...	VersionCompar...	2025-07-15
Ingress Nginx [REDACTED]	Input Validati...	VersionCompar...	2025-03-24
Ingress Nginx [REDACTED]	Input Validati...	VersionCompar...	2025-03-24
Tomcat [REDACTED]	Resource Ma...	VersionCompar...	2025-07-10
Tomcat [REDACTED]	Race Condition	VersionCompar...	2025-07-10
Oracle WebLogic Server Denial of Service V...	Denial of Serv...	VersionCompar...	2025-07-15
Apache Kafka Client [REDACTED]	Server-Side R...	Condition	2025-06-10
Apache Batik [REDACTED]	Server-Side R...	VersionCompar...	2022-09-22
H2Console Parameter Injection Vulnerability	Injection Vuln...	VersionCompar...	2022-01-19
XStream [REDACTED]	OS Command...	VersionCompar...	2013-12-22
GeoServer XML [REDACTED]	Serv... +1	VersionCompar...	2025-06-10

At the bottom of the table, it says "990 items" and has a page navigation bar with buttons for 1, 2, 3, 4, 5, ..., 20, >, and "50 Item/Page". Below the table are "Cancel" and "Confirm" buttons.

(2) Weak Passwords: Select Detection Applications

The screenshot shows a modal dialog titled "Detection Strategy Configuration". At the top, there are radio buttons for "Policy Type": "POC" (unchecked) and "WeakPassword" (checked). Below this is a "Select Detection Application" button. The main area is a table with three columns: "Application Name", "Application Type", and "Operation". The table header says "No Data".

Application Name	Application Type	Operation
No Data		



6.3.3. Execution Records

This feature displays the historical records and execution status of detection tasks for host risks, container risks, and cluster risks within the past 180 days.

Statistical Cards: The system provides three statistical boards (Task Execution Completed, Task Execution Failed, Task Pending Execution) to show the total number of tasks in different execution states at a glance.

Universal Search: The system includes a universal search box, supporting unified retrieval across multiple filter options such as task name, task type, policy, detection type, execution status, and task start time.

steps:

- In this feature, you can query all detection tasks (for host, container, and cluster risks) from the past 180 days. Tasks are categorized into three types: Quick Scan, Custom Task, and System Scheduled Task. Tasks initiated from the risk analysis page are Quick Scans; tasks

configured in the detection task feature are Custom Tasks and System Scheduled Tasks.

- Tasks of the same detection type will enter the queue and be processed in the order of their trigger time, with the execution status marked as "Queuing".
- You can click the highlighted task name to jump to the detection task page, then click the "End Task" button in the action bar corresponding to the listed data. For manually terminated tasks, the execution status will be updated to "Failed"; if there are "Queuing" tasks in the queue, they will automatically start executing in sequence.
- You can click the "View Details" button in the action bar of a Custom Task or System Scheduled Task to check the task details and latest execution results.
- If there are failures in the execution results, you can click the "View Failed Items" button in the action bar to view the list of failed execution objects in the side window.

Risk Discovery > Detection > Execution Records

Execution Records

View history of on-demand scans initiated from the host, container, and cluster risk pages, including scan execution status and results

Task execution completed	Task execution failed	Task pending execution
5015	216	0

Please select filter content

Task Trigger ...	Task Name	Task Type	Policy	Detection Object	Detection T...	Task start time	Operation
2025-12-24 11:24:00	Weak Password	System Prese...	Weak Passwo...	Server	Host Risk_We...	2025-12-24 11:24:00	End Task View Failed Item
2025-12-24 11:22:00	container weak password	System Prese...	Weak Passwo...	Container	Container Ris...	2025-12-24 11:22:00	End Task View Failed Item
2025-12-24 09:30:01	-PC-2025-12-01 2...	Custom	Patch Detection	PC	Host Risk_Pat...	2025-12-24 09:30:36	End Task View Failed Item
2025-12-24 09:30:00	Patch-PC	System Prese...	Patch Detection	PC	Host Risk_Pat...	2025-12-24 09:30:00	End Task View Failed Item
2025-12-24 04:40:00	- 2025-12-01 2...	Custom	Vulnerability d...	Container	Container Ris...	2025-12-24 04:45:31	End Task View Failed Item
2025-12-24 04:40:00	container vulnerability	System Prese...	Vulnerability d...	Container	Container Ris...	2025-12-24 04:40:00	End Task View Failed Item

5231 items

The screenshot shows the Sentry CWPP web interface. On the left, there's a sidebar with navigation links: Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery, Analysis, Remediation History, Detection, Task List, Policies, Execution Records (which is currently selected), and Library Query. The main area is titled 'Risk Discovery > Detection > Execution Records' and displays 'Execution Records' with a count of 5015 completed tasks and 216 failed tasks. Below this, there's a table with columns for Task Trigger, Task Name, and Task Type, showing various scheduled tasks like 'Patch' and 'Weak Password'. To the right, a modal window titled 'List of Failed Objects' shows a single entry: '10.106' with a failure reason of 'Agent script execution failed'. There are also icons for a warning and a refresh.

6.4. Library Query

With the Library Query function, you can use the filter options to query whether the vulnerability patches within a specified range are supported in the rule database of the Qingteng Host Security Platform.

Page Display: You can see the total number of rules supported by the current vulnerability database for detection on the main query page.

General Search: The system has set up a general search box, which supports searching by risk level, risk item name, CVE number, CNNVD number, risk characteristics, and release time.

Steps:

- Fill in the filter options to be queried, and separate multiple filter options with the Enter key.
After completion, click the button to search.
- If it exists, the basic information of the corresponding risk item will be displayed. You can click the "View Details" button to see the detailed information of the risk item, including description, repair suggestions, reference information, CVSS score, etc.

- If it does not exist, no data will be returned.

Risk Discovery Risk Discovery > Library Query

- Analysis
- Remediation Hi...
- Detection
- Library Query**

Vulnerability Database Search

You can search the vulnerability database here, with basic information available for 140001 vulnerabilities

Q

Risk Discovery Risk Discovery > Library Query > Library Query Result

Library Query Result

CVE Number: CVE-2024-...

⚠ Total of 1 items; up to 500 filtered results displayed. You can refine the results by adding more filter criteria.

Severity	Risk Item name	CVE Number	CNNVD number	Risk Features	Release Time	Operation
Critical	Windows TCP/IP [REDACTED]	CVE-2024-38063	CNNVD-202408-1091	hasRemoteExec	2024-08-13 00:00:00	View Details

1 items

Critical Windows TCP/IP [REDACTED] (CVE-2024-38063) X

Description

Microsoft Windows TCP/IP [REDACTED] <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063>
Microsoft Windows TCP/IP [REDACTED] : <https://www.catalog.update.microsoft.com/>

ID: QTV-2024-025505
Release ... : 2024-08-13
Vulnerabil...: [REDACTED]
Risk Feat...: hasRemoteExec

Repair Suggestions

[REDACTED] <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063>
[REDACTED] : <https://www.catalog.update.microsoft.com/>

Reference Information

CVE	CWE	CNVD	CNNVD
CVE-2024-38063	CWE-191	-	CNNVD-202408-1091

CVSS Score: 9.8

Attack Vector
Availability
Integrity
Confidentiality
Privileges
User Interaction
Impact Scope

Note: A maximum of 500 results will be displayed for each query. It is recommended to narrow down and refine the query results by adding more filtering conditions.

7. Compliance

The security baseline is the minimum security guarantee of an information system, which refers to the basic security requirements that the information system needs to meet. Information system security often requires a balance between the cost of security and the security risks that can be tolerated, and the security baseline is the reasonable boundary of this balance. If the most basic security requirements of the system are not met, the resulting security risks cannot be borne, and it will also result in excessive security costs. Therefore, constructing an information system security baseline has become the primary step in system security engineering, as well as a prerequisite for conducting security assessments and solving information system security issues.

7.1. Baseline Check

Baseline check is a baseline check job created by the user. Each inspection task is a task based on multiple baseline rules for a batch of hosts.

General Search: The system has set up a general search box, supporting unified retrieval of baseline inspection tasks according to different conditions.

Quick Filtering: The system lays out four key option categories and filter values, namely baseline type, inspection environment, inspection object, and inspection method, facilitating users to trigger result filtering with one-click and quickly.

List Display: Baseline inspection tasks are displayed in the form of cards. You can view information such as task name, task execution result pass rate, inspection scope, inspection baseline type, inspection environment, and inspection object.

Baseline Type	Check Environment	Check Object	Check mode
等保合规	49 Linux	47 System	53 One-time Check
Container Security	29 Windows	21 Application	25 Scheduled Check
CIS合规	26 Container	31 Image	9 119
集群合规	20 Orchestration	23 Docker Host	7
安全实践	21	Docker Container	19

Total 122 items

<input type="checkbox"/> test123 Cybersecurity Compliance Linux Application	26.3% Check scope 10.106.144.223 k8s-node1 +1 items	Last run time 2025-11-21 14:53:14	Next run time -	Creation Time 2025-11-19 19:28:14
<input type="checkbox"/> test-container Container Security Container Image	0% Check scope	Last run time -	Next run time -	Creation Time 2025-11-18 20:57:07

steps:

- If you want to create a new inspection task, you can click the "New Inspection" button or quickly create it in Baseline Configuration - New Inspection.
- You can control whether it is a single task or a scheduled inspection task by checking the cycle. If it is a periodic task, there will be an icon on the task card.
- If you want to immediately perform a certain inspection task to view the results, you can also click .
- After execution, the page will display the execution result pass rate of this task. Among them:
 - When the pass rate is $\geq 90\%$, the statistical chart displays in green.
 - When the pass rate is between 60% and 90%, the statistical chart is displayed in yellow.
 - When the pass rate is less than 60%, the statistical chart displays in red.
- You can also edit, delete, and export existing inspection tasks.
- If you want to view the details of the inspection task results, you can directly click on a single piece of data to enter the details page, which displays various statistics and detailed data of the inspection results.

- According to different inspection environments and inspection objects, the system provides different views of inspection results and can view the details of each result.

Among them:

- In the Linux/Windows inspection environment, the baseline view and the host view are displayed.
 - Baseline View: Statistical analysis is performed from the baseline dimension, showing all inspection items of the baseline and the pass rate of the selected host under each item.
 - Host View: Statistical analysis is performed from the host dimension, showing the pass rate of each baseline and all inspection items within the baseline under the selected host.
- In a container environment, display inspection item views and host/container/image views separately based on the different inspection objects.
 - Inspection item view: Statistics are conducted from the perspective of inspection items, listing all inspection items of the baseline and the pass rate of the selected inspection objects under each item.
 - Host view: Statistically display all hosts under the baseline and the pass/fail status of inspection items on each host from the host dimension.
 - Container view: Statistically display all containers under the baseline and the pass/fail status of inspection items in each container from the container dimension.

- Image view: Statistically display all mirrors under the baseline and the pass/fail status of inspection items in each mirror from the mirror dimension.
- Display the inspection item view and resource object view in the orchestration environment.
- Inspection item view: Statistics are conducted from the perspective of inspection items, listing all inspection items of the baseline and the pass rate of the selected cluster resource objects under each item.
- Resource Object View: Statistically display the relevant information of resource objects under the baseline and the pass/fail status of selected inspection items on each object from the dimension of resource objects.
- On this detail page, you can also edit, export, and execute the inspection task.

Check Item count	Passed Items	Not Passed Items	Failed Items	Total Hosts Checked	Compliant Hosts	Non-compliant Hosts	Failed Hosts
19	5	14	0	1	0	1	1

Importance	Check Item Name	Type	Reference Rules	Pass Rate	Operation
Minor	Check if Apache is configured to wait for 1...	Residual Information Protection	-	0%	View Details
Minor	Check if the default port has been changed	Access Control	-	0%	View Details
Minor	Check if the log recording format is config...	Security Audit	-	100%	View Details

Credential Management

Credentials management is used to centrally manage various login credentials required for baseline

checks, currently covering credentials for MySQL and Weblogic in host applications.

For example, during the baseline check process, when it is necessary to check items such as "Check whether to delete the test library installed for testing" in the MySQL application baseline, it is necessary to access the database and therefore rely on the user password of the database. And these user passwords can be uniformly managed and stored in the "credential management" system.

steps:

- The security requirements for this feature are high, and you need to verify the password of your system account in order to access "Credential Management" function
- If you want to add credentials, first select the application to be used as the sidebar, then click "Add credentials", fill in the relevant information such as the scope of application, database username, password, port, etc. to complete the addition. When the scope of application includes added credentials, the added credentials will be updated.
- You can also import credentials directly from external sources, click the "Add Credentials" button, fill in the import template content according to the functional specifications, and then select the file to complete the import.
- For added credentials, the system supports editing and deleting.

The screenshot shows the Sentry CWPP web interface. The top navigation bar includes links for Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery, Compliance (which is selected), and More. On the far right, there are links for General, Tools, Messages (with 999+ notifications), and a user icon for admin. The left sidebar has sections for Compliance, Baseline Check (selected), and Baseline Manager. The main content area is titled 'Compliance > Baseline Check > Credential' under 'MySQL'. It shows a table with one item: Host 10.106.10.106, Port 30, Username RO, Last update time 2025-11-04 16:58:11, Operator admin. There are buttons for Delete, Import credentials, and Add credentials. At the bottom, there are pagination controls for 1 item and 50 Item/Page.

7.2. Baseline Management

Baseline Template Configuration supports customizing baseline templates.

7.2.1. Baseline Template Configuration

7.2.1.1. System Preset

This function displays the baseline templates configured by the product's internal operation platform, which are preset by the system. Such baseline templates only support creating new checks and creating copies, and do not support modification.

General Search: The system has set up a general search box, which supports unified retrieval of baseline information according to different conditions.

Quick Filtering: The system arranges three key filtering items, namely baseline type, inspection environment, and inspection object, along with their filtering values, facilitating users to trigger result filtering with one-click quickly.

List Display: It displays the baseline templates preset by the system, where you can view basic information such as baseline name, inspection environment, inspection object, and the number of inspection items.

The screenshot shows the Sentry CWPP interface under the Compliance tab, specifically the Baseline Management section. It displays a list of baseline types: Container Security, Linux, Windows, Container, Orchestration, System, Application, Image, Docker Host, Docker Container, and others. Below this, two specific baseline templates are shown in cards:

- test-log-test-log-1**: Linux, System. Details: Check Object: System, Operating System: Unlimited, CPU Architecture: No Limit, Application: -, Number of Check Items: 1.
- test-log-test-log**: Linux, System. Details: Check Object: System, Operating System: Unlimited, CPU Architecture: No Limit, Application: -, Number of Check Items: 3.

Steps:

- Click on a single baseline template card to jump to the baseline template details page, where you can view the baseline information and the details of the included inspection items.

The screenshot shows the Sentry CWPP interface under the Compliance tab, specifically the Baseline Management section, with the Baseline Template Detail view for the "Classified Protection Ubuntu 24 System Baseline Check".

Basic Information

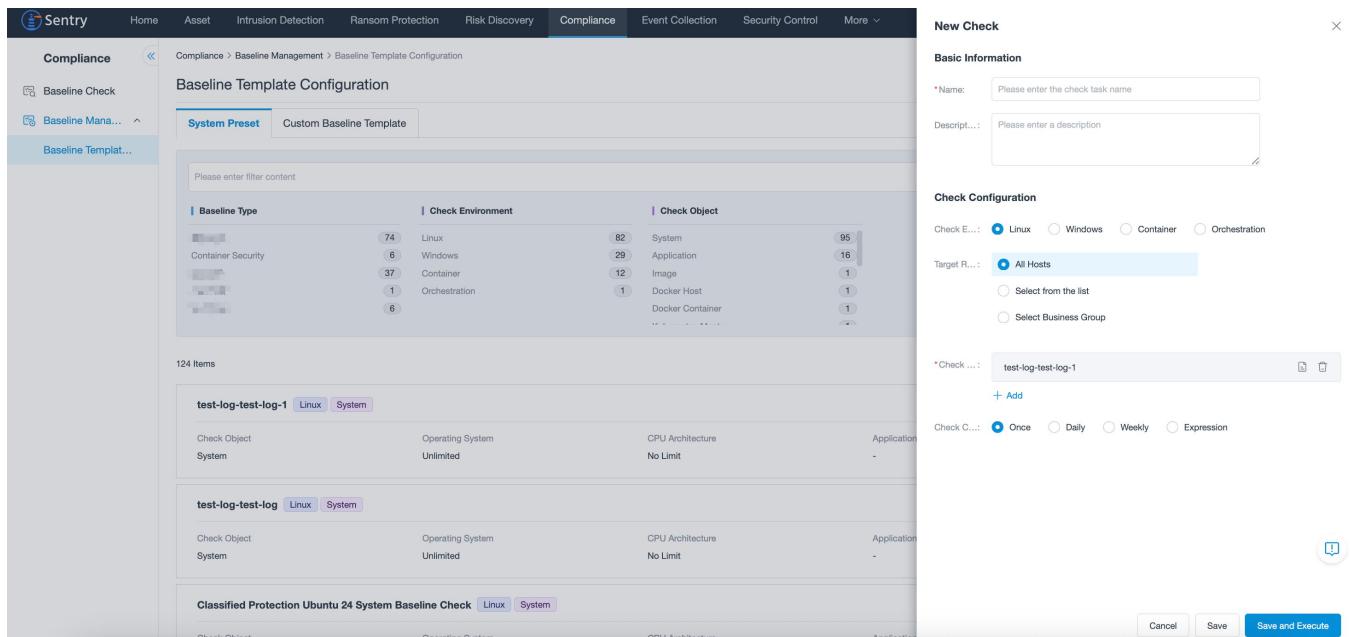
- Baseline Type: Cybersecurity Compliance
- Operating System: Ubuntu 24.04,Ubuntu 24.10
- Check Object: Linux
- CPU Architecture: No Limit
- Check ...: System
- Whether ...: Non-Innovation

Check Item

Importance	Category	Check Item Name	Type	Check Item Description	Customization ...
Major	System Preset	Check if the system account is disabled	Access Control	System accounts are for internal use only, not for logging into ...	No
Major	System Preset	Check if the audit log file permissions are set	Security Audit	Audit information (audit records, audit settings, audit reports) ...	No
Major	System Preset	Check if the permissions for /etc/shadow are configured.	Access Control	The /etc/shadow file is used to store critically important inform... No	
Major	System Preset	Check if the syslog service is enabled.	Security Audit	Enable syslog system log auditing function	No
Major	System Preset	Check if the user's home directory permissions are 750 or stri...	Access Control	Although the system administrator can set security permission...	No
Major	System Preset	Check if the account using the su command is restricted	Access Control	The su command is used to switch between different account... No	
Major	System Preset	Check if the ssh public and private key file permissions are co...	Access Control	SSH private key is one of the two files used in SSH public key ... No	
Major	System Preset	Check if the permissions for /etc/passwd are configured.	Access Control	The /etc/passwd file contains user account information used b... No	
Major	System Preset	Check if root is the only user with UID 0.	Identity Authentication	Any account with a UID of 0 has superuser privileges on the s... No	
Major	System Preset	Check if duplicate UIDs do not exist.	Identity Authentication	Although the useradd program does not allow the creation of ... No	

- If you want to initiate an inspection for a baseline template, click the "Create Inspection" button. In the pop-up page, fill in the basic information of the task and select the inspection configuration. After filling in, you can click the "Save and Execute" button to execute the task and view the task results under the [Baseline Inspection] function. You can also click the "Save" button to only save the task without executing it temporarily.

- Click the  button after the inspection baseline to jump to a new page to view the details of this baseline template.
- If you want to delete this baseline, click the  button.
- If you want to add other inspection baselines, click the  **添加** button.



The screenshot shows the Sentry CWPP interface. On the left, there's a sidebar with 'Compliance' selected. Under 'Compliance', 'Baseline Check' is active. In the main area, 'Baseline Management' is selected, and 'Baseline Template Configuration' is shown. A 'System Preset' tab is selected, showing a grid of baseline types like Container Security, Linux, Windows, Container, and Orchestration, each with a count (e.g., 74, 6, 37, 1, 6). Below this is a table for 'test-log-test-log-1' with columns for Check Object, Operating System, GPU Architecture, and Application. Another table for 'test-log-test-log' follows. At the bottom is a table for 'Classified Protection Ubuntu 24 System Baseline Check'. To the right, a 'New Check' dialog box is open, titled 'Basic Information'. It has fields for 'Name' (with placeholder 'Please enter the check task name') and 'Description' (with placeholder 'Please enter a description'). Below that is the 'Check Configuration' section, which includes 'Check E...:' (Linux is selected), 'Target R...:' (All Hosts is selected), and a 'Check ...:' field containing 'test-log-test-log-1' with a '+ Add' button. At the bottom of the dialog are 'Cancel', 'Save', and 'Save and Execute' buttons.

- If you need to customize based on the system-preset baseline template, click the "Create Copy" button to jump to the new baseline template creation page, where you can modify the baseline name and add/remove inspection items.
 - Click the "Add" button to pop up a list of inspectable items. Check the inspection items you need to add and click the "Confirm" button to save.
 - Click the "Remove" button to delete the selected inspection items, supporting single or batch deletion.

The screenshot shows the 'New Baseline Template' configuration page. Key fields include:

- Baseline Name:** test-log-test-log-1_Copy_20251024183454
- Baseline Description:** (empty)
- Whether:** Innovation
- Check Target:**
 - Check E...: Linux
 - Operating System: Unlimited
 - CPU Arc...: No Limit
 - Check ...: System
- Check Item:**

Check Item Name	Type	Description	Customization Status	Operation
Check if login failure lockout is configured.	Identity Authentication	To ensure the security of the user system, it is recommended that users set a threshold for...	No	Remove

Add Check Item

The 'Add Check Item' dialog displays a list of 788 items. Two items are selected on the right:

- Check if the successful file system mounts ...
- Check if the rsh client is not installed.

The 'OK' button at the bottom right is highlighted with a red box.

7.2.1.2. Custom Baseline Template

This function supports users in customizing baseline templates. Such baseline templates support creating new inspections, creating copies, editing, and deleting.

General Search: The system has set up a general search box, which supports unified retrieval of

baseline information according to different conditions.

Quick Filtering: The system arranges three key filtering items, namely baseline type, inspection environment, and inspection object, along with their filtering values, facilitating users to trigger result filtering with one-click quickly.

List Display: It displays customized baseline templates, where you can view basic information such as baseline name, inspection environment, inspection object, and the number of inspection items.

steps:

- Click the "New" button to jump to the new baseline template page. Fill in the basic information, inspection target, and add inspection items. After completion, click the "Save" button to create a customized baseline template.
 - If you select linux/windows as the inspection environment and "System" as the inspection object, you need to select the operating system and CPU architecture. If not selected, the default is "Unlimited" when saving.
 - If you select linux/windows as the inspection environment and "Application" as the inspection object, you need to select the specific application name and version.
 - Click the "Add" button to pop up a list of inspectable items. Check the inspection items

you need to add and click the "Confirm" button to save.

- Click the "Remove" button to delete the selected inspection items, supporting single or batch deletion.

The screenshot shows the 'New Baseline Template' configuration page. In the 'Check Item' section, two items have been selected for addition, indicated by a red box around them. The 'OK' button at the bottom right of the modal is also highlighted with a red box.

Add Check Item

The screenshot shows the 'Add Check Item' dialog box. Two specific check items have been selected for addition, indicated by a red box around them. The 'OK' button at the bottom right of the dialog is also highlighted with a red box.

- Clicking on a single baseline template card can jump to the baseline template details page,

where you can view the baseline information and the details of the included inspection items.

Importance	Category	Check Item Name	Type	Check Item Description	Customization
Major	System Preset	Check if login failure lockout is configured.	Identity Authentication	To ensure the security of the user system, it is recommended to...	No

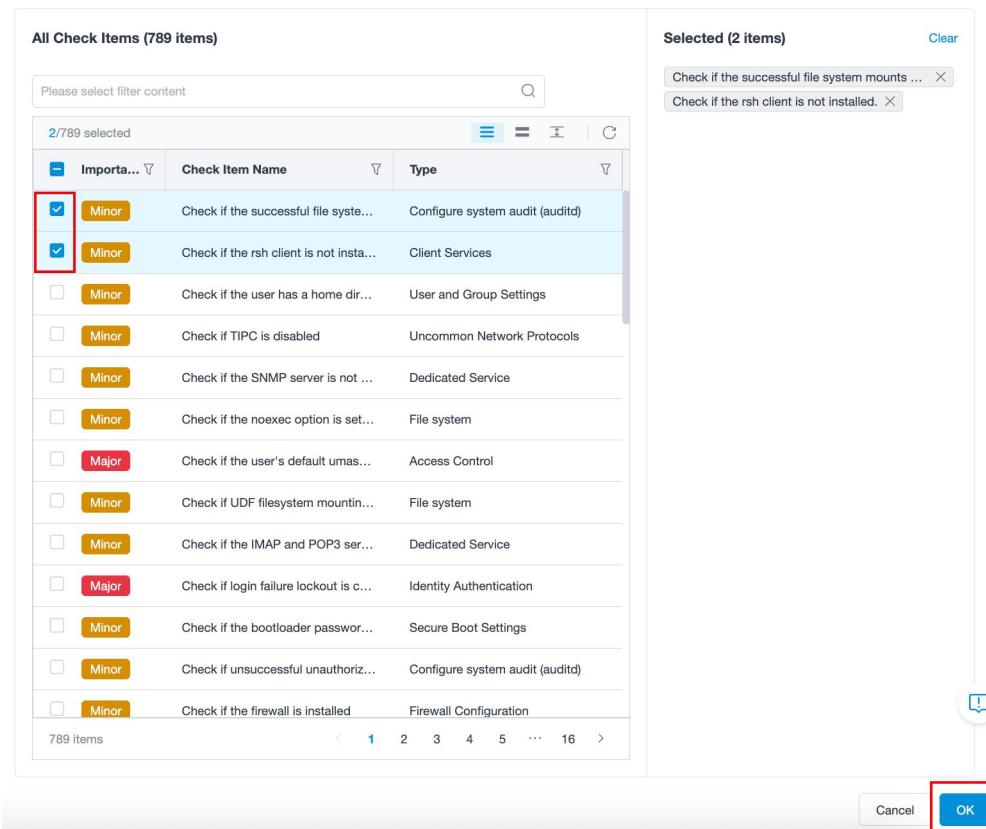
- If you want to initiate an inspection for a baseline template, click the "Create Inspection" button. In the pop-up page, fill in the basic information of the task and select the inspection configuration. After filling in, you can click the "Save and Execute" button to execute the task and view the task results under the [Baseline Inspection] function. You can also click the "Save" button to only save the task without executing it temporarily.

- Click the button after the inspection baseline to jump to a new page to view the details of this baseline template.
- If you want to delete this baseline, click the button.
- If you want to add other inspection baselines, click the + 添加 button.

- If you need to create a new one based on an existing custom baseline template, click the "Create Copy" button to jump to the new baseline template creation page, where you can modify the baseline name and add/remove inspection items.
 - Click the "Add" button to pop up a list of inspectable items. Check the inspection items you need to add and click the "Confirm" button to save.
 - Click the "Remove" button to delete the selected inspection items, supporting single or batch deletion.

The screenshot shows the 'New Baseline Template' configuration page. The top navigation bar includes links for Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery, Compliance, Event Collection, Security Control, DevSecOps, Web Application Firewall, Micro Segmentation, General, Tools, Messages, and a user account icon. The main content area has a breadcrumb path: Compliance > Baseline Management > Baseline Template Configuration > New Baseline Template. On the left, there's a sidebar with 'Baseline Check' and 'Baseline Mana...' sections, and a 'Baseline Template...' item is highlighted. The main form is titled 'Basic Information' and contains fields for 'Baseline Name' (set to 'test2_Copy_20251024163108') and 'Baseline ID'. A 'Whether...' section has radio buttons for 'Innovation' and 'Non-Innovation', with 'Innovation' selected. Below this is the 'Check Target' section, which includes a 'Check E...' dropdown set to 'Linux', and a sub-section for 'Application' targets with fields for 'Application Name' (set to 'Nginx') and 'Version' (set to '1.18.0,1.19.0'). There are also fields for 'Operating...' (set to 'Unlimited') and 'CPU Arc...' (set to 'No Limit'). The final section is 'Check Item', which contains a table of inspection items. The table has columns for 'Import...', 'Check Item Name', 'Type', 'Check Item Description', 'Customization Su...', 'Operation', and buttons for 'Remove' and 'Add'. Two items are listed: 'Tomcat default instance file check' (Security Configuration, Type: Tomcat Configuration) and 'Check if the Nginx log file exists' (File Configuration, Type: File Configuration). Both items have a red 'Major' status indicator. At the bottom right of the table are 'Cancel' and 'Save' buttons.

Add Check Item



- If you need to modify an existing baseline template, click the "Edit" button to jump to the baseline template editing page, where you can modify the baseline name and add/remove inspection items.
 - Click the "Add" button to pop up a list of inspectable items. Check the inspection items you need to add and click the "Confirm" button to save.
 - Click the "Remove" button to delete the selected inspection items, supporting single or batch deletion.

Basic Information

- * Baselin...: test2
- Check ...: Linux
- Operati...: Unlimited
- CPU Ar...: No Limit
- Check ...: Application
- Wheth...: Non-Innovation

Check Item

Import...	Check Item Name	Type	Check Item Description	Customization Su...	Operation
<input type="checkbox"/>	Tomcat default instance file check	Security Configuration	If there are default sample applications like example in the Tomcat service webapps, atta...	No	Remove
<input type="checkbox"/>	Check if the Nginx log file exists	Log Configuration	The nginx log files should be present to enable access log and error log recording; it also ...	No	Remove

2 items 1 50 Item/Page

Add Check Item

All Check Items (789 items)

Please select filter content

Import...	Check Item Name	Type
<input checked="" type="checkbox"/>	Minor	Check if the successful file syste...
<input checked="" type="checkbox"/>	Minor	Check if the rsh client is not insta...
<input type="checkbox"/>	Minor	Check if the user has a home dir...
<input type="checkbox"/>	Minor	Check if TIPC is disabled
<input type="checkbox"/>	Minor	Check if the SNMP server is not ...
<input type="checkbox"/>	Minor	Check if the noexec option is set...
<input type="checkbox"/>	Major	Check if the user's default umas...
<input type="checkbox"/>	Minor	Check if UDF filesystem mountin...
<input type="checkbox"/>	Minor	Check if the IMAP and POP3 ser...
<input type="checkbox"/>	Major	Check if login failure lockout is c...
<input type="checkbox"/>	Minor	Check if the bootloader passwor...
<input type="checkbox"/>	Minor	Check if unsuccessful unauthoriz...
<input type="checkbox"/>	Minor	Check if the firewall is installed

2/789 selected 1 2 3 4 5 ⋯ 16 >

Selected (2 items)

Check if the successful file system mounts ...
Check if the rsh client is not installed.

OK

- If an existing baseline template can be discarded, click the "Delete" button, which supports single or batch deletion.

Instructions:

- All baseline templates generated by creating copies of system-preset baseline templates and

saving them belong to custom baseline templates, which can be viewed in the [Custom Baseline Templates] tab page.

- Deleting a custom baseline template will affect existing inspection tasks. When deleting, you need to confirm the prompt information in the pop-up window. Please delete it carefully to avoid affecting the display of inspection task results.

7.2.2. Check Item Configuration

7.2.2.1. System Preset

This function displays all inspection items included in the system preset baseline template, which are system-preset inspection items. Such inspection items only support viewing details and creating copy operations.

General Search: The system has set up a general search box to support unified retrieval of inspection item information according to different conditions.

Quick Screening: The system arranges the three key screening items, namely importance level, inspection environment, and inspection object, along with their screening values, facilitating users to click with one key and trigger result screening quickly.

List Display: It displays the system-preset inspection items. You can see the inspection item name, importance level, type, inspection environment, and inspection object, and you can choose to display basic information such as the inspection item description.

The screenshot shows the Sentry CWPP web interface. The top navigation bar includes links for Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery, Compliance (which is currently selected), and More. On the far right, there are links for General, Tools, Messages (with 999+ notifications), and a user account for 'admin'. The main content area is titled 'Check Item Configuration' under the 'Compliance' section. It features a sidebar with links for Baseline Check, Baseline Management, Baseline Template, and Check Item Configuration (which is also highlighted). Below the sidebar is a search bar with the placeholder 'Please enter filter content' and a magnifying glass icon. The main panel has three tabs: 'System Preset' (selected) and 'Custom Check Items'. It displays three sections: 'Importance' (Trivial, Minor, Major, Critical), 'Check Environment' (Linux: 15, Windows: 1846, Container: 390), and 'Check Object' (System: 976, Application: 1007, Image: 268, Docker Host: 1765, Docker Container: 218, others: 35, 16). At the bottom, a table lists 2251 items with columns for Importance Level, Check Item Name, Type, Check Environment, Check Object, and Operation. Each row includes a 'View Details' and 'Create a Copy' button.

Steps:

- You can click the "View Details" button to check the basic information, description, and repair suggestions of the inspection item on the pop-up page. If the inspection item has an inspection method with customizable parameters, an additional "Inspection Method" column will be displayed. You can click the button to preview the specific parameters and parameter values in the inspection method.

Minor Check if login failure lockout is configured. 

Basic Information

Type: Identity Authentication

Check ... : Linux

Check ... : System

Category: **System Preset**

Check Item Description

To ensure the security of user systems, it is recommended that users set a threshold for the number of password entry errors (suggested at 3 attempts), as well as an automatic unlock time for users whose password attempts have been locked (suggested at 300 seconds). During the user lockout period, any input is deemed invalid, and the lockout timer will not reset with further user input; once unlocked, the user's record of incorrect entries is cleared. The aforementioned settings can effectively prevent passwords from being brute-forced, thereby enhancing the security of the system.

Repair Suggestions

Edit /etc/pam.d/password-auth and /etc/pam.d/system-auth files, set deny=3 unlock_time=300, for example: auth required pam_env.so auth required pam_faillock.so preauth audit deny=3 even_deny_root unlock_time=300 auth sufficient pam_fprintd.so auth sufficient pam_unix.so nullok try_first_pass auth [default=die] pam_faillock.so authfail audit deny=3 even_deny_root unlock_time=300 auth sufficient pam_faillock.so authsucc audit deny=3 even_deny_root unlock_time=300 auth requisite pam_succeed_if.so uid >= 1000 quiet_success auth required pam_deny.so UOS 1001c/1020a: Edit /etc/pam.d/password-auth and /etc/pam.d/system-auth files, set deny=3 unlock_time=300 before the auth pam_env.so line, for example: auth required pam_faillock.so preauth silent deny=3 even_deny_root unlock_time=300 auth required pam_faillock.so authfail deny=3 even_deny_root unlock_time=300

Major Check if the SSH protocol version is 2

X

Basic Information

Type: Identity Authentication

Check ... : Linux

Check ... : System

Category: **System Preset****Check Item Description**

SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 is the original protocol, constrained by security issues. SSH2 is more advanced and secure.

Check Method

Check whether the value of the specified configuration item in the specified INI file meets the  requirements

Repair Suggestions

Edit the /etc/ssh/sshd_config file, set Protocol to: 2, restart the sshd service.

- If you want to modify the inspection items preset by the system, you can click the "Create a Copy" button to create a new one and modify some information on the pop-up page. The modifiable range includes the inspection item name, importance level, type, inspection item description, output result, and repair suggestion. After saving, a new custom inspection item will be generated. If the inspection item has an inspection method with customizable parameters, an additional "Inspection Method" column will be displayed, and you can click the  button to modify the parameter values in the inspection method.

Create New Check Item

Basic Information

* Check It... : Check if login failure lockout is configured._Copy_20251124163907

* Importance: Minor

* Type: Identity Authentication

Check En... : Linux Windows Container

* Check O... : System Application

* Check It... : To ensure the security of user systems, it is recommended that users set a threshold for the number of password entry errors (suggested at 3 attempts), as well as an automatic unlock time for users whose password attempts have been locked (suggested at 300 seconds).

During the user lockout period, any input is deemed invalid, and the lockout timer will not reset with further user input; once unlocked, the user's record of incorrect entries is cleared. The aforementioned settings can effectively prevent passwords from being brute-forced, thereby enhancing the security of the system.

Check Configuration



* Output R... :
{% if (status==0 %}Password attempt failed 3 times, locked for 300 seconds
{% else %}
 {% if (check1.status==1 || check2.status==1 || check3.status==1) &&
 (check7.status==1 || check8.status==1 %}{% if (check1.path) file not configured for
 password attempt failed 3 times, locked for 300 seconds

Create New Check Item

Basic Information

* Check It... : Check if the SSH protocol version is 2_Copy_20251124163840

* Importance: Major

* Type: Identity Authentication

Check En... : Linux Windows Container

* Check O... : System Application

* Check It... : SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 is the original protocol, constrained by security issues. SSH2 is more advanced and secure.

Check Configuration

* Check M... : Check whether the value of the specified configuration item in the specified INI file meets the requirements

* Output R... :
{% if (status==0) %}{{ path }} file {{ item }} set to {{ real_value }}
{% elif (status==1) %}{{ path }} file {{ item }} set to {{ real_value }}
{% elif (status==2) %}{{ path }} file does not exist
{% elif (status==4) %}{{ path }} file {{ item }} does not exist, default is 2
{% endif %}



[View Examples](#)

Cancel

Save

7.2.2.2. Custom Check Items

This function supports users to customize inspection items. The product system will provide different inspection methods and corresponding parameters for users to select and fill in. New inspection items will be generated by encapsulating different parameter values in the inspection methods, so as to meet users' needs more flexibly.

General Search: The system has set up a general search box, which supports unified retrieval of inspection item information according to different conditions.

Quick Screening: The system arranges three key screening items, namely importance level, inspection environment, and inspection object, along with their screening values, facilitating users to click with one key and quickly trigger result screening.

List Display: It displays user-defined inspection items. You can see the inspection item name, importance level, type, inspection environment, inspection object, creation time, and latest update time. You can choose to display basic information such as the inspection item description.

Importance	Check Item Name	Type	Check Environment	Check Object	Creation Ti...	Last updat...	Operation
Major	test222_copy_20251125163658	Security Audit	Linux	System	2025-11-25 1...	2025-11-26 1...	View Details Create a Copy Edit Delete
Minor	test111	Access Control	Windows	System	2025-11-25 1...	2025-11-26 1...	View Details Create a Copy Edit Delete

Steps:

- You can click the "Create New Inspection Item" button to customize and create a new inspection item on the pop-up page. You need to fill in or select the basic information and inspection configuration of the inspection item.
 - Inspection Item Name: Text input, mandatory.
 - Importance Level: Single selection, mandatory.
 - Type: Single selection, mandatory.
 - Inspection Environment: Single selection, mandatory. The selected inspection environment will be used as a condition to match the baseline template. Only when the inspection environment of the baseline template is consistent with that of the

inspection item can it be selected from the baseline template and added to the inspection item.

- Inspection Object: Single selection, mandatory, and selected in linkage with the inspection environment. The selected inspection object will be used as a condition to match the baseline template. Only when the inspection object of the baseline template is consistent with that of the inspection item can it be selected from the baseline template and added to the inspection item.
- Inspection Item Description: Text input, mandatory.
- Inspection Method: One inspection method can be added to an inspection item. Click the **+Add** button to select the execution object and detection content on the pop-up page. After selection, the parameters that can be filled in for the inspection method are determined. Please fill in or select the specified value according to the parameter name. You can click the **i** button to view the parameter filling instructions and fill in the correct specified value according to the guidelines. After completion, click the "Save" button.

Add Check Method

Basic Information

* Execution target :

* Testing content :

Parameter Information

Add Check Method

Basic Information

* Execution Environment:

* Testing Configuration:

Parameter Information

* Target Parameter

Check Parameters	Specified Value
<input type="text" value="Redacted"/>	<input type="radio"/> true <input type="radio"/> false

* Check Parameters

Check Parameters	Specified Value
<input type="text" value="Redacted"/>	<input type="text" value="Please enter a specified value"/>
<input type="text" value="Redacted"/>	<input type="radio"/> true <input type="radio"/> false



-

- Output Result: Text input, mandatory. If the inspection method has a default output result template, the system will bring it out automatically, and you can modify it as needed based on the default template. If the inspection method does not have a default output result template, you can click the "View Example" button to fill it in according to the example format.

Check Item Name: Verify Password Reuse is Restricted

Result: {<% if (status==0) %>}The system has been configured to prevent reuse of the last 5 previously used passwords.
{<% elif (status==1) %>}Password reuse restriction is not configured.
{<% elif (status==2) %>}{{ path }} file does not exist.
{<% endif %>}

Note: Please follow the format above. 'status' indicates the check result: 0 means pass, 1 means fail, 2 means the target content does not exist.

The screenshot shows a configuration interface for a check item. On the left, there is a code editor containing a snippet of Python-like pseudocode that checks the status of password reuse. On the right, there is a preview window showing the results of the check for different status values (0, 1, 2). Below the preview is a "View Example" button.

- - Repair Suggestion: Text input, mandatory.
- You can click the "View Details" button to check the basic information, description, and repair suggestions of the inspection item on the pop-up page. If the inspection item has an inspection method with customizable parameters, an additional "Inspection Method" column will be displayed. You can click the button to preview the specific parameters and parameter values in the inspection method.

Minor test11 X

Basic Information

Type: Access Control

Check ...: Windows

Check ...: System

Category: Custom

Check Item Description

Access Control

Repair Suggestions

Access Control

Major test222_copy_20251125163658 

Basic Information

Type: Security Audit

Check ...: Linux

Check ...: System

Category: Custom

Check Item Description

rsyslog [REDACTED]

Check Method

Check whether the specified file contains the specified string



Repair Suggestions

/etc/rsyslog.conf [REDACTED]
[REDACTED]

- If you want to modify an existing custom inspection item, you can click the "Create Copy" button to create a new one and modify some information on the pop-up page. The modifiable range includes the inspection item name, importance level, type, inspection item description, output result, and repair suggestion. After saving, a new custom inspection item will be generated. If the inspection item has an inspection method with customizable parameters, an additional "Inspection Method" column will be displayed, and you can click the  button to modify the parameter values in the inspection method.

Create New Check Item

Basic Information

* Check It... : test111_Copy_20251126151417

* Importance: Minor

* Type: Access Control

Check En... : Linux Windows Container

* Check O... : System Application

* Check It... : Access Control

Check Configuration

* Output R...: Access Control

[View Example](#)



* Repair S... : Access Control

Cancel

Save

Create New Check Item

Basic Information

* Check It... : test222_copy_20251125163658_Copy_20251126151440

* Importance: Major

* Type: Security Audit

Check En... : Linux Windows Container

* Check O... : System Application

* Check It... : rsyslog用于将收集的日志发送到远程主机或接收来自远程主机的消息，减少管理开销

Check Configuration

* Check M...: Check whether the specified file contains the specified string



* Output R...:

```
{% if (status==0 ){{ path }}文件中{{ patterns }}存在
{% elif (status==1 ){{ path }}文件中{{ patterns }}不存在
{% elif (status==2 ){{ path }}文件不存在
{% endif %}}
```



[View Example](#)

[Cancel](#)

[Save](#)

- If you want to modify an existing custom inspection item, you can click the "Edit" button to modify some information of the inspection item on the pop-up page. The modifiable range includes the inspection item name, importance level, inspection item description, output result, and repair suggestion. If the inspection item has an inspection method with customizable parameters, an additional "Inspection Method" column will be displayed, and you can click the button to modify the parameter values in the inspection method.

Edit Check Item

Basic Information

* Check It... : test111

* Importance: Minor

* Type: Access Control

Check En... : Linux Windows Container

* Check O... : System Application

* Check It... : Access Control

Check Configuration

* Output R...: Access Control

[View Example](#)



* Repair S... : Access Control

Cancel

Save

Edit Check Item

Basic Information

* Check It... : test222_copy_20251125163658

* Importance: Major

* Type: Security Audit

Check En... : Linux Windows Container

* Check O... : System Application

* Check It... : rsyslog

Check Configuration

* Check M...: Check whether the specified file contains the specified string

* Output R...:

```
{% if (status==0) %}{{ path }}  
{%- elif (status==1) %}{{ path }}  
{%- elif (status==2) %}{{ path }}  
{%- endif %}
```

[View Example](#)

Cancel Save

- You can click the "Delete" button to delete inspection items individually or in batches.

Compliance > Baseline Management > Check Item Configuration

Check Item Configuration

The screenshot shows the 'Check Item Configuration' page. At the top, there are two tabs: 'System Preset' and 'Custom Check Items'. The 'Custom Check Items' tab is selected, indicated by a blue border. Below the tabs is a search bar with placeholder text 'Please enter filter content' and a magnifying glass icon. To the right of the search bar is a 'Collapse' button.

Below the search bar is a summary section with three columns: 'Importance', 'Check Environment', and 'Check Object'. The 'Importance' column shows counts for Trivial (6), Minor (6), Major (7), and Critical (3). The 'Check Environment' column shows counts for Linux (17), Windows (5), and Container (0). The 'Check Object' column shows counts for System (20), Application (2), Image (0), Docker Host (0), and Docker Container (0).

Below this summary is a table listing 2/22 selected check items. The table has columns: Importance, Check Item Name, Type, Check Envi..., Check Object, Creation Ti..., Last updat..., and Operation. Two rows are visible:

Importance	Check Item Name	Type	Check Envi...	Check Object	Creation Ti...	Last updat...	Operation
Major	test222_copy_20251125163658	Security Audit	Linux	System	2025-11-25 1...	2025-11-26 1...	View Details Create a Copy Edit Delete
Minor	test111	Access Control	Windows	System	2025-11-25 1...	2025-11-26 1...	View Details Create a Copy Edit Delete

A red arrow points from the 'Importance' column of the first row to the 'Delete' button in the 'Operation' column of the same row. Another red box highlights the 'Delete' button in the 'Operation' column of the second row.

Note:

- After editing, all baseline templates that include this inspection item will be affected. If a baseline template already has an inspection task, you need to re-execute the task to perform relevant inspections according to the edited inspection item content.
- After deletion, all baseline templates that include this inspection item will be affected. If a baseline template already has an inspection task, the relevant inspection will no longer be performed when the task is executed next time.

8. Event Collection

8.1. Introduction to Event Collection

Event collection refers to the process of gathering security-related logs, operation records, and system behavior information from host systems (such as servers, virtual machines, containers, etc.). CWPP event collection has the capability to collect and export events from hosts, PCs, and containers, and then send them to the target environment for processing and analysis via the data export app.

8.2. Use of event collection

The use of event collection is divided into the following main stages:

- Purchase and activate event collection authorization
- Enable event collection
- Configure collection and filtering strategies
- Configure data outsourcing

8.3. Event collection function

The main features of event collection are in the collection configuration, which includes:

- Asset perspective allocation
- Host event configuration
- Container event configuration
- Edr event configuration

8.3.1. Asset perspective allocation

Configure event collection from the asset perspective, by host or cluster.

8.3.1.1. Host perspective

View the list of hosts/PCs with event collection authorization enabled. For each host/PC, view enabled event details, collection status, and configure collection parameters.

The screenshot shows the 'Asset perspective configuration' page under 'Event Collection Configuration'. At the top, there's a note about enabling event collection scopes for specific devices. Below it, there are tabs for 'Host' and 'Cluster', with 'Host' selected. A search bar and a 'Batch Configuration' button are also present. The main area displays a table with 75 items, showing columns for Host, Business Group, Agent ID, Host Collection Status, Enable Events, Abnormal events, Latest reporting time, and Action. The table includes icons for hosts and business groups, and a heatmap for Agent ID. The 'Host Collection Status' column shows values like 'Unopened', 'Event Exception', and 'Normal'. The 'Enable Events' and 'Abnormal events' columns show counts (e.g., 0, 42, 113). The 'Latest reporting time' column shows dates like '2025-11-28 16:52:04'. The 'Action' column contains links labeled 'Collection Co...'.

- **Host:** Display host IP and host name
- **Business Group:** Belonging Business Group
- **AgentID:** The host's AgentID. Click to view Agent details
- **Enable event:** Events that have been enabled for collection on the current host/PC
- **Collection Status:** The current event collection status of the host
 - **Not Enabled:** Indicates that no events are configured for this host
 - **Host Exception:** Indicates that the host Agent is offline, disabled, or degraded, resulting in collection exceptions. This affects all events on the host, preventing

normal collection.

- Event Exception: Indicates that the host Agent is functioning normally, but an enabled event has an exception, often due to an unenabled event source, uninstalled plugin, or unconfigured collection policy. This affects certain events on the host, preventing normal collection.
 - Normal: Indicates that the host Agent is functioning normally, and all enabled events are exception-free
- Abnormal Events: Events that are enabled on the host but have a collection status of "Event Exception"
 - Latest reporting time: the time when the current host last reported any event
 - Operation: Configure event scope to define the range of events collected on the host

8.3.1.2. Cluster perspective

View the list of clusters with event collection authorization enabled. For each cluster, view enabled event details, collection status, and configure collection parameters.

The screenshot shows the 'Asset perspective configuration' section of the Sentry CWPP interface. At the top, there's a message bar stating: 'Asset perspective configuration allows you to enable or adjust event collection scopes for specific devices. The event collection scope for newly authorized hosts can be configured in Default Configuration.' Below this is a navigation bar with 'Host' and 'Cluster' tabs, where 'Cluster' is selected. A search bar and a 'Collection Configuration' button are also present.

Under the 'Collection Status' section, there are four categories: Normal (0), Unopened (6), Event Exception (0), and Host Abnormal (0). A note says 'No data'.

The main table lists 6 items, each representing a cluster component. The columns are: Cluster, Cluster Component ID, Collection Status, Enable Events, Abnormal events, and Action. The data is as follows:

Cluster	Cluster Component ID	Collection Status	Enable Events	Abnormal events	Action
Cluster 1	Component 1	Unopened	0	0	Event Scope ...
Cluster 1	Component 2	Unopened	0	0	Event Scope ...
Cluster 1	Component 3	Unopened	0	0	Event Scope ...
Cluster 1	Component 4	Unopened	0	0	Event Scope ...
Cluster 1	Component 5	Unopened	0	0	Event Scope ...
Cluster 1	Component 6	Unopened	0	0	Event Scope ...

- Cluster: Cluster Name
- Cluster Component ID: Cluster Component ID
- Collection Status: The current event collection status of the cluster component
 - Cluster Exception: Indicates that the cluster component is offline, disabled, or degraded, resulting in collection exceptions
 - Event Exception: Indicates that the cluster component is functioning normally, but an enabled event has an exception, often due to an unenabled event source, uninstalled plugin, or unconfigured collection policy
 - Normal: Indicates that the cluster component is functioning normally, and all enabled events are exception-free
- Enabled Events: Events for which collection is currently enabled on the cluster component
- Events in Collection: Events with a "Collecting" status

- Events with Collection Exceptions: Events with an "Collection Exception" status
- Operation: Collection Configuration – Reconfigure collection parameters

8.3.2. Host event configuration

Configure event collection from the host event perspective, by host event, categorized by system type:

Linux events and Windows events.

8.3.2.1. Linux Events

The screenshot shows the 'Host Event Configuration' page with the 'Linux Events' tab selected. On the left, there's a sidebar with 'Event Classification (6)' and a search bar. Below it is a list of categories: Account Management (3), Bash Event(1), File Event(1), Account Login Log ... (2), Network Event(2), and Process Event(2). A red box highlights the 'Account Management (3)' category. In the main area, there's a table showing three specific events: 'User account change event', 'Local user group change event', and 'sudo change event'. Each row has an 'Event Switch' toggle switch, which is turned on for all three. The table includes columns for 'Event Collection Scope' (0, 0, 1), 'Host Status Abnormal' (0, 0, 1), and 'Event anomaly' (0, 0, 0). At the bottom right, there are navigation buttons for '1' and '50 Item/Page'.

- Event classification: List the supported event categories, each containing multiple specific events. Support searching by event category name.
- Event List: Display Specific Events
 - Event Name
 - Event Switch: A global switch that controls whether the event is enabled. If turned off, the event cannot be collected by any host
 - Collecting: Activate the current event and collect the host in progress
 - Exception collection: Activate the current event and collect the host with exceptions
 - Collection configuration: Collection parameters can be reconfigured

8.3.2.2. Windows Events

The screenshot shows the 'Host Event Configuration' interface. At the top, there are tabs for 'Linux Events' and 'Windows Events', with 'Windows Events' being the active tab. Below the tabs is a search bar labeled 'Event Classification (3)' and a 'Search Event Type/Name' input field. A sidebar on the left lists categories: 'Account Login Log... (2)', 'Network Event(1)', and 'Process Event(1)'. The main area displays two items under 'Event Classification': 'Account login event' and 'Account logout event'. Each item has a checkbox, a toggle switch, and three numerical values: 'Event Collection Scope' (0), 'Host Status Abnormal' (0), and 'Event anomaly' (0). At the bottom right, there is a page navigation section with arrows and a '50 Item/Page' dropdown.

- **Event Categories:** Lists supported event categories, each containing multiple specific events.
Supports searching by category name.
- **Event List:** Displays specific events
 - Event Name
 - Collecting: Hosts with the event enabled and in the "collecting" state
 - Collection Exception: Hosts with the event enabled and in the "collection exception" state
 - Collection Configuration: Allows reconfiguration of collection parameters

8.3.3. Container Event Configuration

Configure event collection from the container event perspective, by container/cluster event, categorized by type: container events and cluster events.

8.3.3.1. Container Events

Event Classification	Event Name	Event Collection Scope	Host Status Abnormal	Event anomaly
Network Event(2)	Container network connection event	0	0	0
	Container network monitoring events	0	0	0

- **Event Categories:** Lists supported event categories, each containing multiple specific events.
- Supports searching by category name.
- **Event List:** Displays specific events
 - Event Name
 - Event Switch: A global switch that controls whether the event is enabled. If turned off, the event cannot be collected by any host
 - Collecting: Hosts/PCs with the event enabled and in the "collecting" state
 - Collection Exception: Hosts/PCs with the event enabled and in the "collection exception" state
 - Default Policy: Some events require a default policy, which defines collection rules. Only events that meet the rules will be collected.
 - Collection Configuration: Allows reconfiguration of collection parameters

8.3.3.2. Cluster Events

Event Classification	Event Name	Event Collection Scope	Host Status Abnormal	Event anomaly
Cluster Event(1)	Cluster audit event	0	0	0

- Event Categories: Lists supported event categories, each containing multiple specific events.
Supports searching by category name.
- Event List: Displays specific events
 - Event Name
 - Event Switch: A global switch that controls whether the event is enabled. If turned off, the event cannot be collected by any host
 - Collecting: Hosts/PCs with the event enabled and in the "collecting" state
 - Collection Exception: Hosts/PCs with the event enabled and in the "collection exception" state
 - Collection Configuration: Allows reconfiguration of collection parameters

8.3.4. EDR event configuration

Configure event collection from the PC event perspective, by PC event, categorized by system type:

Linux events and Windows events.

8.3.4.1. Linux Events

The screenshot shows the 'Edr Event Configuration' page with the 'Linux Events' tab selected. On the left, there's a sidebar with a search bar and a list of event categories: Account Management(2), Bash Event(1), File Event(1), Account Login Log(2), File System Event(2), Network Event(2), and Process Event(2). The main area displays two specific events: 'User account change event' and 'sudo change event', each with a toggle switch, event count (0), and status metrics (Event Collection Scope: 0, Host Status Abnormal: 0, Event anomaly: 0). There are also buttons for 'Event Switch' and 'Event Classification (7)'.

- Event classification: List the supported event categories, each containing multiple specific events. Support searching by event category name.
- Event List: Display Specific Events

- Event Name
- Event Switch: A global switch that controls whether the event is enabled. If turned off, the event cannot be collected by any host
- Collecting: Activate the current event and collect the PC in progress
- Exception collection: Activate the current event and collect the PC with exceptions
- Collection configuration: Collection parameters can be reconfigured

8.3.4.2. Windows Events

The screenshot shows the 'Edr Event Configuration' interface. At the top, there are tabs for 'Linux Events' and 'Windows Events', with 'Windows Events' being the active tab. On the left, a sidebar lists various event categories with their counts: Account Management (2), Command Event (2), File Event (1), Account Login Log... (2), Module Event (2), Network Event (2), Permission Event (1), PowerShell Event (2), Process Event (2), Registry Event (1), Scheduled Task M... (2), System Service Ev... (1), and Windows System ... (1). The main area displays two specific events: '(Domain) Computer account creation event' and 'User account change event'. Each event entry includes a checkbox, an enable/disable switch, event collection scope (0), host status abnormal (0), and event anomaly (0). The bottom right corner shows a page navigation bar with '1' and '50 Item/Page'.

- Event Categories: Lists supported event categories, each containing multiple specific events.
Supports searching by category name.
- Event List: Displays specific events
 - Event Name
 - Event Switch: A global switch that controls whether the event is enabled. If turned off, the event cannot be collected by any host
 - Collecting: /PCs with the event enabled and in the "collecting" state
 - Collection Exception: PCs with the event enabled and in the "collection exception"

state

- Collection Configuration: Allows reconfiguration of collection parameters

8.4. Purchasing and Enabling Event Collection

8.4.1. Event Collection Specifications

Event collection is an independent feature app that requires separate purchase and authorization.

Event collection is divided into: host event collection, endpoint event collection, and container event collection. The specifications are as follows:

Specification	Included Events	Purchase Method
Host Event Collection	All host events	Subscription
		Perpetual License
Endpoint Event Collection	All PC events	Subscription
		Perpetual License
Container Event Collection	All container events + cluster events	Subscription
		Perpetual License

- The above specifications can be purchased individually, in combination, or all at once.
- After purchase, the authorization file will include the corresponding event collection specifications.

8.4.2. Event Collection Authorization

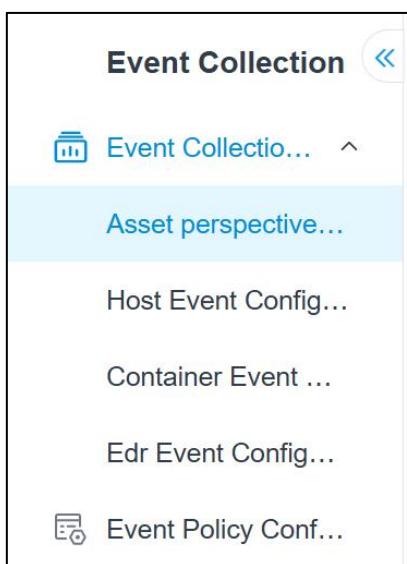
Event collection authorization information includes event collection specifications, authorization

points, and authorization validity period.

Host Event Collection	Number: 100	Start and end time: 2025-03-04 ~ 2026-03-04
Container Event Collection	Number: 100	Start and end time: 2025-03-04 ~ 2026-03-04
Endpoint Event Collection	Number: 100	Start and end time: 2025-03-04 ~ 2026-03-04

8.4.2.1. Authorization Control Function Menu

After purchasing the corresponding authorization, the corresponding event collection features become available, and the corresponding function menu is visible.



Purchase Status	Interface Display Description
Only Purchased Host Event Collection	<p>Only the host perspective is displayed in the "Asset Perspective Configuration" menu.</p> <ul style="list-style-type: none">- The "Host Event Configuration" menu is displayed.- The "Container Event Configuration" menu is not displayed.- The "EDR Event Configuration" menu is not displayed.

	<ul style="list-style-type: none">- The "Event Policy Configuration" menu is displayed.
Only Purchased Container Event Collection	<p>Only the cluster perspective is displayed in the "Asset Perspective Configuration" menu.</p> <ul style="list-style-type: none">- The "Host Event Configuration" menu is not displayed.- The "Container Event Configuration" menu is displayed.- The "EDR Event Configuration" menu is not displayed.- The "Event Policy Configuration" menu is displayed.
Only Purchased EDR Event Collection	<p>Only the EDR perspective is displayed in the "Asset Perspective Configuration" menu.</p> <ul style="list-style-type: none">- The "Host Event Configuration" menu is not displayed.- The "Container Event Configuration" menu is not displayed.- The "EDR Event Configuration" menu is displayed.- The "Event Policy Configuration" menu is displayed.
Purchased Host Event Collection, EDR Event Collection, and Container Event Collection	The menu is fully displayed.

8.5. How to Enable Event Collection

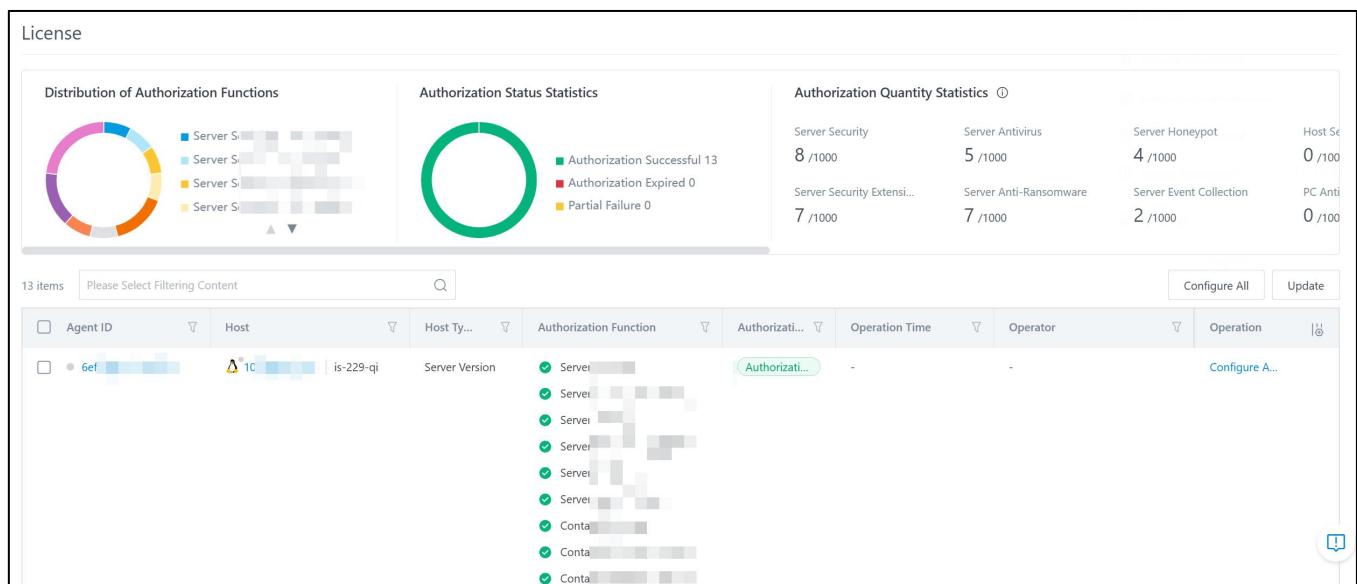
Enabling event collection involves three steps:

- Enabling Agent authorization
- Enabling plugins
- Configuring collection parameters

8.5.1. How to Enable Agent Authorization

8.5.1.1. Enabling Authorization on Installed Agents

Go to [Probes] → [Probe Management] → [License] , and enable event collection authorization for the target host/PC or container agent.

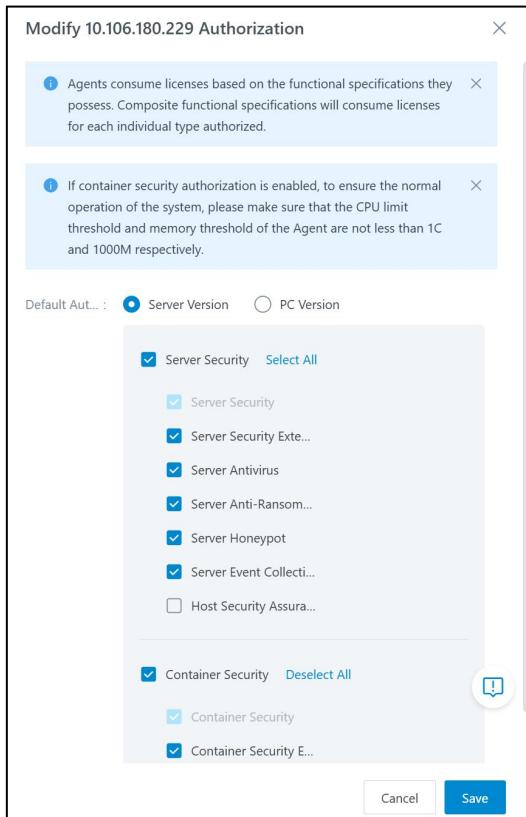


- In the Agent authorization interface:
 - Server version options: Host Event Collection, Container Event Collection
 - PC version options: Endpoint Event Collection, Container Event Collection

- Select the corresponding event collection specification to enable.

8.5.1.2. Enabling Authorization on New Agents

Go to **[Probes]→[Installation]→[Agent]**, and enable event collection authorization for new agents.



- In the Agent installation interface:
 - Server version options: Host Event Collection, Container Event Collection
 - PC version options: Endpoint Event Collection, Container Event Collection
- Select the corresponding event collection specification to enable.

8.5.2. How to Enable Plugins

Event collection is completed through plugins that obtain and report event logs. The corresponding plugins must be enabled before collection can begin.

8.5.2.1. Event and Plugin Correspondence

Plugin Name	Applicable	Reported Events
	System	
Bash Plugin	Host - Linux	Bash events - Bash audit logs
DNS Plugin	Host - Linux	Network events - DNS query events
CMD Audit Plugin	Host - Windows	CMD audit - CMD process start events - CMD user input events - CMD command execution restore events
PowerShell Audit Plugin	Host - Windows	PowerShell class start events - PowerShell interactive command input events - PowerShell command execution restore events - PowerShell script file path and identification events
Sysmon Plugin	Host - Windows	Registry events - Process events - WMI events - File events - Module events - Sysmon source status change events - Pipe events
k8s Log Audit Component	Cluster	Kubernetes API audit logs

8.5.2.2. Enabling Plugins

Go to [Probes] → [Component] → [Plugin], and enter the corresponding plugin management page.

Plugins	
5 Items	
Bash Plugin New Version	Reported Events Description
Applicable Probes: Host - Linux Agent	Applicable Scope: CentOS 5.3 and above, Ubuntu 12.04 and above (excluding 20.04)
Function: The Bash plugin audits the security of commands executed within the Bash program by monitoring command execution behavior.	Introduction
DNS Plugin	Reported Events Description
Applicable Probes: Host - Linux Agent	Applicable Scope: CentOS 5.3 and above, Ubuntu 12.04 and above (excluding 20.04)
Function: The DNS plugin audits DNS domain name resolution behavior by monitoring the system's DNS domain name resolution.	Introduction
CMD Audit Plugin	Reported Events Description
Applicable Probes: Host - Windows Agent	Applicable Scope: Windows 7 SP1 and above or Windows Server 2008 R2 and above
Function: The CMD audit plugin monitors command execution behavior in the CMD and audits the security of the commands executed within it.	Introduction
PowerShell Audit Plugin	Reported Events Description
Applicable Probes: Host - Windows Agent	Applicable Scope: Windows 7 SP1 and above or Windows Server 2008 R2 and above(The kernel version must be greater than 6.0)
Function: The PowerShell auditing plugin works by monitoring command execution behavior within PowerShell to audit the security of the commands executed.	Introduction

In the plugin list page, select the target agent and enable the plugin (using Bash plugin as an example).

Bash Plugin New Version		The Bash plugin audits the security of commands executed within the Bash program by monitoring command execution behavior.				Create Task	
The Bash plugin audits the security of commands executed within the Bash program by monitoring command execution behavior.							
Applicable Probes	Applicable Scope	Latest Version	Total Agents (hosts)	Not Installed (hosts)	Normal Running (hosts)	Abnormal Running (hosts)	
Host - Lin...	CentOS 5.3 and above, Ubuntu 12.04 a...	1.5.15(linux-x86_64),1.5.15(linux-aarch64)	12	8	4	0	
12 items Please Select Filtering Content <input type="text"/> Export All							
<input type="checkbox"/> Agent ID ▼ Host ▼ Plugin ... ▼ Plugin ... ▼ Last Ex... ▼ Last Execution Ti... ▼ Installation Time ▼ Operation							
<input type="checkbox"/> 1bcd1 10 ceph-test-2 Normal 1.5.14 Upgraded 2024-10-31 09:36:30 2024-09-10 17:05:06 Uninstall Upgrade							
<input type="checkbox"/> eb88 10 it-10076-jinyan.xu Normal 1.5.12 - - 2024-11-12 16:06:17 Uninstall Upgrade							
<input type="checkbox"/> 4aae 17 localhost.localdomain Not Installed - - - - Install							
<input type="checkbox"/> 62cf 10 localhost.localdomain Not Installed - Installation 2024-12-05 11:39:36 - Install							

Search for the target agent and click "Install".

8.5.3. How to Configure Collection Parameters

8.5.3.1. Configuring by Asset Perspective

Navigate to 【Event Collection】 → 【Asset View Configuration】 , select the Host View Tab (using host configuration as an example here), and click the "Batch Configuration" button in the upper right corner of the list.

The screenshot shows the 'Asset perspective configuration' page under 'Event Collection Configuration'. At the top, there's a message about asset perspective configuration allowing you to enable or adjust event collection scopes for specific devices. Below this are tabs for 'Host' and 'Cluster', with 'Host' selected. A search bar and a 'Collapse' button are also present.

Below the search bar, there are three sections: 'Event Collection Authorization' (with counts for Authorized: 45, Unauthorized: 14), 'Collection Status' (with counts for Normal: 11, Unopened: 14, Event Exception: 1, Host Abnormal: 19), and 'Event anomaly' (with count 1). A 'CMD plugin uninstalled' message is also shown.

The main area displays a table of 45 items (hosts) with columns: Host, Business Group, Agent ID, Collection Status, Enable Events, and Abnormal events. One host entry is highlighted with a red box, showing 'Host Abnormal' status and 124 enable events. A 'Batch Configuration' drawer is open on the right, listing 'Linux Events', 'Windows Events', and 'Container Events'.

- Select the event sources you wish to configure, including Linux events, Windows events, and container events. After selecting, choose the required event scope and host scope in the right-side drawer, as shown in Figure 5-6.
- After selecting the event and host scope, click "Save and Synchronize".

Collection Configuration

Basic Information

Please select filter content Remove **Select Event**

0 items

<input type="checkbox"/> Event Category	<input type="checkbox"/> Event Name	Action
No Data		

*** Event Collection Scope**
Adding a host means turning on the event collection switch, removing a host means turning off the event collection switch

Add the Following Hosts Remove the Following Hosts

Please select filter content Remove **Select Host**

0 items

<input type="checkbox"/> Host	<input type="checkbox"/> Host Type	Action
No Data		

Cancel **Save and Sync**

8.5.3.2. Configuring by Event Perspective

Go to **【Event Collection】 → 【Host Event Configuration】**, select the Windows Events Tab (using host

event configuration as an example here), choose the target event, and click the number under the "Collection Scope" field.

Figure 5-7 Collection Configuration - By Event

The screenshot shows the Sentry CWPP interface for 'Host Event Configuration'. On the left, there's a sidebar with navigation links like Asset, Intrusion Detection, Ransom Protection, Risk Discovery, Compliance, Event Collection (which is selected and highlighted in blue), Security Control, DevSecOps, and Micro Segmentation. Below the sidebar, there are tabs for 'Linux Events' and 'Windows Events'. The main area displays a list of events under 'Event Classification (9)' with a search bar. One event, 'User account change event', is selected and highlighted with a red box around its 'Collection Scope' value of '15'. Other events listed include 'User space open event', 'User space shutdown event', 'User password verification event', 'User authorization event', 'Credential refresh event', 'Voucher generation event', 'Document destruction event', and 'sudo change event', each with a 'Collection Scope' value of '0'. To the right, a modal window titled 'Collection Scope' is open, showing 'Event Information' (Event Name: User account change event, Event Category: Account Management Event, Operating System: Linux) and a 'Collection Host Range' table. The table has columns for Host, Business Group, Collection Status, and Action. It lists 15 items, mostly uncollected hosts, with a 'Select Host' button at the top right of the table area, which is also highlighted with a red box.

- Click "Select Hosts" to add the hosts that need to have collection enabled.
- After selecting the events, click "Save".

8.6. How to Configure Collection/Filtering Policies

After enabling event collection, a large number of event records will be generated. Events unrelated to the business or those that do not require attention can be filtered out by configuring collection and filtering policies.

Additionally, for certain events, such as file events, specific directories must be designated for collection. By configuring collection policies, only events that meet the policy criteria will be collected and reported.

8.6.1. Filtering Policies

A filtering policy prevents the collection and reporting of event logs that match the rules defined within the policy.

Go to the **【Event Collection】 → 【Event Policy Configuration】** page. The Filtering Policy page is displayed by default.

The screenshot shows the "Event Policy Configuration" page. At the top, there is a note about filtering and collection policies. Below this, there are two tabs: "Filtering Policy" (which is selected and highlighted with a red box) and "Collection Policy". A search bar and a "Create New Policy" button are also present. The main area contains a table with the following data:

Enable...	Policy Name	Event Name	Creation Type	Applicat...	Policy Description	Latest updat...	Operator	Action
<input checked="" type="checkbox"/>	-	Process creation event (Host Event ...)	preset	All Hosts	-	2025-10-20 18:11:52	system	View Policy

At the bottom of the table, it says "1 items". There are navigation arrows and a "50 Item/Page" dropdown.

Click the "Create New Policy" button in the upper-right corner of the list to edit the policy details

New Custom Filtering Policy

Basic Information

* Policy ... : Please enter the policy name

* Event: Host Event / Linux / Process Event / Process creation event >

Policy D...: Please enter a policy description

Application Scope

Applic...: All Hosts Select some hosts

Policy Rule

Rule 1

Process Name:

1	Please enter the full process name separate multiple with newlines
2	
3	

Command Line:

1	<output>: Can input part of the command line separate multiple with n
2	
3	

Process File ... :

1	Please enter the full process file path separate multiple paths with new
2	
3	

Parent Proces...:

1	Please enter the full process name separate multiple with newline
2	
3	

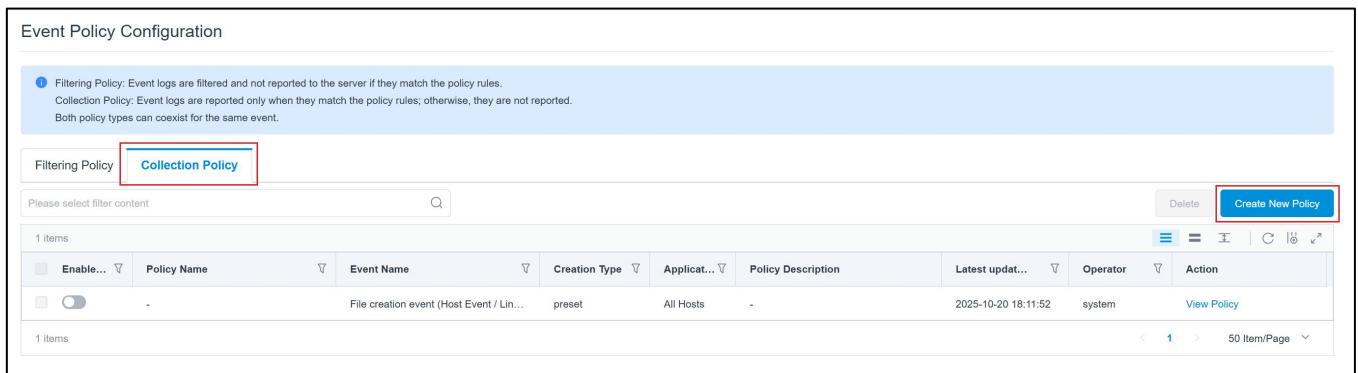
Cancel

- Event: Select the event for which you want to configure the policy. After selection, you can configure the application scope and policy rules below.
- Application Scope: Select the Agents to which this policy applies.
- Policy Rules: Configure rules for the selected event. Multiple rules are supported, with an "OR" relationship between rules. Within each rule, the configuration of each field has an "AND" relationship.

8.6.2. Collection Policies

Collection Policy: Only events that meet the rules defined in the collection policy will be collected and reported.

Go to the [Event Collection] → [Event Policy Configuration] page and switch to the [Collection Policy] tab.



The screenshot shows the "Event Policy Configuration" page. At the top, there is a note about Filtering Policy and Collection Policy. Below this, there are two tabs: "Filtering Policy" and "Collection Policy", with "Collection Policy" being the active tab and highlighted with a red box. A "Create New Policy" button is located in the upper-right corner of the main content area. The main content area displays a table with one item, showing columns for Enable..., Policy Name, Event Name, Creation Type, Application, Policy Description, Latest update..., Operator, and Action. The table also includes a search bar, a delete button, and various filter and export options. The table shows one item: "File creation event (Host Event / Lin..." with "preset" creation type, "All Hosts" application, and "system" operator.

Click the "Create New Policy" button in the upper-right corner of the list to edit the policy content.

New Custom Collection Policy

Basic Information

* Policy ... : Please enter the policy name

* Event: Host Event / Linux / File Event / File creation event >

Policy D...: Please enter a policy description

Application Scope

Applic...: All Hosts
 Select some hosts

Policy Rule

Rule

* File Path: 1 Please enter the full file path, separate multiple paths with a newline.
2
3

!

Cancel Save

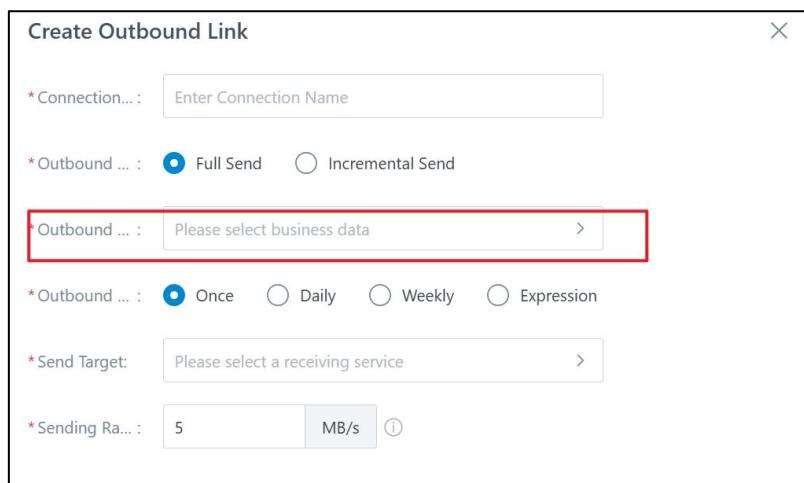
- Event: Select the event for which you want to configure the policy. After selection, you can configure the application scope and policy rules below.
- Application scope: This policy can be applied to hosts/PCs and containers that can be selected to take effect
- Collection rule: Only events that meet the criteria of the rule will be collected and reported

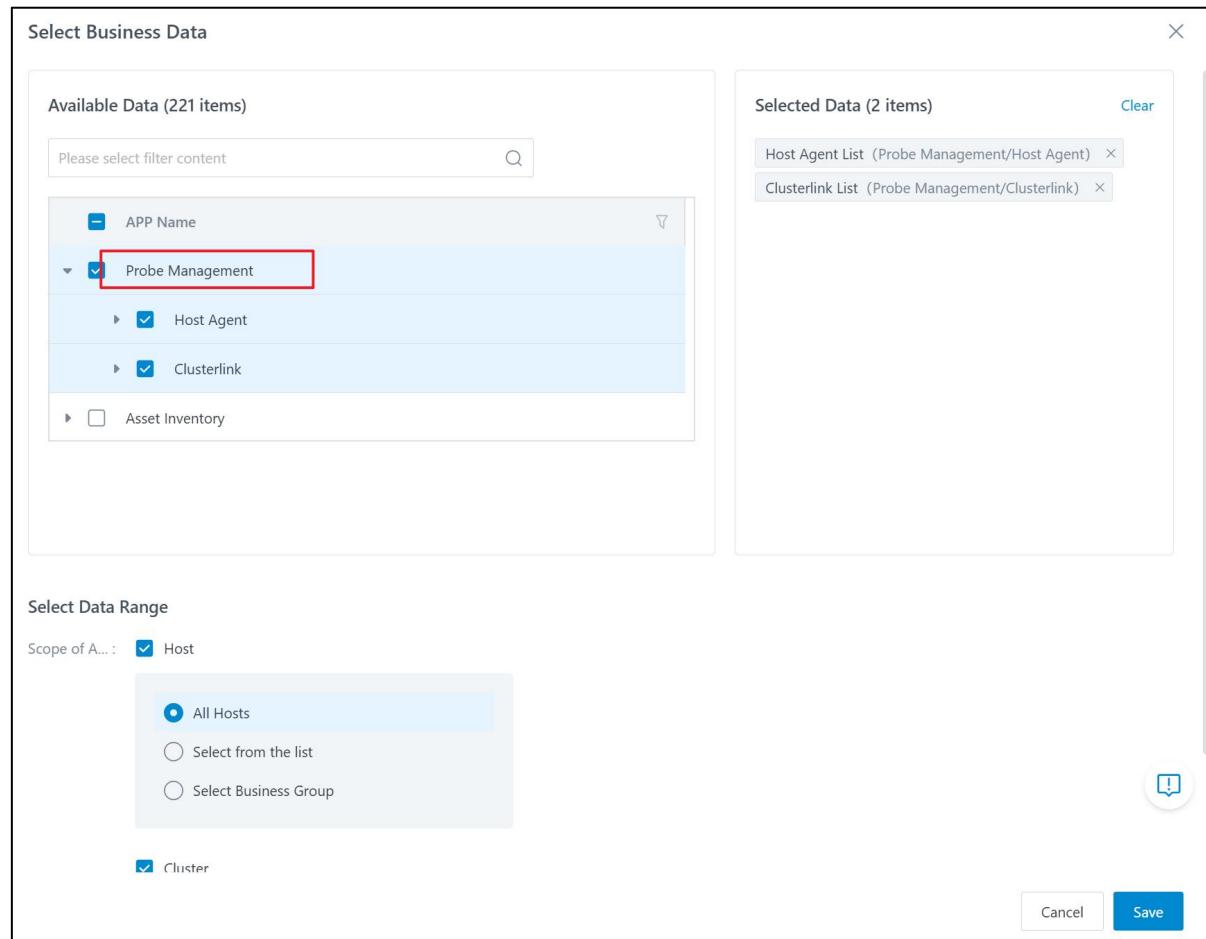
8.7. How to Configure Data Export

After enabling event collection and configuring collection/filtering policies, event data will be continuously collected and reported. This data needs to be sent to the target environment for processing via the data export app.

Go to **[Outgoing]→[Outgoing Connection Management]**, create a new export connection, and select the events from event collection for export.

After establishing the export connection, event collection data will be automatically exported to the target environment.





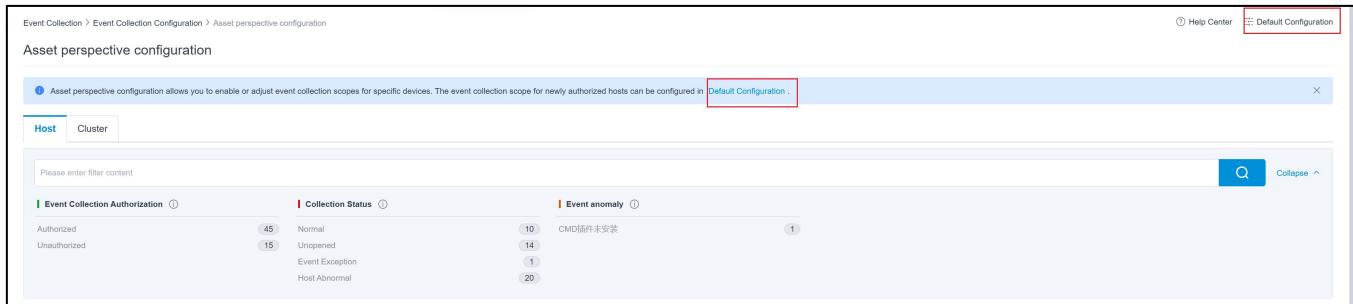
- Select event collection app
- Select the events to be outsourced
- Select the host/PC and container that need to be outsourced

8.8. How to Automatically Enable Event Collection for Newly Authorized Hosts

For newly authorized hosts, the range of events to be automatically enabled can be set in the default configuration, without the need for continuous manual follow-up.

Steps:

- Go to [Asset View Configuration], and click the "Default Configuration" button in the upper right corner.



- Configure the automatic collection scope for Linux events, Windows events, container events, and cluster events separately. Taking Linux events as an example, go to the Linux event scope configuration page, click the "Select Events" button in the upper right corner of the list, and add events.

This screenshot shows the 'Host Event Scope Configuration' dialog box. It lists various event types such as Account logout event, DNS query event, Process script detection event, etc., each with a checkbox, an 'Event Category' column, and a 'Remove' button in the 'Action' column. A blue 'Add Event' button is highlighted in the top right corner of the list area. The sidebar on the left shows the navigation path: Event Collection > Event Collection Configuration > Asset perspective configuration > Default Configuration > Collection Scope Configuration.

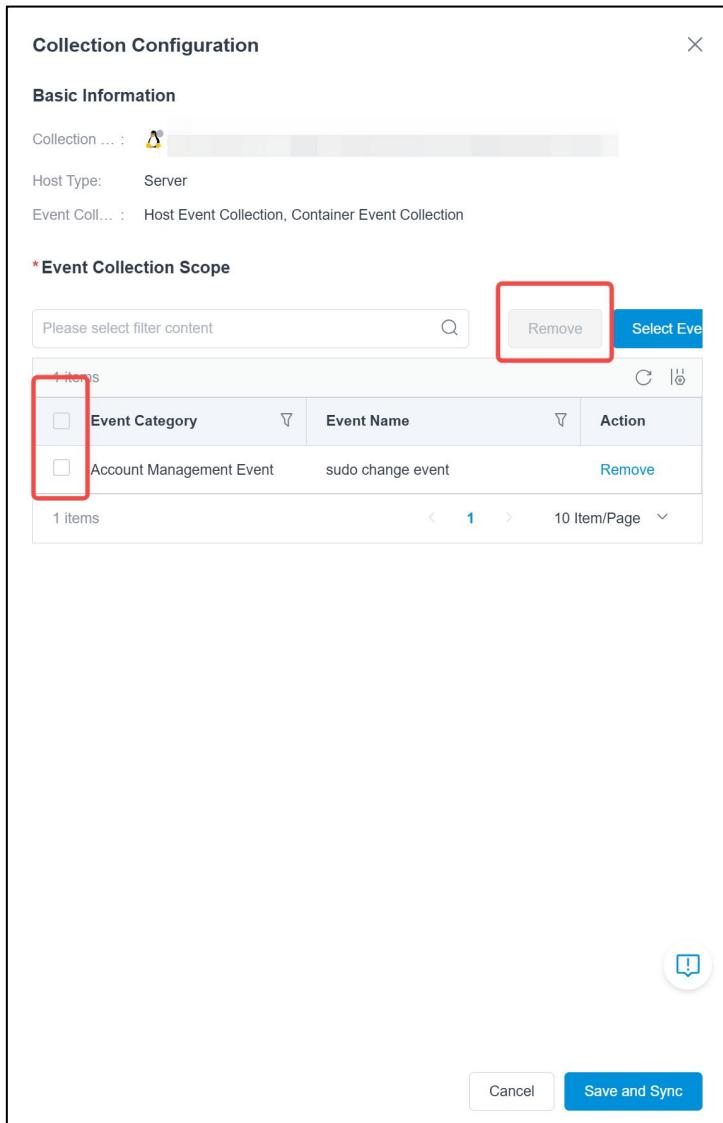
8.9. How to Disable Event Collection

8.9.1. Disabling Event Collection by Host/PC or Container

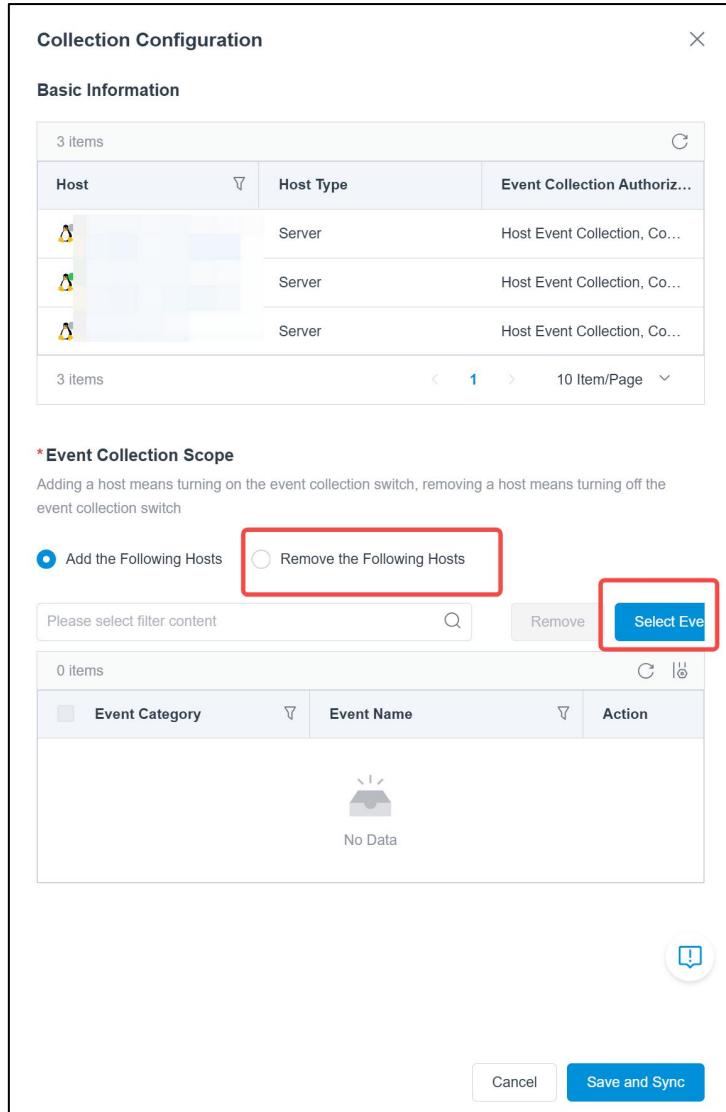
Navigate to **[Asset Perspective Configuration]**, under the "**Host Perspective**" tab:

- Select a single host/PC, click "**Collection Configuration**" to view all events collected by the host. In the event collection scope list, click the "**Remove**" button in the action column to disable collection for that event.

- Alternatively, check the boxes for multiple events and click "**Remove**" to perform batch event removal.

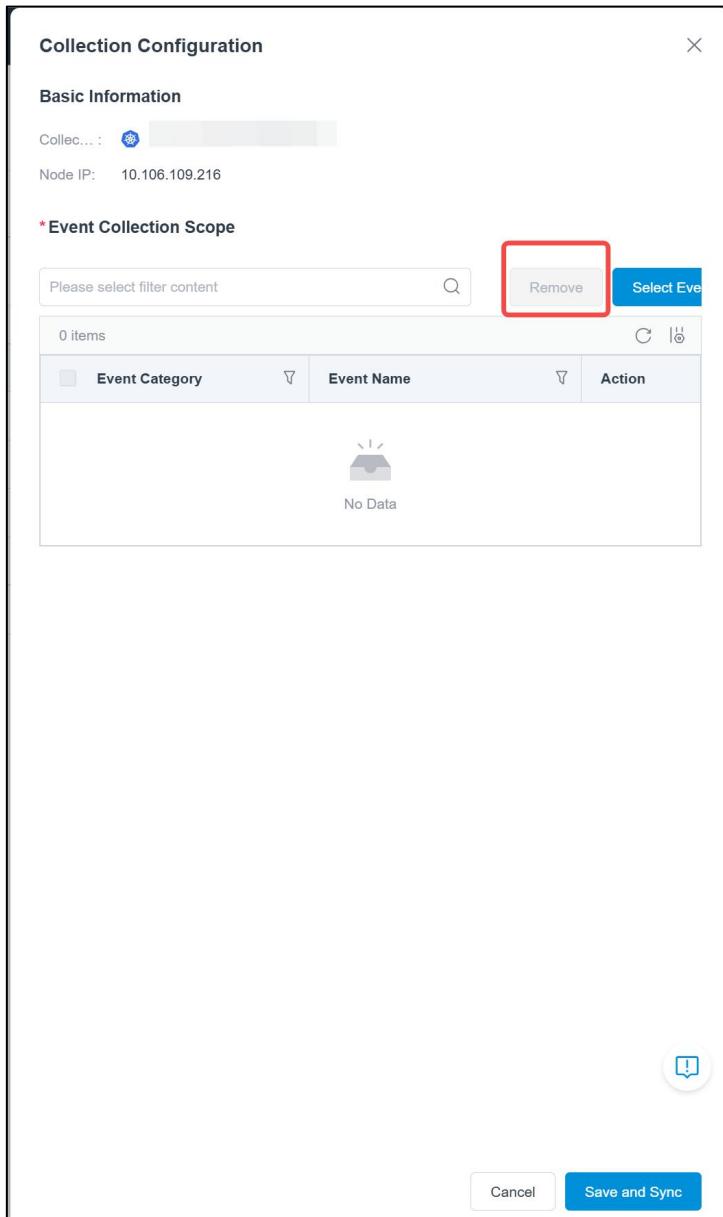


- Select multiple hosts/PCs, click "**Batch Configuration**", then in the event collection scope, click "**Select Events**". After choosing the events, select the "**Remove Selected Events**" button.



Navigate to [Asset Perspective Configuration] and select the "Cluster Perspective" tab

- Select a single cluster, click "**Collection Configuration**" to view all events collected by the cluster. In the event collection scope list, click the "**Remove**" button in the action column to disable collection for that event.
- Alternatively, check the boxes for multiple events and click "**Remove**" to perform batch event removal.



8.9.2. Disable event collection by event category

To disable event collection on an event-specific basis, the operations on the three pages—【Host Event Configuration】，【Container Event Configuration】，and 【Endpoint Event Configuration】—are the same. Using the 【Host Event Configuration】 page as an example, note that this operation only supports single-event actions.

Go to 【Host Event Configuration】，and in the event list:

- Select a single event, click the statistical number under the "Collection Scope" for that event,

then in the host collection scope, select the hosts from which event collection needs to be disabled, and finally click the "Remove" button in the upper right corner of the list.

The screenshot shows the Sentry CWPP interface for Host Event Configuration. On the left, there's a sidebar with navigation links like Asset, Intrusion Detection, Ransom Protection, Risk Discovery, Compliance, Event Collection (which is selected), Security Control, DevSecOps, and Micro Segmentation. Below this is a breadcrumb trail: Event Collection > Event Collection Configuration > Host Event Configuration. The main area is titled 'Host Event Configuration' and has tabs for 'Linux Events' (selected) and 'Windows Events'. On the left, under 'Event Classification (9)', there's a search bar and a list of event types: Account Manage... (10), Bash Event(1), File Event(14), Account Login Log... (2), Module Event(3), Network Event(3), Process Event(5), System Service Ev... (2), and USB Device Event(2). Each item has a checkbox and a 'Collection Scope' value. A red box highlights the 'User account change event' entry with a scope of 15. To the right, there's a 'Collection Host Range' section with a table showing 15 items. The table columns are Host, Business Group, Collection Status, Collection Exc..., and Action. Each row has a 'Remove' button in the Action column. A red box highlights the 'Selected Host' button at the top right of the table header. The table also includes a search bar, filter icons, and pagination controls.

9. Security Control

9.1. Control Event

This function displays various alarm information of the security management module, including peripheral control, file control, and process control. You can filter the alarm according to the alarm type, danger level, alarm status, alarm time, and other conditions, and mark the alarm status according to the handling research and judgment.

Steps:

- Filter alarm data based on alarm type, danger level, alarm status, alarm time, and other conditions.
- Click View Details to view the details of the alarm.
 - For peripheral control alarms, the details include detection information, device information, and handling suggestions.
- Alarm markers:
 - Single mark: Click the drop-down list in Alarm Status to mark the alarm data as processing, confirmed, or ignored based on the actual analysis situation
 - Batch tagging:
 - Select the list data and click "Mark" to mark all the selected data in a unified state. For alarms that have been marked as acknowledged, ignored, or in process, the alarm status will be overwritten after all alarms are marked.
 - After filtering the list data, click "Mark All" to mark all the filtered results in a unified state. For alarms that have been marked as acknowledged, ignored, or

in process, the alarm status will be overwritten after all alarms are marked.

- Data export: You can select and export lists in batches or export selected data.

Control Event

The screenshot shows the Control Event interface. At the top, there is a summary table with columns for Risk Level, Alarm Type, Alarm status, and Alarm time. Below this is a detailed list of 16 items, each with columns for Risk Level, Alarm time, Alarm Type, Alarm description, Affected devices, and Operation. Each item in the list includes a 'View Details' link.

Risk Level	Alarm Type	Alarm status	Alarm time
Critical Risk	Red list process terminated in violation	Pending processing	Last 1 hour
High Risk	Unauthorized write to device	True Positive	Last 1 day
Medium Risk	Custom file changes	False Positive	Last 7 days
Low Risk	Peripheral illegally inserted into host		Last 30 days
	System core file changes		

Risk Le...	Alarm time	Alarm Type	Alarm description	Affected devices	Operation
Low Risk	2025-06-24 16:05:09 2025-06-24 16:05:09	Red list process terminated in violation	Red list process PING.EXE terminated in violation	100.64.3.43 DESKTOP-I2C531M	View Details
Low Risk	2025-06-24 15:52:10 2025-06-24 15:52:10	Red list process terminated in violation	Red list process PING.EXE terminated in violation	100.64.3.43 DESKTOP-I2C531M	View Details
Low Risk	2025-06-24 15:52:10 2025-06-24 15:52:10	Red list process terminated in violation	Red list process PING.EXE terminated in violation	100.64.3.43 DESKTOP-I2C531M	View Details
Low Risk	2025-06-24 15:42:46	Red list process terminated in violation	Red list process PING.EXE terminated in violation	100.64.3.43 DESKTOP-I2C531M	View Details

9.2. Peripheral Control

The peripheral management and control function supports monitoring and logging of the activities of hardware devices and hardware ports, identifies basic information of devices, and intercepts and protects unauthorized devices from unauthorized access and writes, and provides alarm notifications, so as to facilitate timely detection of risk problems and prevent host business information leakage and virus infection.

9.2.1. Peripheral Policies

It can monitor the behavior of hardware devices and hardware ports accessing the host, and control the use rights of hardware devices on the host and provide alarms for violations. You can set a default policy that takes effect globally, or you can set a custom policy with a higher priority for the host in a specified range, and specify the validity period of the policy.

The following peripherals are supported:

- Hardware devices include: USB storage devices (such as USB flash drives, mobile hard disks,

mobile phones, memory cards, etc.), Bluetooth, cameras, optical drives, etc. You can control the enable, disable, and write ban permissions of the device.

- Hardware ports include: USB port. You can control the permissions to enable and disable ports.

The following device permissions can be set:

- Enabled: Allows access and write to the device
- Disabled: Access is not allowed, and the device will be automatically popped up and alarms and notifications will be performed
- Write-Prohibited: If the device permission is set to Write-Prohibit, the preceding behaviors are blocked and an alarm is generated

Write device behaviors include: copying files from the host to the USB flash drive, creating new files in the USB flash drive, creating a new file directory in the USB flash drive, deleting files in the USB flash drive, modifying the contents of files in the USB flash drive, and renaming files in the USB flash drive.

Note:

The peripheral management function supports driver and non-driver modes, and the specific differences are as follows:

- **When the driver is not turned on:**
 - Linux hosts: Only non-driver solutions are supported. The insertion and unplugging of controlled devices is supported, but the writing behavior of controlled devices is not supported.
 - Windows host: only supports the insertion and unplugging behavior of controlled

devices, but does not support the behavior of controlling and writing devices.

Identification of exception devices is not supported.

- If the driver and driver event source are enabled: (The Windows host needs to restart the driver after it is enabled)

- Windows host: supports the insertion, unplugging, and reading and writing behaviors of controlled devices, and supports the identification of exception devices.

Peripheral Strategy

Default policy

Status	Application Scope	Policy Description	Control validity period	Last modified time
<input checked="" type="checkbox"/>	10.106.110.181 50	The default policy that applies globally has a lower priority than custom policies.	Permanent	2025-07-04 14:48:12

Custom policy

Customize policy scope priority: Select hosts by list > Select hosts by business group. Duplicate configurations are not allowed, meaning a host will only apply one policy.						
<input type="text"/> Please enter a search item <input type="button" value="Search"/> Delete Disable Enable <input type="button" value="New"/> ☰						
Is it enabled?	Policy Name	Policy Descr...	Application Scope	Strategy validity period	Last modified time	Operation
<input checked="" type="checkbox"/>	test	-	10.106.110.240 1	Permanent	2025-07-04 14:50:09	Edit Delete
1 items						



1. If you need to set a comprehensive control policy for the global scope, you can configure the default policy. Steps:

- Enable the default policy and configure the policy content, which takes effect for all hosts and is valid for permanent.
- The default policy takes precedence over the custom policy.

2. If you need to set a specific policy for a small range of hosts, you can click "New" to configure a custom policy. Steps:

- Custom Policy Scope Priority: Select hosts by list > Select hosts by business group. It is configured with a host range that does not allow duplication, that is, only one policy will be applied to a host.
- Basic policy information: whether the policy is enabled, name, description, and validity

period. If the policy expires, the control becomes invalid.

- Scope of policy application
- Policy content: Click on the device type to select the USB device and hardware port to set permissions



3. For specific blacklist and whitelist devices, they can be added to the exception policy, and the system will identify and control them according to the device serial number and the manufacturer/product ID of the device. Steps:

- In the global policy or custom policy, click Add in the Exception Device information area and fill in the device information and device permissions
- You can add devices by serial number, vendor ID, or product ID
 - Known device information: You can enter it directly
 - Unknown device information: You can insert the device into the host where the agent is installed, and the system will collect and report the device information and record it in the peripheral logs.

The screenshot shows the Sentry CWPP interface. On the left, there's a navigation bar with tabs like Asset, Intrusion Detection, Ransom Protection, Risk Discovery, and More. Below the navigation is a section titled 'Create a custom policy'. It lists 'USB camera' and 'USB optical drive' under 'Hardware port' with a plus sign to add more. A note says 'Please select an external device from the peripheral log'. On the right, a modal window titled 'Add exceptional device(s)' is open. It has two radio buttons: 'By serial number' (selected) and 'By Manufacturer ...'. Below this is a section for 'Equipment information' with a text input field 'Equipment ...:' and a placeholder 'Please enter the device serial number'. Under 'Device permissions', there's a note 'To recognize exception devices on Windows hosts, the driver function must be enabled, and the host needs to be restarted to take effect.' There's a table for 'Exceptional devices' with columns 'Equipment serial number', 'Manufacturer ID', and 'Product ID'. The table shows 'No Data'. At the bottom of the modal are 'Cancel' and 'Save' buttons.

9.2.2. Peripheral Logs

It monitors and logs the insertion and withdrawal of hardware devices on terminals, and analyzes how many devices have been connected to a host and how many hosts a device has been connected to a device by aggregation by host and device dimensions.

Steps:

- You can specify a device type to view the data
- You can switch the aggregation dimension to view the data
- You can view the data based on the relevant search criteria
- List data can be exported

Host	Equipment type	Manufacturer	Product name	Device position	Terminal	Operation time
100.64.2.196 STMM	Unknown typ...	-	USB Type-C ...	Read Write	Device inser...	2025-06-30 17:31:5
100.64.2.196 STMM	Unknown typ...	AUDITORYW...	Hamedal Spe...	Read Write	Device pulli...	2025-06-30 17:30:1
100.64.2.196 STMM	Unknown typ...	AUDITORYW...	Hamedal Spe...	Read Write	Device inser...	2025-06-30 16:56:4
100.64.2.196 STMM	Unknown typ...	-	USB Type-C ...	Read Write	Device inser...	2025-06-30 11:42:2
100.64.2.196 STMM	Unknown typ...	AUDITORYW...	Hamedal Spe...	Read Write	Device pulli...	2025-06-30 11:39:0
100.64.2.196 STMM	Unknown typ...	AUDITORYW...	Hamedal Spe...	Read Write	Device inser...	2025-06-30 11:28:6
100.64.2.196 STMM	Unknown typ...	-	USB Type-C ...	Read Write	Device inser...	2025-06-26 17:48:1
100.64.0.228 HAOJIE	Unknown typ...	AUDITORYW...	Hamedal Spe...	Read Write	Device pulli...	2025-06-26 15:26:5
100.64.0.228 HAOJIE	Unknown typ...	AUDITORYW...	Hamedal Spe...	Read Write	Device inser...	2025-06-26 14:29:4

9.2.3. Peripheral Alarm Notifications

Alarms are intercepted and notified of device violations that hit the policy, and multiple notification methods are supported. Steps:

- Click the icon on the right side of the top bar of the system to view the relevant alarm

notifications, view the message details, and mark the message status.



- Click to enter the message configuration page, you can configure the notification of

peripheral control events according to the alarm type, and support the methods of internal message, email, SMS, and group robot.



Security Control	Batch Set Receiving Method	Batch Set Receiver	Batch Set Group Robot	<input checked="" type="checkbox"/>
Aggregated Alert				Edit
Receive M... : Website Message, Email, SMS Message, Group Robot Receive Gr... : [509] 10.106.110.123	Receiver:	admin		
Process Control-Black list process startup				Edit
Receive M... : Website Message, Email, SMS Message, Group Robot Receive Gr... : -	Receiver:	admin		
Device Insertion Illegally				Edit
Receive M... : Website Message, Email, SMS Message, Group Robot Receive Gr... : [509] 10.106.110.123	Receiver:	admin		
Write to Device Illegally				Edit 
Receive M... : Website Message, Email, SMS Message, Group Robot Receive Gr... : [509] 10.106.110.123	Receiver:	admin		
File Control-Customize file changes				Edit

9.3. File Control

File Control allows users to add monitoring and protection policies and including whitelists for System core files, Web tamper-proof, web middleware configuration, and custom policy. Any abnormal file operations will be logged, alerted, or blocked to prevent malicious tampering with critical website configurations, directory files, and core system configurations on the device.

Generated alerts will be displayed in the Control Events section.

9.3.1. File Control Strategy

Users can create, enable, or disable file monitoring and protection policies for the following scenarios:

- System core files
- Web tamper-proof
- Web middleware configuration
- Custom policy

Supported actions: Enable, disable, edit, delete, create new policies, and view associated records.

Policy Matching: The most recently updated policy takes priority. If multiple policies apply to the same file, the priority order is: Interception Mode > Alert Mode > Observation Mode.

Protection Strategies: Users can apply the three protection strategies in different scenarios:

- **Observation Mode:**

Scenarios:

-

- Risk assessment period: Before deploying a new strategy, first observe which users/departments frequently trigger the rules to avoid misjudgment.
- Compliance audit: Record the traces of file operations (e.g., who accessed customer data).
- Strategy verification: Test whether new rules cover real risks (for example: monitor the behavior of "uploading files to network disks").

Operation: No blocking occurs; users can operate normally. The system silently generates logs for post-event analysis, which can be viewed in associated events.

- **Alert Mode:**

Scenarios:

-

- Moderate-risk operations: For example, an employee attempts to send a file classified as "internal" to external partners via email.
- Scenarios requiring evidence retention: Record violations (such as an employee copying customer data) and notify the security team to provide a basis for subsequent accountability.

- High tolerance for false positives: Operations are suspicious but may have reasonable causes (e.g., financial personnel need to send encrypted reports to banks).

Operation: The operation can continue to be completed, but the administrator will be notified in real-time (via email/SMS).

- **Interception Mode:**

Scenarios:

-

- Core data protection: Prevent the leakage of source codes, trade secrets, customer databases, etc., through channels such as USB drives and network disks.
- Clear violations: For example, attempting to upload files to prohibited applications (such as personal network disks) or sending emails to blacklisted domains.
- Legal mandatory requirements: Involving personal privacy (e.g., an employee arbitrarily exporting users' ID card numbers) or financial regulatory data.
- High-risk operations: Ransomware encrypting files, unauthorized processes modifying important documents, etc.

Operation: Real-time forced blocking; the user's operation is terminated, and detailed logs are recorded (viewable in control events).

Viewing Policy Associated Records:

- Alert/Interception Mode: Associated records in Alert or Block Mode support querying the following fields: Risk level; Alarm description; Alarm time; Host IP; Alarm status.
- Observation Mode: Associated records in Observation Mode only support querying: Last update time; Alarm description; Host IP.

1. Associated Records in Alert Mode and Interception Mode:

Associated records

Multiple filter tags are separated by the Enter key.

Risk Level	Alarm time	Alarm Type	Alarm desc...	Affected devices	Operation
Critical Risk	2025-05-22 19:58:05	Custom file changes	The process mv was found to rename the file /opt/sc_test/test111_2 to /opt/sc_test/test111_1	192.168.252.130 junw(Default Busi...)	View Details
Critical Risk	2025-05-22 18:09:19	Custom file changes	The process mv was found to rename the file /opt/sc_test/test2 to /opt/sc_test/test2_2	192.168.252.130 junw(Default Busi...)	View Details
Critical Risk	2025-05-22 18:04:54	Custom file changes	The process mv was found to rename the file /opt/sc_test/test111_1 to /opt/sc_test/test111_2	192.168.252.130 junw(Default Busi...)	View Details

3 items

Click View Details to access: Detection Information; Process Chain Information; File Information;

Suggestions for Handling; The interface also supports adding the item to a whitelist.

Critical Risk Custom file changes Rename the file is blocked

The process mv was found to rename the file /opt/1.txt to /opt/2.txt

Add to whitelist	True Positive
<input checked="" type="checkbox"/>	True Positive

Detection information

- Alarm time: 2025-05-22 18:26:18 — 0 times — 2025-05-22 18:26:18
- Alarm ID: 682efbcad3f3755a7603ba7c
- Hit strate...: gyw-Custom policy
- Respons...: Block Succeeded
- Affected ...: 10.42.0.0 | lirui(lirui的业务组)
- File oper...: Rename
- Original f...: /opt/1.txt
- Current f...: /opt/2.txt

Process Chain Information

file information

Suggestions for handling

Check whether it is a normal file change operation and adjust the file control strategy or add to the whitelist as needed

2.Associated records in observation mode:

Associated records

Multiple filter tags are separated by the Enter key.

Last update time	Behavior description	Affected devices	Type
2025-06-18 11:58:21	The process rm performed D elete operation on the file /op t/abc	192.168.70.129 localhost.localdomain(Default B...)	Custom file changes
2025-06-18 11:58:36	The process mv was found t o rename the file /opt/abc to / opt/dd	192.168.70.129 localhost.localdomain(Default B...)	Custom file changes

2 items

Create New Policies: Supports policy creation based on specific protection scenarios.

After clicking Confirm, the configuration details are displayed on the right panel for editing or policy creation.

Create New Policy

Supports quick creation of file directory protection policies through application scenarios and custom methods.

- System core file**
E.g., /etc/passwd in Linux and C:\Windows\System32 in Windows
- Web tamper-proof**
E.g., /var/www/example.com/ for Linux web sites and C:\Websites\example.com in Windows
- Web middleware configuration**
E.g., /conf/server.xml for Tomcat and /WEB-INF/web.xml for Jetty
- Custom policy**
Support custom file directory protection policies

Cancel Confirm

Scenario 1: System Core Files

System core file management refers to the protection strategies set for system core files (such as kernels, system libraries, configuration files, executable programs, etc.) to prevent unauthorized tampering, malicious deletion, or illegal access. After selecting system core files on the new creation

page and clicking Confirm, the specific operation steps are as follows:

1. Basic Information:

Users can enable or disable this policy. They can also change the policy status in the policy list after creation. Fill in the policy name, policy description, and select the device types to be managed (Linux; Windows; Containers).

2. Trigger Conditions:

Click "Select System Core Files" to import the files to be managed. The file data comes from the system's default configuration, and up to 100 directory paths can be imported. Provide users with 6 system file templates (different templates for Linux and Windows), supporting filtering by template name. Click "View Details" to see specific paths, supporting filtering by path.

Select the file operations that need to be monitored. Once a configured file undergoes the selected operations, the protection policy will be automatically triggered.

Exclusion Settings: Users can customize exclusions for process files, subdirectories, specified files, and file types. After exclusion, the policy will not take effect on these paths and file types.

Select System core files

The following data comes from default system configurations. You can import up to 100 directory paths. Configure protection policies for system core files carefully.

All (6 items)	Selected (0 items)
<input type="checkbox"/> Template name	
<input type="checkbox"/> Startup directory file m... Linux 8	View Details
<input type="checkbox"/> Scheduled task monito... Linux 15	View Details
<input type="checkbox"/> User account passwor... Linux 13	View Details
<input type="checkbox"/> Kernel module monitori... Linux 14	View Details
<input type="checkbox"/> System and package ... Linux 6	View Details
<input type="checkbox"/> Executable file director... Linux 4	View Details

No Data

Cancel Save

Select System core files

The following data comes from default system configurations. You can import up to 100 directory paths. Configure protection policies for system core files carefully.

All (6 items)		
Please enter a search item		
6 items		
<input type="checkbox"/> Template name	<input type="checkbox"/> Platform type	Num
<input type="checkbox"/> Startup directory file m... Linux 8		
<input type="checkbox"/> Scheduled task monito... Linux 15		
<input type="checkbox"/> User account passwor... Linux 13		
<input type="checkbox"/> Kernel module monitori... Linux 14		
<input type="checkbox"/> System and package ... Linux 6		
<input type="checkbox"/> Executable file director... Linux 4		

Details

Basic Information

Templ... : Startup directory file monitoring
Descri... : Monitor startup items in startup directories and their loaded files

Path list

Path
/boot/
/etc/bashrc
/etc/depmod.d
/etc/modules-load.d/
/etc/profile
/etc/profile.d/
/etc/rc.d/
/sbin/modprobe

3. Protection Strategy: Users select a protection strategy according to their own needs.

4. Application Scope: Select the scope of hosts or business groups where the strategy is to be deployed.

Scenario 2: Web tamper-proof

Web tamper-proof is an active defense technology aimed at real-time monitoring and protecting the integrity of website pages (such as static files like HTML, JS, CSS, images, etc.), preventing them from being illegally modified by hackers, implanted with malicious code, or having their content replaced. Its core goal is to ensure that webpage content is legitimate and trustworthy, avoiding security risks caused by users accessing tampered pages. The specific operations are as follows:

1. Basic Information:

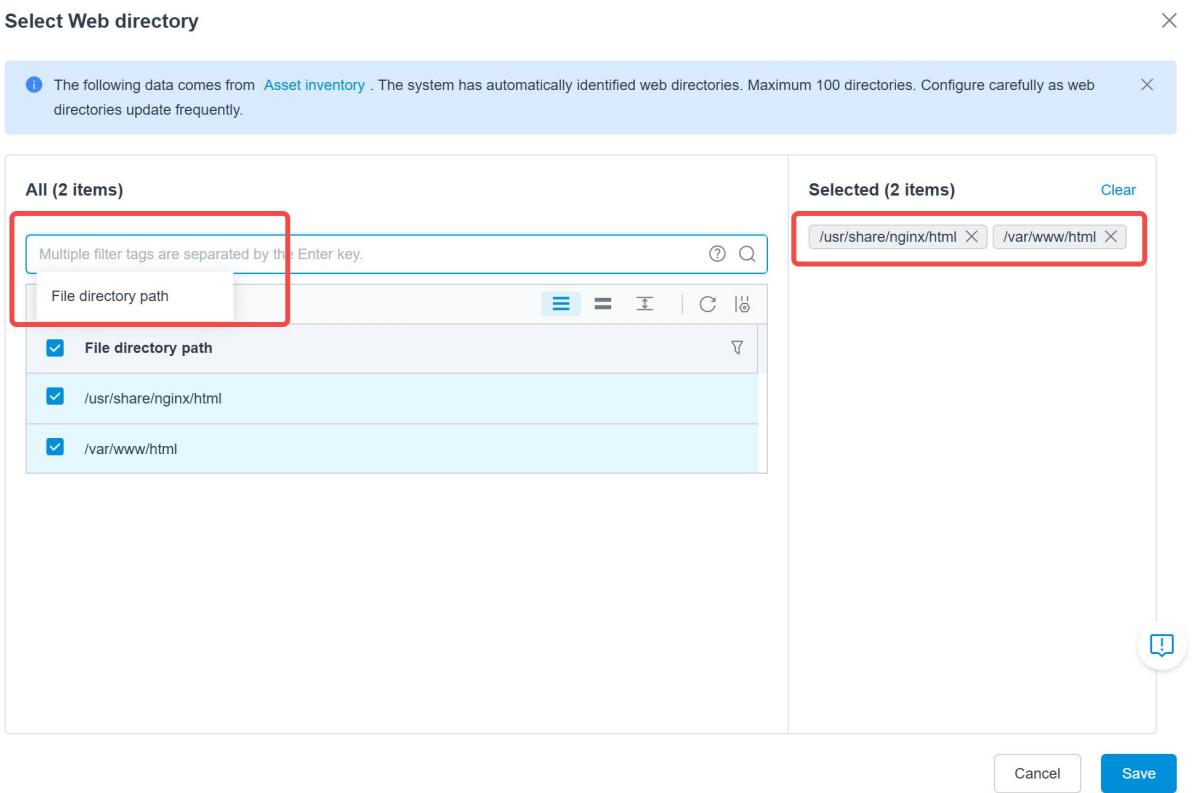
Users can enable or disable this policy, and can also change the policy status in the policy list after creating it. Fill in the policy name and policy description, and select the types of devices to be controlled (Linux; Windows; Containers).

2. Trigger Conditions:

Click "Select Web Directories" to import files. The data comes from asset inventory, which are the web site directories deployed on machines identified by the program. A maximum of 100 directories can be selected, and filtering by file directory path is supported.

Select the file operations to be monitored. Once the configured files perform the selected operations, the protection policy will be automatically triggered.

Exclusion Settings: Users can customize exclusions for process files, subdirectories, specified files, and file types. After exclusion, the policy will not take effect on these paths and file types.



3. Protection Strategy: Users select a protection strategy according to their own needs.

4. Application Scope: Select the scope of hosts or business groups where the strategy is to be deployed.

Scenario 3: Web Middleware Configuration

Manage web middleware configuration files (such as Nginx's nginx.conf, Tomcat's server.xml, etc.) to ensure they are not illegally tampered with, deleted, or accessed beyond authorized permissions, thereby guaranteeing the secure and stable operation of the middleware. The specific operation steps are as follows:

1. Basic Information:

Users can enable or disable this policy, and can also change the policy status in the policy list after creation. Fill in the policy name, policy description, and select the device types to be managed (Linux; Windows; Containers).

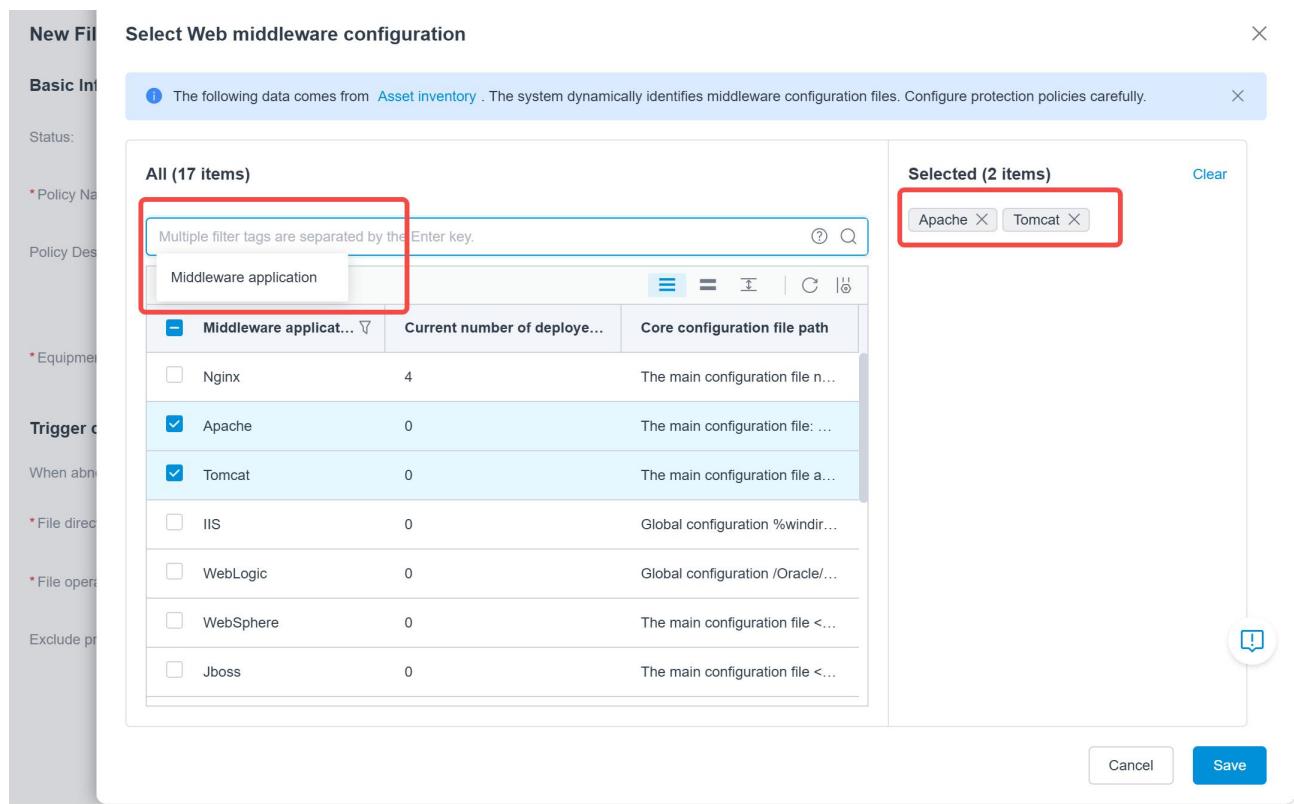
2. Trigger Conditions:

Click to select "Web Middleware Configuration". The data comes from asset inventory, and the program dynamically identifies middleware-related configuration files deployed on the machine.

Filtering by middleware application is supported.

Select the file operations to be monitored. Once the configured files undergo the selected operations, the protection policy will be automatically triggered.

Exclusion Settings: Users can enter process file directories to exclude process files. After exclusion, the policy will not take effect on these paths.



3. Protection Strategy: Users select a protection strategy according to their own needs.

4. Application Scope: Select the scope of hosts or business groups where the strategy is to be deployed.

Scenario 4: Custom Policy

Users can customize file and directory protection policies. The specific operation steps are as follows:

1. Basic Information:

Users can enable or disable this policy, and can also change the policy status in the policy list after creation. Fill in the policy name, policy description, and select the device types to be managed (Linux; Windows; Containers).

2. Trigger Conditions:

Users enter the absolute paths of files or directories. Among them, directories support up to 10 levels, and multiple values can be entered, with a maximum of 100 values.

Select the file operations to be monitored. Once the configured files perform the selected operations, the protection policy will be automatically triggered.

Exclusion Settings: Users can enter process file directories to exclude process files. After exclusion, the policy will not take effect on these paths.

3.Protection Strategy: Users select a protection strategy according to their own needs.

4.Application Scope: Select the scope of hosts or business groups where the strategy is to be deployed.

9.3.2. Alarm list

In a management event, different alarm types are assigned to different application scenarios.

- System Core Files: System core files changes
- Web Tamper Proof: web page files changes
- Web Middleware Configuration: web middleware configuration changes
- Custom policy: Custom file changes

Control Event

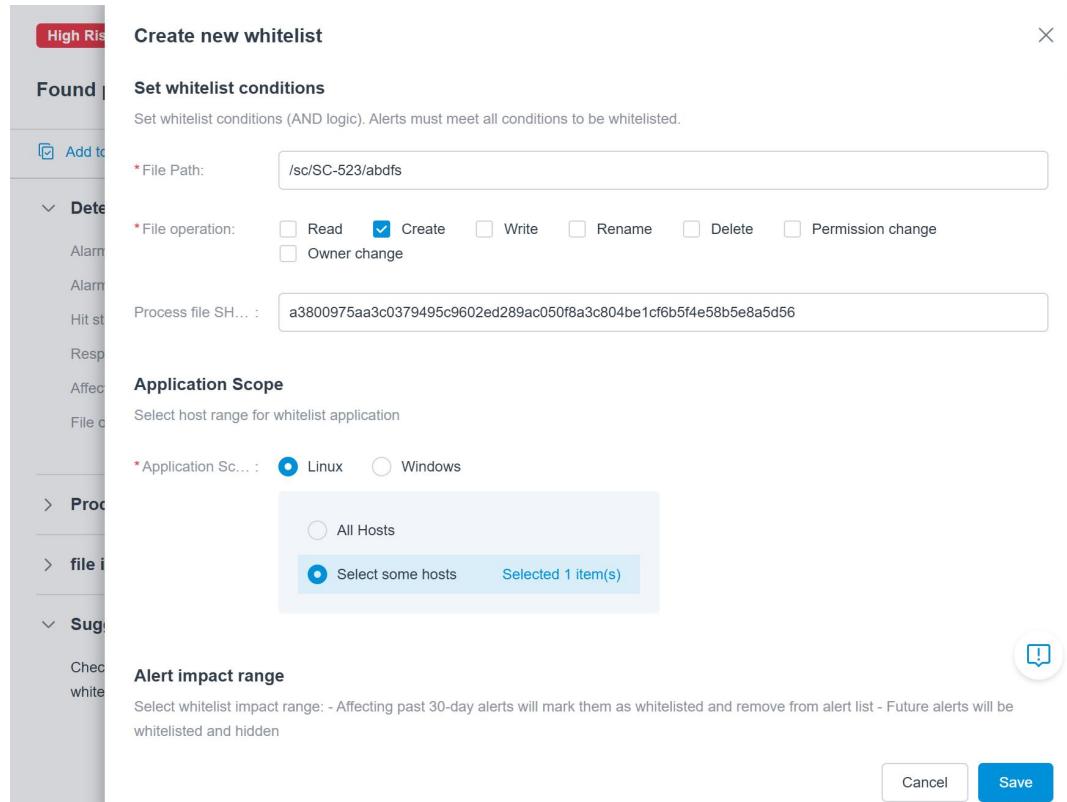
The screenshot shows the 'Control Event' section of the Sentry CWPP interface. At the top, there are filters for 'Alarm time: 2025-04-23 1...' and 'Alarm Type: web page file...'. Below the filters are four sections: 'Risk Level', 'Alarm Type', 'Alarm status', and 'Alarm time'. The 'Alarm Type' section has a red box around the 'System core file changes' row. The 'Alarm time' section also has a red box around the same row. Below these sections is a table with 8 items, showing columns for Risk Level, Alarm time, Alarm Type, Alarm description, Affected device, and Operation. Two rows are highlighted with red boxes: the first row for 'High Risk' with 'Custom file changes' and the second row for another 'High Risk' entry.

Risk Level	Alarm Type	Alarm status	Alarm time
Critical Risk (21)	Peripheral illegally inserted into ... (2)	Pending (28)	Last 1 hour (0)
High Risk (13)	Unauthorized write to device (0)	processing (0)	Last 1 day (8)
Medium Risk (2)	System core file changes (0) 	True Positive (12)	Last 7 days (19)
Low Risk (0)	web page file changes (0) 	False Positive (0)	Last 30 days (40)

Risk Level	Alarm time	Alarm Type	Alarm description	Affected device	Operation
High Risk	2025-05-16 10:49:21 2025-05-16 10:49:21	Custom file changes	Found process touch creating file /sc/SC-523/abdfs	192.168	View Details
High Risk	2025-05-09 16:48:09 2025-05-09 16:48:09	Custom file changes	Found process touch creating file /sc/SC-523/abcdfsa	192.168	View Details

On the alarm details page: Users can view detection information, process chain information, file information, and processing suggestions. Supports adding to the whitelist.

The screenshot shows the 'alarm details' page for a 'High Risk' event. The event is identified as 'Custom file changes' and is described as 'Found process touch creating file /sc/SC-523/abdfs'. The status is 'Pending'. The page is divided into several sections: 'Detection information' (including alarm time, ID, hit rate, response, affected device, and file operation), 'Process Chain Information', 'file information', and 'Suggestions for handling'. A note in the 'Suggestions for handling' section suggests checking if it's a normal file change operation and adjusting the file control strategy or adding to the whitelist.



9.3.3. File White List

Users can add blank to the operation of specified files by creating a new entry on the current list page and confirming the addition on the alarm details page. After whitening, it will not be alerted or blocked.

The whitelist supports filtering by whitelisting criteria, host IP addresses, and update timestamps.

Users can view detailed information including whitelisting conditions, device types, scope of application, associated alerts and so on.

Multiple filter tags are separated by the Enter key.

Whitelist conditions	Device type	Application scope	Affected alerts	Remarks	Update time	Operation
<input checked="" type="checkbox"/> 文件路径:/o... <input checked="" type="checkbox"/> 文件路径:D:... <input checked="" type="checkbox"/> 文件路径:D:... <input checked="" type="checkbox"/> 文件路径:D:... <input checked="" type="checkbox"/> 文件路径:/o... <input checked="" type="checkbox"/> 文件路径:/o...	Linux <input checked="" type="checkbox"/> 192.168.252.130 <input checked="" type="checkbox"/> 192.168.57.158 <input checked="" type="checkbox"/> 192.168.252.130 <input checked="" type="checkbox"/> 192.168.252.131 <input checked="" type="checkbox"/> 10.42.0.0	<input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 1	-	2025-05-22 19:59:22	Edit Delete	
<input checked="" type="checkbox"/> 文件路径:/o... <input checked="" type="checkbox"/> 文件路径:D:... <input checked="" type="checkbox"/> 文件路径:D:... <input checked="" type="checkbox"/> 文件路径:D:... <input checked="" type="checkbox"/> 文件路径:/o... <input checked="" type="checkbox"/> 文件路径:/o...	Linux <input checked="" type="checkbox"/> 192.168.252.130 <input checked="" type="checkbox"/> 192.168.57.158 <input checked="" type="checkbox"/> 192.168.252.130 <input checked="" type="checkbox"/> 192.168.252.131 <input checked="" type="checkbox"/> 10.42.0.0	<input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 1	-	2025-05-22 18:08:02	Edit Delete	
<input checked="" type="checkbox"/> 文件路径:/o... <input checked="" type="checkbox"/> 文件路径:D:... <input checked="" type="checkbox"/> 文件路径:D:... <input checked="" type="checkbox"/> 文件路径:D:... <input checked="" type="checkbox"/> 文件路径:/o... <input checked="" type="checkbox"/> 文件路径:/o...	Windows <input checked="" type="checkbox"/> 192.168.252.130 <input checked="" type="checkbox"/> 192.168.252.131 <input checked="" type="checkbox"/> 192.168.252.131 <input checked="" type="checkbox"/> 192.168.252.131 <input checked="" type="checkbox"/> 10.42.0.0	<input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 1	-	2025-05-22 17:50:53	Edit Delete	
<input checked="" type="checkbox"/> 文件路径:/o... <input checked="" type="checkbox"/> 文件路径:D:... <input checked="" type="checkbox"/> 文件路径:D:... <input checked="" type="checkbox"/> 文件路径:D:... <input checked="" type="checkbox"/> 文件路径:/o... <input checked="" type="checkbox"/> 文件路径:/o...	Windows <input checked="" type="checkbox"/> 192.168.252.130 <input checked="" type="checkbox"/> 192.168.252.131 <input checked="" type="checkbox"/> 192.168.252.131 <input checked="" type="checkbox"/> 192.168.252.131 <input checked="" type="checkbox"/> 10.42.0.0	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 1	-	2025-05-22 17:48:43	Edit Delete	
<input checked="" type="checkbox"/> 文件路径:/o... <input checked="" type="checkbox"/> 文件路径:D:... <input checked="" type="checkbox"/> 文件路径:D:... <input checked="" type="checkbox"/> 文件路径:D:... <input checked="" type="checkbox"/> 文件路径:/o... <input checked="" type="checkbox"/> 文件路径:/o...	Linux <input checked="" type="checkbox"/> 192.168.252.130 <input checked="" type="checkbox"/> 192.168.57.158 <input checked="" type="checkbox"/> 192.168.252.130 <input checked="" type="checkbox"/> 192.168.252.131 <input checked="" type="checkbox"/> 10.42.0.0	<input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 0 <input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 1	-	2025-05-22 17:38:09	Edit Delete	

6 items

operate : Edit, delete, Create whitelist

Create or edit whitelist: Users fill in whitelisted file information (file path, file operation, etc.), and can choose whether to affect alarm records from the past 30 days. If the option to affect alarms from the past 30 days is selected, the previous alarms will be marked as whitelisted and removed from the alarm list; users need to view them in the whitelist list. At the same time, new alarms in the future will be whitelisted and not displayed.

Create new whitelist

Set whitelist conditions
Set whitelist conditions (AND logic). Alerts must meet all conditions to be whitelisted.

* File Path:

* File operation: Read Create Write Rename Delete Permission change
 Owner change

Process file SH... :

Application Scope
Select host range for whitelist application

* Application Sc... : Linux Windows
 All Hosts
 Select some hosts Please select

Alert impact range
Select whitelist impact range: - Affecting past 30-day alerts will mark them as whitelisted and remove from alert list - Future alerts will be whitelisted and hidden

Alert impact range

Select whitelist impact range: - Affecting past 30-day alerts will mark them as whitelisted and remove from alert list - Future alerts will be whitelisted and hidden

Alert impact range: Only affect current and future alerts Affect past 30-day alerts

Remarks

Remarks:



Whitelist Synchronization:

1. The driver whitelist created from the list page has a synchronization button on the page after saving, and it will be synchronized immediately after clicking it (at this time, the data created from the list and alarm details page will be synchronized).

2. The whitelist created from the details page will be synchronized regularly (once every 5 minutes).

Logic for the whitelist to take effect:

1. The agent only applies the whitelist in the blocking mode, and will not report the blocking alarm if

the whitelist is matched.

2. The server only applies the whitelist in the alert mode, and if the alarm reported by the agent hits the alarm mode, the server will add the whitelist, and the alarm will be displayed in the file whitelist - affected alarm record.

File White List

Supports creating whitelists through manual entry or confirming from alert details. Whitelisted file operations will not trigger alerts or blocks.

File White List						
6 items						
<input type="checkbox"/> Whitelist ...	Device type Application scope	Affected alerts	Remarks	Update time	Operation	
<input type="checkbox"/> File Path:/o...	Linux 192.168.252.130	⚡ 0	-	2025-05-22 19:59:22	Edit Delete	
<input type="checkbox"/> File Path:/o...	Linux 192.168.57.158	⚡ 0	-	2025-05-22 18:31:10	Edit Delete	
<input type="checkbox"/> File Path:/o...	Linux 192.168.252.130	⚡ 0	-	2025-05-22 18:08:02	Edit Delete	
<input type="checkbox"/> File Path:D:...	Windows 192.168.252.131	⚡ 0	-	2025-05-22 17:50:53	Edit Delete	
<input type="checkbox"/> File Path:D:...	Windows 192.168.252.131	⚡ 1	-	2025-05-22 17:48:43	Edit Delete	
<input type="checkbox"/> File Path:/o...	Linux 10.42.0.0	⚡ 1	-	2025-05-22 17:38:09	Edit Delete	

9.4. Process Control

The process management and control function supports monitoring processes in hosts and containers. It allows customizing process blacklists and whitelists to implement process management and control strategies that meet users' protection scenarios. When a blacklisted process is started or is running in the system, a management and control alert will be generated or the process will be blocked for security management and control. It protects security - type and monitoring - type software that are running processes on the whitelist in the system.

9.4.1. Process Control Strategy

9.4.1.1. Process Blacklist

Set up process blacklist strategies. When a blacklisted process is started, security management and

control will be carried out. When the same process matches multiple strategies, it will be handled according to the one with a higher priority, and blocking takes precedence over alerting.

For existing strategies, they can be enabled or disabled to flexibly manage whether the strategy takes effect. Disabled strategies will not be used for process matching. If the content of a strategy needs to be modified, it can be edited on the original basis. After saving, process matching will be carried out according to the modified strategy content. If a strategy is no longer needed, it can be directly deleted.

The screenshot shows the Sentry CWPP interface with the 'Process Control' tab selected. The main area displays a table titled 'Process Control Strategy' with two entries:

Status	Risk Level	Policy Name	Policy Descrip...	Device type Application scope	Control met...	Update time	Operator	Operation	
<input checked="" type="checkbox"/>	Enable	High Risk	If-test	-	Container 1	Alert	2025-06-18 12:14:17	admin	Edit Delete
<input checked="" type="checkbox"/>	Enable	Critical Risk	jw-test-win	-	Windows 1	Block	2025-05-20 10:57:51	admin	Edit Delete

New Policy: Fill in Basic Information, Application Scope, and Control Methods

The screenshot shows the 'New process Red List strategy' configuration page. It includes sections for 'Basic Information', 'Application Scope', and 'Strategy content'.

Basic Information:

- Status:
- *Risk L... : Please select hazard level
- *Policy ... : Please enter the policy name
- Policy D...: Please enter a policy description

Application Scope:

- *Applic... : Linux Windows Container
- All Hosts
- Select some hosts Please select
- Select Business Group

Strategy content:

Detailed content is shown in a modal window:

- Buttons: Delete, Enable, Disable, New, Cancel, Save
- Text: Detailed content is shown in a modal window.

(1) Basic Information: Fill in the Policy Name and Select the Policy Risk Level

Basic Information

Status:

* Risk L... :

* Policy ... :
High Risk
Medium Risk
Low Risk

Policy D...:

(2) Application Scope: Select hosts under Linux or Windows. When choosing partial hosts, only the host list within the account's data permissions can be selected.

Application Scope

* Applic... : Linux Windows Container

All Hosts
 Select some hosts
 Select Business Group

(3) Policy Content: Create new process rules. It supports configuring rules for four process conditions: process name, process command line, process file path, and process file SHA256. Select the operator and fill in the condition value according to the requirements of rule judgment. Multiple rules can be configured for one policy.

For existing rules, you can enable or disable them to flexibly manage the rules that need to be run by the policy. Disabled rules will not take effect. If you need to modify a rule, you can edit it on the original basis. After saving, the judgment will be made according to the modified rule. If a rule is not needed, it can be directly deleted.

NewBlacklist process rules X

Basic Information

Rule sw...:

* Rule n... :

Rule configuration

Process conditions	Operator	Condition value
Please select process	Please select a	Multiple condition values separated by commas Delete
Process Name		
Process Command		
Process File Path		
Process File SHA256		

(4) Control Method: The automatic response method when a process matches the corresponding policy. You can choose to alarm or block.

- Alert: When a blacklist process starts, the system will generate a control alarm.
- Block: When a blacklist process starts, security control is carried out by blocking the process.

▼ Control method

- * Control method: Alert
When blacklist process starts: generate control alerts.
 Block
When blacklist process starts: terminate through blocking or other security controls.

9.4.1.2. Process red List

Set the process red list policy. When a process on the red list starts, security protection will be implemented. When the same process matches multiple policies, it will be handled according to the control method with the higher priority. Protection after startup takes precedence over alarming. For existing policies, you can enable or disable them to flexibly manage whether the policy takes effect. Disabled policies will not be used for process matching. If you need to modify the content of a policy, you can edit it based on the original version. After saving, process matching will be carried out according to the modified policy content. If a policy is no longer needed, it can be directly deleted.

The screenshot shows the Sentry CWPP web interface. The top navigation bar includes links for Home, Asset, Intrusion Detection, Ransom Protection, Risk Discovery, Compliance, Event Collection, More, General, Tools (with 678 messages), and a user account for admin. The main content area is titled "Process Control Strategy" under "Security Control". The "Process red list" tab is active. A note says: "Set a red list policy to protect red-listed processes after startup. When multiple policies match the same process, higher priority control methods take precedence - post-startup protection precedes alerts." Below is a table with one row:

Status	Risk Level	Policy Name	Policy Descrip...	Device type Application scope	Control met...	Update time	Operator	Operation
<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable	Low Risk	test	Linux 2	Alert	2025-06-19 18:25:30	admin	Edit Delete

New Policy: Fill in Basic Information, Application Scope, Policy Content, and Control Methods

New process Blacklist strategy

Basic Information

- Status:
- * Risk L... : Please select hazard level
- * Policy ... : Please enter the policy name
- Policy D... : Please enter a policy description

Application Scope

- * Applic... : Linux Windows Container
- All Hosts
- Select some hosts Please select
- Select Business Group

Strategy content

Please enter a search item

(1) Basic Information: Fill in the Policy Name and Select the Policy Risk Level

Basic Information

- Status:
- * Risk L... : Please select hazard level
- * Policy ... : Please enter the policy name
- Policy D... : Please enter a policy description

Risk L... :

- Critical Risk
- High Risk
- Medium Risk
- Low Risk

(2) Application Scope: Select hosts under Linux or Windows. When choosing partial hosts, only the host list within the account's data permissions can be selected.

Application Scope

*Applic... : Linux Windows Container

All Hosts
 Select some hosts Please select
 Select Business Group

(3) Policy Content: Create new process rules. It supports configuring rules for four process conditions: process name, process command line, process file path, and process file SHA256. Select the operator and fill in the condition value according to the requirements of rule judgment. Multiple rules can be configured for one policy.

For existing rules, you can enable or disable them to flexibly manage the rules that need to be run by the policy. Disabled rules will not take effect. If you need to modify a rule, you can edit it on the original basis. After saving, the judgment will be made according to the modified rule. If a rule is not needed, it can be directly deleted.

NewRed List process rules

X

Basic Information

Rule sw... :

* Rule n... :

Rule configuration

Process conditions	Operator	Condition value
<input type="text" value="Please select process"/>	<input type="text" value="Please select a"/>	<input type="text" value="Multiple condition values separated by commas"/> Delete
<input type="checkbox"/> Process Name <input type="checkbox"/> Process Command <input type="checkbox"/> Process File Path <input type="checkbox"/> Process File SHA256		

(4) Control Method: The automatic response method when a process matches the corresponding policy. You can choose to alarm or apply post - startup protection.

- Alert: When a process on the red list stops, a control alarm will be generated.
- Post - start Protection: Rely on enabling the driver; after the process starts, protect its

operation.

▼ **Control method**

- * Control method: Alert
When a red-listed process stops, generate a control alert.
 Post-start Protection
Dependent on driver activation - protects process operation after startup.

10. Web Application Firewall

The Web Application Firewall provides comprehensive traffic security protection for websites, APPs, and containerized applications. This module performs real-time detection and in-depth analysis of HTTP traffic, identifies and blocks malicious characteristics, and forwards the scrubbed safe traffic back to the server. This prevents servers from being maliciously attacked and compromised, protects applications from being trojaned and tampered with, safeguards core data security, and ensures stable business operations.

10.1. Feature Authorization

The Web Application Firewall feature is authorized for Linux, Docker, K8s, and OpenShift Server Agents, as well as Container Security nodes.

The screenshot shows the "Agent" section of the "Installation" page. It highlights the "Server Agent" tab, which is described as "Used for server security protection scenarios, flexibly adapts to various environments". Below this, there are sections for "Linux", "Docker", "Kubernetes", and "OpenShift", each with a red border around its icon. The "Linux" section indicates support for Cent OS, Debian, KylinSec, and others. The "Installation Method" section shows "Command Installation" as the selected option. A note at the bottom states that administrators can pre-configure commands before execution.

Only hosts with Agents that have purchased products including container asset authorization (such as Container Security Posture) and have been assigned the "Web Application Firewall" authorization will possess the Web Application Firewall functionality.

Method 1: Authorize During Agent Installation

Assign authorization during Agent installation. Navigate to the "Probes - Installation - Agent"

interface, select the corresponding operating system and authorization features. For example, using the Server Agent - Linux command installation as a guide.

Agent management > Installation > Agent > Command Installation

Server Agent-Linux-Command Installation

Basic Configuration

Business G...: Default Business Group
If you need to add a business group, please click [Business Group Management](#).

Connection...: Direct Connection (selected) Proxy

Connection...: Default connection address
To add a connection address, click [Connection Address Configuration](#).

Functional Configuration

Installation ...:

- To ensure the normal operation of the system when enabling container security authorization, please make sure that the CPU limit threshold and memory limit threshold of the Agent are not less than 1C and 1000M respectively.

> Host Security		3 item(s) selected
< Container Security		2 item(s) selected
<input type="checkbox"/> Select All	<input checked="" type="checkbox"/> Container Security Posture	<input type="checkbox"/> Container Intrusion Detection and Response
<input type="checkbox"/> Cluster Security Posture	<input type="checkbox"/> Container Security Assurance	<input type="checkbox"/> Container Event Collection
<input checked="" type="checkbox"/> Web Application Firewall		

Method 2: Modify Agent Authorization

After Agent installation, you can modify the authorization information and assign the "Web Application Firewall" authorization. Navigate to the "Probes - Probe Management -License" interface, click "Configuration Authorization", and modify the authorization as shown below:

Agent manag... < Agent management > Running Monitor > License

License

Distribution of Authorization Functions

Authorization Status Statistics

Please Select Filtering Content

95 items

Agent ID	Host	Host Type	Business...	Authorizati...
6e5c388cf150a67f	[redacted]	Server Version	test-an	<input checked="" type="checkbox"/> Host Sec... <input checked="" type="checkbox"/> Host Intr... <input checked="" type="checkbox"/> Host Sec... <input checked="" type="checkbox"/> Host Micr... <input checked="" type="checkbox"/> Host Micr... <input checked="" type="checkbox"/> Container

threshold and memory threshold of the Agent are not less than 1C and 1000M respectively.

Authorization Method: Append (selected) Overwrite Delete

Default Aut...: Server Version

Container Security: Select All

Container Security Posture
 Container Intrusion Detection and Response
 Cluster Security Posture
 Container Security Assurance
 Container Event Collection
 Web Application Firewall (highlighted with a red box)

Micro-segmentation
PC Version

10.2. Attack Alerts

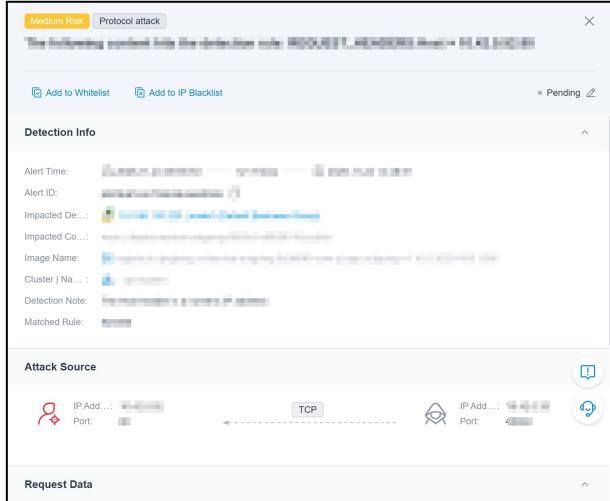
Displays detected alert information and alert details.

- Alert List: Centrally displays all security events.
 - Key information includes: Risk Level, Alert Time, Alert Type, Alert Description, Affected Object, Attack Source, and Alert Status.
 - Filtering: Supports filtering by Alert ID, Time Range, Risk Level, Alert Type, Alert Status, fields related to the Affected Object, Attacker IP, Victim IP, etc.
 - Sorting: Supports sorting by Risk Level (descending), First Alert Time (descending), and Latest Alert Time (descending).
 - Supports batch marking and data export.
- Alert Details: View detailed alert information, including: Detection Information, Attack Source, Request Data, Response Data, and Recommendation etc.
- Alert Status: Supports full lifecycle management of alerts. Statuses include Pending, Progressing, Confirmed, Ignored and White(the latter applies only after an alert has been whitelisted), which can be marked according to the actual situation.
- Add to Blacklist/Add to Whitelist: Apply blacklisting or whitelisting to the current alert. Click to navigate to the drawer for creating a new blacklist/whitelist (see 1.3.3, 1.3.4), with some information automatically filled in.

The screenshot shows the Sentry CWPP interface for the Web Application Firewall (WAF) module. The 'Attack Alerts' section is active. The 'Web Application Firewall' tab is highlighted with a red box. The main area displays a table of alerts with the following columns:

Risk Level	Alert Time	Alert Type	Alert Description	Affected Object	Victim	Attacker	Alert Status
High Risk	2023-01-01 00:00:00 - 2023-01-01 23:59:59	Denial of Service	Denial of service attack detected on port 80. Target IP: 192.168.1.100. Victim IP: 192.168.1.101. Attacker IP: 192.168.1.102.	192.168.1.100	192.168.1.101	192.168.1.102	Pending
Medium Risk	2023-01-01 00:00:00 - 2023-01-01 23:59:59	Denial of Service	Denial of service attack detected on port 80. Target IP: 192.168.1.100. Victim IP: 192.168.1.101. Attacker IP: 192.168.1.102.	192.168.1.100	192.168.1.101	192.168.1.102	Pending
Medium Risk	2023-01-01 00:00:00 - 2023-01-01 23:59:59	Denial of Service	Denial of service attack detected on port 80. Target IP: 192.168.1.100. Victim IP: 192.168.1.101. Attacker IP: 192.168.1.102.	192.168.1.100	192.168.1.101	192.168.1.102	Pending
Medium Risk	2023-01-01 00:00:00 - 2023-01-01 23:59:59	Denial of Service	Denial of service attack detected on port 80. Target IP: 192.168.1.100. Victim IP: 192.168.1.101. Attacker IP: 192.168.1.102.	192.168.1.100	192.168.1.101	192.168.1.102	Pending
Medium Risk	2023-01-01 00:00:00 - 2023-01-01 23:59:59	Denial of Service	Denial of service attack detected on port 80. Target IP: 192.168.1.100. Victim IP: 192.168.1.101. Attacker IP: 192.168.1.102.	192.168.1.100	192.168.1.101	192.168.1.102	Pending
Medium Risk	2023-01-01 00:00:00 - 2023-01-01 23:59:59	Denial of Service	Denial of service attack detected on port 80. Target IP: 192.168.1.100. Victim IP: 192.168.1.101. Attacker IP: 192.168.1.102.	192.168.1.100	192.168.1.101	192.168.1.102	Pending

At the bottom of the table, there is a footer with the text 'Total 33291' and a page navigation bar with links 1, 2, 3, 4, 5, ..., 1696, 50 items/Page.



10.3. Monitoring Configuration

10.3.1. Rule Configuration

Displays system default rules.

- Rule Configuration List: Used to manage traffic detection rules. There are 14 system alert types in total.
 - Rule Fields include: Enable Status, Rule ID, Rule Name, Rule Level, Risk Level, Update Time.
 - Rule Levels include: Low, Medium, High, Strict.
 - Severity Levels include: Low Risk, Medium Risk, High Risk, Critical Risk.
- List Operations:
 - Enable/Disable rules; supports batch enabling and disabling of rules. Editing, creating new rules, or modifying existing ones is not allowed.
 - Filtering: Supports filtering by Enable Status, Rule ID, Rule Name, Rule Level, Risk Level.
 - Sorting: Supports sorting by Enable Status, Rule Level, Risk Level, Update Time. Default

order is by Rule Level sequence - then by Risk Level (descending).

- Synchronization: After modifying the rule enable/disable status, manually click the "Sync" button to sync the changes to the client.
 - Protection Level Settings: Located in the upper right corner of the page, allows setting a global protection level. After saving, rules with a Rule Level higher than the Protection Level cannot be enabled. Rules with a Rule Level lower than the Protection Level can be enabled or disabled.

10.3.2. Custom Rules

Stores user-configured custom rules. The alert type for these is "Custom Rules".

- Custom Rule List: Used to detect malicious network access or requests within containers.

Rules can be set for specific network request or response data content to monitor for behaviors with the same characteristics, enabling real-time detection of whether containers are suffering from corresponding attacks.

 - Rule Fields include: Enable Status, Rule ID, Rule Name, Risk Level, Application Scope, Update Time, and Operator.
 - List Operations:

- Supports rule enabling/disabling, creating new rules, editing, and deletion.
 - Filtering: Supports filtering by Enable Status, Rule ID, Rule Name, Risk Level, fields related to Application Scope, and Operator.
 - Sorting: Supports sorting by Update Time; default is Update Time (descending).
 - Synchronization: After creating, editing rules, or modifying the enable/disable status, manually click the "Synchronize" button to sync the changes to the client.
- New/Edit WAF Custom Rule: Allows setting/editing the rule's basic information, rule content, and application scope. The information set when a rule is triggered will be displayed in the alert list.
 - Basic Information includes: Status, Rule Name, Severity Level, Detection Description, Handling Suggestions. Among these, Rule Name and Detection Description are mandatory.
 - Rule Content: Request information and Response information can be configured. An alert is only triggered if all traffic information matches the set custom rule conditions.
 - Application Scope: Includes Container, Host with Container installed, Business Group, Cluster/Namespace, and Image.

The screenshot shows the Sentry CWPP interface for managing custom rules. The left sidebar has sections for Attack Alerts, Monitor Configuration (with 'Custom Rules' highlighted), Rule Configuration, Whitelist, and Blacklist. The main content area is titled 'Custom Rules' and contains a sub-header: 'Detect malicious network access or requests in containers. Define rules for specific requests or responses to monitor repeated patterns and detect attacks in real time.' Below this is a search bar and filter options. A table displays one rule entry:

Enable St...	Rule ID	Rule Name	Risk Level	Device Type A...	Update Time	Operator	Action
<input type="checkbox"/>	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	Edit Delete

At the bottom of the table, there is a page navigation bar showing '1 items' and '50 Item/Page'.

New WAF Custom Rule

Basic Info

Status:

*Rule Name: Enter Rule Name

Risk Level: Medium Risk

*Detection ... Enter Detection Note

Recommen... Enter Recommendation

Rule Content

Set custom rule conditions. Conditions are in 'AND' relation. Alert triggers only when all conditions match.

Condition	Match Type	Value	Reset
Select Condition	Select Match Type	Enter condition value	<input type="button" value="Delete"/>

+ Add Condition

Scope

Select Rule Scope

10.3.3. Whitelist

The whitelist page displays all created whitelists and supports creating and managing whitelists.

- Displayed fields include: Whitelist Conditions, Device Type | Application Scope, Affected Records, Remarks, Update Date, operator, etc.;
- List operations:
 - Filtering: supports filtering by whitelist conditions, device, update date, operator, and more;
 - Sorting: supports sorting by update date, with the default being descending order by update date;
 - Synchronization: after creating, editing, or deleting rules, you must manually click the "Sync" button to synchronize with the client.
 - Supports creating new rules, as well as single or batch deletion.

Web Application Firewall > Monitor Configuration > Whitelist

Whitelist

Whitelist rule creation, modification, and deletion are asynchronous operations. When the data volume is large, it may take some time. Please refresh the page manually after a while to get the latest data.

Whitelisting Cond...	Device Type Application Scope	Affected Reco...	Remark	Updated Date	Ope...	Actions
Container	Container 1	2	-	2023-09-04	Open	Edit Delete

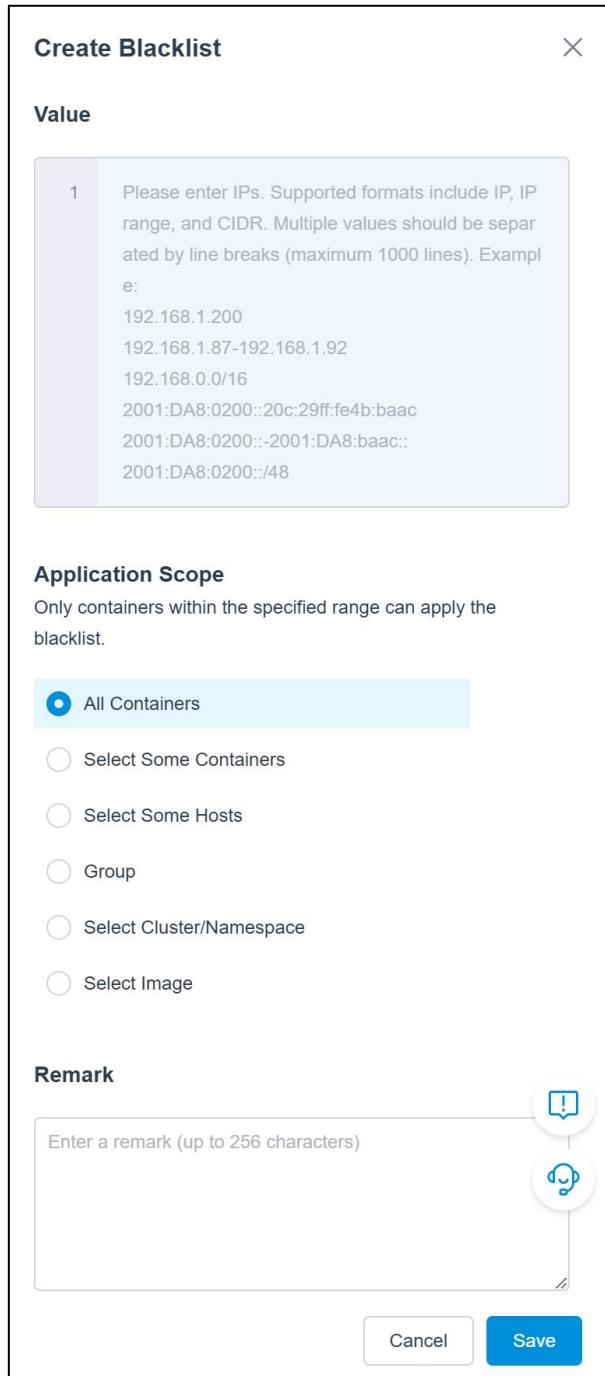
1 items

Please select filter content

[Delete](#) [Sync](#) [Create](#)

1 50 Item/Page [First](#) [Last](#)

- **Create/Edit Whitelist:** You can set or edit whitelist information, including whitelist conditions, application scope, affected alert range, and Remark;
 - **Application Scope:** Includes Container, Host with Container installed, Business Group, Cluster/Namespace, and Image.



- **Affected Records:** Displays alerts that meet the whitelist conditions. The details button can navigate to the alert details drawer.
 - **List display fields:** Risk Level, alert type, alert description, whitelisting time, actions
 - **Filter fields:** Risk level, alert type, alert description
 - **Sort fields:** Whitelisting time

10.3.4. Blacklist

The blacklist page displays all created whitelists and supports creating and managing whitelists.

- Displayed fields include: Blacklist IP, Device Type | Application Scope, Affected Records, Remarks, Update Date, operator, etc.;
- List operations:
 - Filtering: supports filtering by blacklist IP, device, update date, operator, and more;
 - Sorting: supports sorting by update date, with the default being descending order by update date;
 - Synchronization: after creating, editing, or deleting rules, you must manually click the "Sync" button to synchronize with the client.
 - Supports creating new rules, as well as single or batch deletion.

The screenshot shows the 'Blacklist' section of the Sentry CWPP interface. The left sidebar has a tree structure: 'Web Application Firewall' is expanded, showing 'Monitor Configuration' which is also expanded, revealing 'Blacklist'. A red box highlights the 'Blacklist' option. The main content area is titled 'Blacklist' and contains a note: 'The creation, modification, and deletion of blacklist rules are asynchronous operations. When handling large data volumes, the process may take a long time. Please manually refresh the page after some time to get the latest data.' Below this is a search bar with placeholder 'Please select filter content' and a magnifying glass icon. To the right are 'Delete', 'Sync', and 'Create' buttons. A table follows, showing one item: 'Container | 1'. The table columns include 'Blacklist IP', 'Device Type | Application Scope', 'Affected Reco...', 'Remark', 'Updated Date', 'Ope...', and 'Actions'. The 'Actions' column shows 'Edit' and 'Delete' links. At the bottom of the table is a pagination control with '1' and '50 Item/Page'.

- **Create/Edit Blacklist:** You can set or edit blacklist information, including value, application scope, affected alert range, and Remark;
 - **Application Scope:** Includes Container, Host with Container installed, Business Group, Cluster/Namespace, and Image.

The screenshot shows the 'Create Whitelist' dialog box. It starts with 'Set Whitelisting Conditions' where users can define conditions using a condition dropdown, match type, and value input field. There's a '+ Add Condition' button. Next is 'Application Scope', which allows selecting hosts within a range: 'All Containers' (selected), 'Select Some Containers', 'Select Some Hosts', 'Group', 'Select Cluster/Namespace', and 'Select Image'. Then comes 'Affected Alert Range', with options to 'Affect only current and future alerts' (selected) or 'Affect alerts from the past 30 days'. Finally, there's a 'Remark' section with a text input field and a 'Save' button at the bottom.

- **Affected Records:** Displays alerts that meet blacklist conditions. The details button can navigate to the alert details drawer. Similarly affected records that are on the whitelist.
 - **List display fields:** Risk Level, alert type, alert description, Blacklist time, actions

- Filter fields: Risk level, alert type, alert description
- Sort fields: Blacklist time

10.4. Alert Notification

For alert types related to the Web Application Firewall, both individual alert notifications and aggregated alert notifications are supported. Receipt methods include Website Message, Email, SMS Message, and Group Robot.

The screenshot shows the Sentry CWPP interface. On the left, there's a sidebar with 'Message Center' selected. The main area displays a list of message notifications. The 'Web Application Firewall' category is highlighted with a red border and has a count of 7 notifications. Other categories shown include All messages (127), Intrusion Not... (86), Security Control (1), Image Security (3), System Mon... (30), System Update ... (0), and Microsegmentat... (0).

This screenshot shows the configuration interface for alert notifications. On the left, there's a sidebar with 'Message Configuration' selected. The main area has two main sections: 'Intrusion Notification' and 'Web Application Firewall'. Each section has three buttons: 'Batch Set Receiving Method', 'Batch Set Receiver', and 'Batch Set Group Robot'. The 'Web Application Firewall' section also includes 'Aggregated Alert Notification' and 'Alert Notification' settings. The 'Receive Method' dropdown in the 'Web Application Firewall' section lists 'Website Message, Email, Group Robot'.

11. Probes Installation

11.1. Introduction to the Agent

Agents can be deployed in different forms in the environment and are key modules to implement security functions, which need to be installed on each protection node.

Linux, Windows, Docker, Kubernetes/OpenShift environments, servers, PCs, containers, and clusters are supported.

- Server Agent: Used in server security protection scenarios, it can flexibly adapt to various running forms according to the specific operating environment differences.
- PC Agent: Runs on the terminal host in the form of a process, focusing on terminal security protection. Real-time monitoring of endpoint risk issues and anomalous behaviors to effectively defend against threat events.
- Cluster Agent: A cluster component. It is deployed in the cluster in the form of a deployment, monitors and manages the security situation of the cluster, and works with the server agent to protect the security of the cluster.

11.1.1. Installation

11.1.1.1. Agent

11.1.1.1.1. Server Agent

Server Agent is used in server security protection scenarios and can flexibly adapt to a variety of running forms according to the specific operating environment differences.

11.1.1.1.1.1. Server Agent--Linux

Supporting Environment

- Supports all major Linux versions
 - China-specific operating systems: including BC-Linux, CTyunOS, OpenEuler, UOS, YHKylin, etc
 - Non-China-specific operating systems: including CentOS, Debian, Oracle, RHEL, SUSE, Ubuntu, etc. (the default curl versions of CentOS 5, Oracle 5, and RHEL 5 do not support command-line installation of agents, and can only be supported through **offline installation**).
- The system has the Curl program installed and the version is 7.19 or higher
- The system starts the Cron scheduled task service
- OpenSSL version 1.0.0 or later
- The firewall of the direct-connected host needs to ensure that it can communicate with the server
- The host to which the proxy is connected needs to be connected to the SOCK5 proxy service | of the management server [Installation method](#):

Installation Methods :

On the Agent Management -> Installation -> Agent page, select the Server Agent -> Linux tab, select Command Installation, and configure the parameters.

The installation parameters are described as follows:

- Service group: If you want to automatically assign hosts to a specified service group after the agent is installed, you can specify this in the installation parameters, and the hosts will be automatically assigned after the agent is installed. If you need to add a business group, you

can click the highlighted "Business Group Management" to jump to create a new business group.

- Connection method: Two modes, "Direct Connection" and "Proxy", are supported, and "Direct Connection" is selected by default. If "Proxy" is selected, you need to add new proxy information or select an existing proxy in the "Socks5 Proxy Server Information" section below. The proxy information includes: "Proxy Address" (format: domain:port or proxy-ip:port), and the corresponding "Username" and "Password".
- Connection address configuration: It is the address where the Agent connects to the server. By default, the "default connection address" configured by the system is selected. If you need to change it, click on the highlighted "Connection Address Configuration" to jump to the configuration page, where you can edit the existing configuration (After editing the connection address configuration that has already been used by the Agent. The "Configure Connection Address" task needs to be reissued to the Agent or the Agent needs to be restarted for it to take effect) . Alternatively, a new connection address can be created.
- Installation features:
 - When each agent is installed, you need to select the initial functions to be successfully installed (some functions will be checked by default), and the optional functions and available credits are derived from the tenant's authorization quota.
 - An agent can select multiple functions at the same time, and the selected functions will consume a license for each of them.
 - After the agent is installed, if you want to view the installed functions or modify them, go to the Agent Management - Running Monitor - License page. If you want to delicense and release the license, uninstall the agent.

- Advanced Configuration:
 - WanXiang System Synchronization Configuration: If a "WanXiang" Agent is already installed on the host, this system will automatically read the data from the "WanXiang" Agent configuration file and assign the same Agent ID to the ShenRui Agent. You need to fill in the path to the "WanXiang" Agent configuration file.
 - Installation configuration: You can customize the agent installation path and process name.
 - Running configuration:
 - You can set root permission to run and non-root permission to run. You can specify an account that is not running as root.
 - You can set resource limits and downgrade thresholds for agents
 - CDN configuration: When the number of agents is large but the bandwidth of the server is limited, CDN can be used to accelerate downloads, for example, the agent can download a file package from CDN to Upgrade or import rules.
 - - CDN nodes are added, including the node name and address (only the HTTPS protocol is supported), and can be Uninstalld.
 - This configuration is configured at the tenant level, and all accounts share the configured CDN node data.
 - Before installing the agent, ensure that the CDN nodes are connected.
 - When you install a new agent, you can specify whether to specify the CDN node to be bound each time you generate an installation command or installation package. If the agent is installed, bind the CDN

node or modify the CDN configuration, you can use the security tool.

- Installation Credential Management: This feature is used to limit the usage count and validity period of Agent installation credentials, including installation commands and activation codes.
 - Usage Count: The command usage count refers to the number of times a command is executed, regardless of success or failure, each execution counts. When enabled, you can configure the allowed number of uses. Once the count reaches the limit, the command or activation code will expire and cannot be used for further installations.
 - Validity Period: You can specify a specific expiration date and time. Upon reaching that time, the command or activation code will expire and cannot be used for further installations.

1. Command installation: Generate and copy the command, open the Linux terminal, right-click and paste the command in the root directory, press the enter key to execute, and the agent can be installed by itself.

2. Offline installation: Click to generate the installation package, follow the prompt steps to complete the installation. After successful installation, the Agent will automatically connect to the server. Administrators can view the successfully connected machines in the Agent list. **Note: After modifying the configuration, click Generate Installation Package again.**

3. Virtual machine template installation: Click to generate the installation package, follow the prompt steps to complete the installation. After successful installation, the Agent will automatically connect to the server. Administrators can view the successfully connected machines in the Agent list.

Note: After modifying the configuration, click Generate Installation Package again.

Note: If "Agent Self-Protection" or "Prevent closing the Agent process" is enabled in the Agent configuration, users will not be able to install or uninstall Agents in batches using third-party scripts.

Installation FAQs

Choose between three modes in which the agent is pulled up during installation

Add `svc_mode=notset|cron|systemd;` to the installed curl command; There is no `svc_mode` field in the default installation command, and the default mode is to pull up the agent through cron.

- The pull-up mode of the agent is not set: `svc_mode=notset`, the following is an example:

```
[root@localhost install_agent]# curl -s -L -k 'https://cloud.qingteng.cn:8443/client/com-qt-os-agent/service-agent2/agent/v1/host_agent/linux/install_script?agent_name=titanagent&arch=x86_64&conf_path=%2Fetc%2Ftitanagent&cpu_limit=0.50&cpu_max=1.50&guard_name=titan_guard&ins_path=%2Ftitan%2Fagent&log_path=%2Fvar%2Flog%2Ftitanagent&mem_limit=500&mem_max=500&monitor_name=titan_monitor&run_as=root&run_mode=host&tag_value_ids=12&tenant_id=34ff6ae955691600b6bd&token=e%3Ack1vgtv82o0qkd5ln5u0&user_add=true&svc_mode=notset'
```

- Pull up the agent via cron: `svc_mode=cron`; The following is an example:

```
[root@localhost install_agent]# curl -s -L -k 'https://cloud.qingteng.cn:8443/client/com-qt-os-agent/service-agent2/agent/v1/host_agent/linux/install_script?agent_name=titanagent&arch=x86_64&conf_path=%2Fetc%2Ftitanagent&cpu_limit=0.50&cpu_max=1.50&guard_name=titan_guard&ins_path=%2Ftitan%2Fagent&log_path=%2Fvar%2Flog%2Ftitanagent&mem_limit=500&mem_max=500&monitor_name=titan_monitor&run_as=root&run_mode=host&tag_value_ids=12&tenant_id=34ff6ae955691600b6bd&token=e%3Ack1vgtv82o0qkd5ln5u0&user_add=true&svc_mode=cron[1]
```

- Pull up the agent via systemd: `svc_mode=systemd`; Note: The default system of Amazon Linux

2023 no longer comes with crontab service. You need to add `svc_mode=systemd` in the

command for installing the Agent. The following is an example:

```
[root@localhost install_agent]# curl -s -L -k 'https://cloud.qingteng.cn:8443/client/com-qt-os-agent/service-agent2/agent/v1/host_agent/linux/install_script?agent_name=titanagent&arch=x86_64&conf_path=%2Fetc%2Ftitanagent&cpu_limit=0.50&cpu_max=1.50&guard_name=titan_guard&ins_path=%2Ftitan%2Fagent&log_path=%2Fvar%2Flog%2Ftitanagent&mem_limit=500&mem_max=500&monitor_name=titan_monitor&run_as=root&run_mode=host&tag_value_ids=12&tenant_id=34ff6ae955691600b6bd&token=e%3Ack1vgtv82o0qkd5ln5u0&user_add=true&svc_mode=systemd[1]
```

Upgrade

- Method 1: In Agent Management -> Running Monitor -> Agent, click the Agent tab, find the agent you want to Upgrade, select it, and click Upgrade in the More Operations column.
- Method 2: Click the Agent tab in Agent Management -> Running Monitor -> Agent, click Create Management Task, click Agent, select Upgrade as the task type, configure the corresponding parameters, and execute the command.
- Method 3: In Agent Management -> Running Monitor -> Agent, click the Agent tab, select

Details, and click Operation and Maintenance - Upgrade.

Uninstall

(1) Online uninstallation

- Method 1: Go to Agent Management -> Running Monitor -> Agent , click the Agent tab, find the agent you want to uninstall, select it, and click Uninstall in the More Operations column.
- Method 2: Click the Agent tab in Agent Management -> Running Monitor -> Agent Management, click Create Management Task, click Agent, select Uninstall as the task type, set the corresponding parameters, and execute the task.
- Method 3: In Agent Management -> Running Monitor -> Agent Management, click the Agent tab, select Details, and click Operation and Maintenance - Uninstall.

(2) Command line uninstallation

Log in to the machine on which the agent is installed and run the following command:

```
cd /titan/agent;
```

```
bash install_agent.sh disclean
```

If you have adjusted the installation directory and installation parameters, you need to run the following command to uninstall the installation directory:

```
cd Custom installation directory path
```

```
bash install_agent.sh disclean --conf-path configuration file directory path
```

Note: The agent can only be cleaned up on the client machine by deleting it from the command line, and the relevant data information of the agent still exists on the corresponding server. An Online uninstallation is required to achieve a complete uninstall of the agent.

11.1.1.1.2. Server Agent--Windows

Supporting Environment

- Supports all major versions of Windows

Windows version support checklist (64-bit):

System type	Version number
Server version	Windows Server 2008 R2 SP1
	Windows Server 2012
	Windows Server 2012 R2
	Windows Server 2016
	Windows Server 2019
Desktop version	Windows Vista
	Windows 7 SP1
	Windows 8
	Windows 8.1
	Windows 10
	Windows 11

- The firewall of the direct-connected host needs to ensure that it can communicate with the server

- The host to which the proxy is connected needs to be connected to the SOCK5 proxy service | of the management server [Installation method](#):

Installation:

On the Agent Management -> Installation -> Agent page, select Server Agent -> Windows tab, select Command Installation, or Installation Package Installation, and configure the parameters.

The parameter description is the same as that of Server Agent - Linux, and the Windows version does not involve root permissions.

1. Command installation: Select the generate CMD run command or Powershell command, open CMD or Powershell as an administrator, right-click and paste the command, press the enter key to execute, and the agent can be installed by itself.

2. Installation package installation: Click Generate Installation Package, double-click to install it after downloading, and the Agent will be automatically connected after successful installation. **Note: After modifying the configuration, click Generate Installation Package again.**

3. Virtual machine template installation: Click to generate the installation package, follow the prompt steps to complete the installation. After successful installation, the Agent will automatically connect to the server. Administrators can view the successfully connected machines in the Agent list.

Note: After modifying the configuration, click Generate Installation Package again.

Note: If "Agent Self-Protection" or "Prevent closing the Agent process" is enabled in the Agent configuration, users will not be able to install or uninstall Agents in batches using third-party scripts.

Upgrade

The upgrade method is the same as that of Server Agent - Linux.

Uninstall

(1) Online uninstallation

Same as "Server Agent - Linux".

(2) Command line uninstallation

Enter the windows machine where the agent is installed, enter the installation directory of the agent, the default directory: C:\Program Files\TitanAgent, and double-click to execute the following `uninst.exe` program.

Note: The agent can only be cleaned up on the client machine by deleting it from the command line, and the relevant data information of the agent still exists on the corresponding server. An Online uninstallation is required to achieve a complete uninstall of the agent.

11.1.1.1.3. Server Agent--Docker

With the help of the container engine, it runs on the node in the form of a container to protect the node security.

Supporting Environment

- Supports all major Linux versions
 - China-specific operating system: including BC-Linux, CTyunOS, OpenEuler, UOS, YHKylin, etc
 - Non-China-specific operating systems: including CentOS, Debian, Oracle, RHEL, SUSE, Ubuntu, etc. (Currently, the default curl version of CentOS 5, Oracle 5, and RHEL 5 does not support command-line installation of the agent, and can only be **supported through offline installation**)
- Mainstream container runtime versions are supported

The type of container runtime	Supported versions
Docker	1.10.0 and later

- The system has the Curl program installed and the version is 7.10 or higher
- OpenSSL version 1.0.0 or later
- Docker agent uses the host network, and you need to check the network connectivity between the host and the server before installation
 - The network between the host and port 8443 of the server is required.
 - If you use a domain name, the host needs to be able to resolve the IP address of the domain name.
- The host to which the proxy is connected needs to be connected to the SOCK5 proxy service | of the management server [Installation method](#):
 - It is necessary to have a smooth network between the host and the agent machine, and be able to access the port bound to the agent machine;
 - The agent machine can access port 8443 on the server side;
 - If a domain name is used, the proxy machine needs to be able to resolve the IP address of the domain name;
- Resource Needed (Recommended)

resource	size
CPU-limit	1C
memory-limit	1000M

Installation

Note: If "Agent Self-Protection" or "Prevent closing the Agent process" is enabled in the Agent configuration, users will not be able to install or uninstall Agents in batches using third-party scripts. On the Agent Management - > Installation - >Agent page, select Server Agent - >docker tab, select

Command Installation, and configure the parameters.

The parameter description is the same as that of Server Agent - Linux.

After the parameters are configured, the command is generated and executed with the root privilege on the terminal to complete the deployment.

Installation FAQs

Installation scenarios with a non-docker runtime:

For other runtime scenarios such as cri-o and containerd, the container agent installation mode is not supported, and the host agent or cluster agent needs to be installed to support it.

Upgrade

The Upgrade method is the same as that of Server Agent - Linux.

Uninstall

(1) Online uninstallation

Same as "Server Agent - Linux".

(2) Command line uninstallation

Log in to the machine on which the agent is installed and run the following command:

```
docker rm -f $(docker ps -a | grep "hiveagent" | awk '{print $1}')
```

Note: The agent can only be cleaned up on the client machine by deleting it from the command line, and the relevant data information of the agent still exists on the corresponding server.

An Online uninstallation is required to achieve a complete uninstall of the agent.

11.1.1.1.4. Server Agent—Kubernetes

With the help of Kubernetes, an orchestration tool, DaemonSet resources are used to run on nodes in the form of pods to protect node security. **We recommend that you install the Cluster Agent before**

installing the Kubernetes Agent.

Supporting Environment

- Supported Orchestration Tool Versions:

Cluster type	Supported versions
Kubernetes	1.9.6 and above

- Mainstream container runtime versions are supported

The type of container runtime	Supported versions
Docker	1.10.0 and later
Containerd	1.2.4 and later
CRI-O version	1.9 ~ 1.11、1.20

- Supports mainstream container cloud platforms
 - Alibaba Cloud, Tencent Cloud, Huawei Cloud, Rancher, and Miaoyun
- The Cluster Agent uses the host network, and you need to check the network connectivity between the host and the server before installation
- Resource Needed (Recommended)

resource	size
CPU-limit	1C
memory-limit	1000M
CPU-request	0.5C
memory-request	500M

Installation

On the Agent Management - > Installation - > Agent page, select Server Agent - > Kubernetes tab, select Command Installation, yaml File Installation, or Cluster API installation mode.

Parameter description:

- Node CPU architecture: Select x86 or ARM based on the CPU architecture of the pre-installed machine.
- Configure Image Repository: This parameter is used to use the image repository where the cluster agent exists. (If you have not obtained the cluster agent image, you can click Download Cluster Agent image on the page and push it to the image repository.))
- Image pull key: the key used to pull the agent image from the image repository
- YAML Template Policy: Used to select different YAML file templates
 - **Default Template:** The YAML template selected by default
 - **AppArmor High-Version Adaptation (Kubernetes Version ≥ 1.3):** When the Kubernetes version is ≥ 1.3 , select this YAML template if you need to configure AppArmor using the appArmorProfile field
- Advanced configuration
 - Resource Name: If the specified resource name is different from the agent installed in the cluster, it will not take effect
 - Privileged container: We recommend that you select the privileged container mode to run. The unprivileged container mode does not support ebpf event sources, driving capabilities, and network blocking capabilities on hosts, which may affect some agent self-protection, intrusion response, event collection, and peripheral management and control functions.

- Scheduling Range: To enhance the deployment capability of agents in a Kubernetes environment, you can add tolerance configurations to enable agents to tolerate taints on nodes, thereby meeting deployment requirements on special nodes.
- The other parameters are described in the same way as Server Agent - Linux.

1. Command installation: Generate and execute the command on the corresponding machine to download the relevant yaml file directly to the machine.
2. YAML file installation: Select the parameters, click to download the YAML file to the local computer, then upload the YAML file to the machine, and run the following command to declare the resource:

```
kubectl apply -f hiveagent_daemonset.yaml
```

3. Cluster API installation: **Make sure that the Cluster Agent in the environment has been successfully installed and is running normally.** Click Create Task to set the parameters related to the task. After a task is executed, you can view the task execution status in Task Management. If the installation is successful, you can see the details of the agent in the agent management, and its running mode will be displayed as pod.

Note: If "Agent Self-Protection" or "Prevent closing the Agent process" is enabled in the Agent configuration, users will not be able to install or uninstall Agents in batches using third-party scripts.

Upgrade

The upgrade method is the same as that of Server Agent - Linux.

Note:

- If the Cluster Agent is installed, the Cluster Agent will be sent an Upgrade task to modify the DaemonSet image of the Kubernetes Agent, and then restart the pod to complete the Upgrade
- If the Cluster Agent is not installed, the Kubernetes agent is sent an Upgrade task from inside

the pod, and the Kubernetes agent can perform the Upgrade task even if the Kubernetes agent is offline

Uninstall

(1) Online uninstallation

Same as "Server Agent - Linux".

(2) Command line uninstallation

- Log in to the master node of the cluster and query the Agent's Daemonset resource name:

```
kubectl get daemonset -n hivesec      # Replace 'hivesec' with the actual namespace where the Agent  
is located
```

- To uninstall the agent on the specified node, run the following command:

```
kubectl edit ds hiveagent -n hivesec  
  
# Replace 'hiveagent', 'hivesec' with the Agent's actual Daemonset resource name and the Agent's  
actual namespace
```

Add the hostname of the node that needs to uninstall Agent in node affinity:

```
affinity:  
    nodeAffinity:  
        requiredDuringSchedulingIgnoredDuringExecution:  
            - matchExpressions:  
                - key: kubernetes.io/hostname  
                  operator: NotIn  
                  values:  
                      - ""          # Add the hostname of the node that needs to uninstall Agent  
inside "", multiple values are separated by commas
```

- To uninstall the agent on all nodes, run the following command:

```
kubectl Uninstall daemonset hiveagent -n hivesec  
# Replace 'hiveagent', 'hivesec' with the Agent's actual Daemonset resource name and the Agent's  
actual namespace  
  
kubectl Uninstall configmap agent-config -n hivesec
```

Note: The agent can only be cleaned up on the client machine by deleting it from the command line, and the relevant data information of the agent still exists on the corresponding server. An Online uninstallation is required to achieve a complete uninstall of the agent.

11.1.1.1.5. Server Agent--Openshift

With the help of the orchestration tool Openshift, DaemonSet resources are used to run on nodes in the form of pods to protect node security. **We recommend that you install the Cluster Agent before installing the Openshift Agent.**

Supporting Environment

- Supported Orchestration Tool Versions:

Cluster type	Supported versions
Openshift	3.9 ~ 3.11、4.7

- The rest of the environment requires the same as "Server Agent - Kubernetes"

Installation:

On the Agent Management - > Installation - > Agent page, select Server Agent - > Kubernetes tab, select Command Installation, yaml File Installation, or Cluster API installation mode.

The parameter description is the same as that of Server Agent - Kubernetes.

1. The command installation steps are the same as those of "Server Agent - Kubernetes".
2. After uploading the file to the machine, run the following command to declare the resource:

```
oc apply -f hiveagent_daemonset.yaml
```

3. The installation steps of the cluster API are the same as those of Server Agent - Kubernetes.

Note: If "Agent Self-Protection" or "Prevent closing the Agent process" is enabled in the Agent configuration, users will not be able to install or uninstall Agents in batches using third-party scripts.

Upgrade

The Upgrade method is the same as that of Server Agent - Linux.

Note:

- If the Cluster Agent is installed, the Openshift Agent is sent an Upgrade task to the Cluster Agent, and the Cluster Agent modifies the DaemonSet image of the Openshift Agent, and then restarts the pod to complete the Upgrade.
- If the cluster agent is not installed, the system sends an Upgrade task to the Openshift agent, which performs a self-Upgrade from the pod.

Uninstall

(1) Online uninstallation

Same as "Server Agent - Linux".

(2) Command line uninstallation

- Log in to the master node of the cluster and query the Daemonset resource name of the Agent:

```
oc get daemonset -n hivesec #Replace 'hivesec' with the actual namespace where the Agent is located
```

- To uninstall the agent on the specified node, run the following command:

```
oc edit ds hiveagent -n hivesec
# Replace 'hiveagent', 'hivesec' with the Agent's actual Daemonset resource name and the Agent's
actual namespace
```

Add the hostname of the node that needs to uninstall Agent in node affinity:

```
affinity:
  nodeAffinity:
    requiredDuringSchedulingIgnoredDuringExecution:
      nodeSelectorTerms:
        - matchExpressions:
          - key: kubernetes.io/hostname
            operator: NotIn
            values:
              - "" # Add node hostname inside "", multiple values are
separated by commas.
```

- Uninstall the agent on all nodes: Run the following command:

```
oc delete daemonset hiveagent -n hivesec
# Replace 'hiveagent', 'hivesec' with the Agent's actual Daemonset resource name and the Agent's
actual namespace

oc delete configmap agent-config -n hivesec
```

Note: The agent can only be cleaned up on the client machine by deleting it from the command line, and the relevant data information of the agent still exists on the corresponding server. An Online uninstallation is required to achieve a complete uninstall of the agent.

11.1.1.1.6. Others

1. Help Center

The Help Center in the upper right corner of the main page of Agent Management -> Installation > Agent provides the installation steps for Server Agents in different environments.

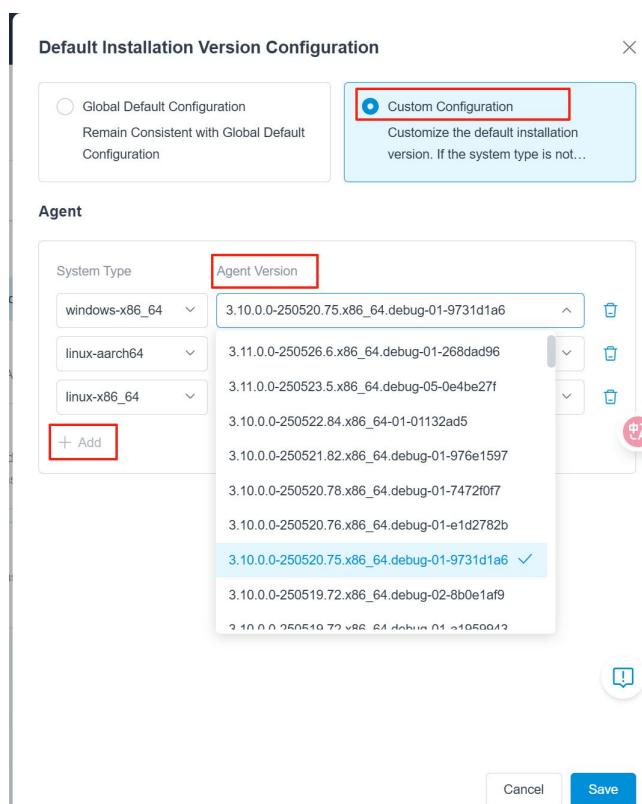
2. Installation records

In the upper right corner of the main page of Agent Management > Installation > Agent, you can view whether the agent was successfully installed, the installation time, and the basic information of the agent. Supports statistics on installations, including the total number of installs, the number of new additions added yesterday, and the number of decreases added yesterday.

3. Default version installation

In the upper right corner of the main page of Agent Management -> Installation -> Agent, you can configure the default installed probe version for agents of different system types.

- Global Default Configuration: This parameter is the same as the global default configuration and does not allow custom selection
- Custom configuration: The default installation version of the custom configuration is the same as the global default configuration for system types that are not customized
- Tenant administrators can upload different versions of probe installation packages and configure the global default probe installation version



11.1.1.1.7. Others

1. Help Center

The Help Center in the upper right corner of the main page of Agent Management -> Installation > Agent provides the installation steps for Server Agents in different environments.

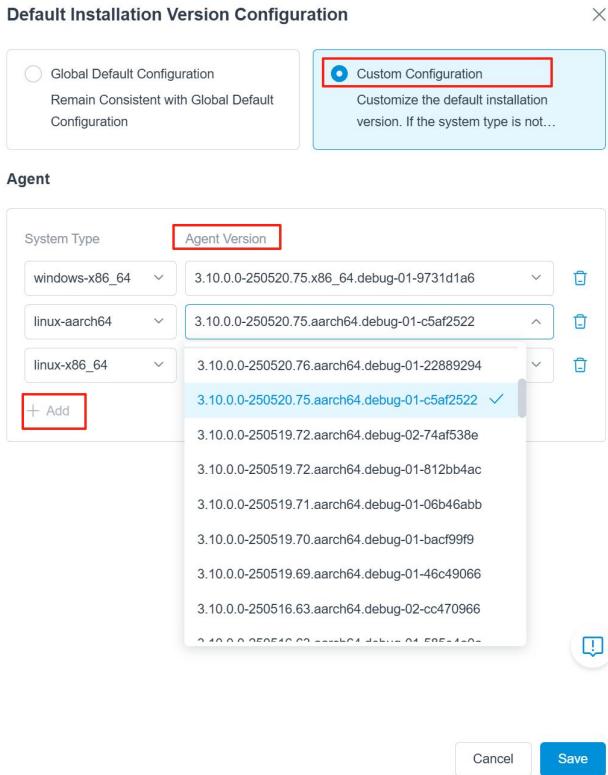
2. Installation Records

In the upper right corner of the main page of Agent Management > Installation > Agent, you can view whether the agent was successfully installed, the installation time, and the basic information of the agent. Supports statistics on installations, including the total number of installs, the number of new additions added yesterday, and the number of decreases added yesterday.

3. Default Installation Version Configuration

In the upper right corner of the main page of Agent Management -> Installation -> Agent, you can configure the default installed probe version for agents of different system types.

- Global Default Configuration: This parameter is the same as the global default configuration and does not allow custom selection
- Custom configuration: The default installation version of the custom configuration is the same as the global default configuration for system types that are not customized
- Tenant administrators can upload different versions of probe installation packages and configure the global default probe installation version



11.1.1.2. Cluster Agent

The Cluster Agent is deployed in the cluster in the form of Deployment to monitor and manage the security posture of the cluster and work with the Server Agent to protect the security of the cluster.

11.1.1.2.1. Cluster Agent--Kubernetes

Supporting Environment

- Mainstream orchestration tool versions are supported

Cluster type	Supported versions
Kubernetes	1.9 and above

- Mainstream container runtime versions are supported

The type of container runtime	Supported versions

Docker	1.10.0 and later
Containerd	1.2.4 and later

- Supports mainstream container cloud platforms
 - Alibaba Cloud, Tencent Cloud, Huawei Cloud, Rancher, and Miaoyun
- Resource Needed (Recommended)

resource	size
CPU	0.3C
memory	800MB

Installation:

On the Agent Management -> Installation -> Agent page, click the Cluster Agent -> Kubernetes tab, and select Command Installation or yaml File Installation to configure the parameters.

Parameter description:

- Cluster Name: Add a custom cluster name for the cluster agent to display. If not filled in, it defaults to default-ID.
- Node CPU architecture: Select x86 or ARM based on the CPU architecture of the pre-installed machine.
- Configure Image Repository: This parameter is used to use the image repository where the cluster agent exists. (If you have not obtained the cluster agent image, you can click Download Cluster Agent image on the page and push it to the image repository.)
- Image pull key: the key used to pull the agent image from the image repository
- Connection address configuration: It is the address where the Agent connects to the server. By default, the "default connection address" configured by the system is selected. If you need

to change it, click on the highlighted "Connection Address Configuration" to jump to the configuration page, where you can edit the existing configuration (After editing the connection address configuration that has already been used by the Agent. The "Configure Connection Address" task needs to be reissued to the Agent or the Agent needs to be restarted for it to take effect) . Alternatively, a new connection address can be created.

- Advanced configuration
 - Resource Name: If the specified resource name is different from the agent installed in the cluster, it will not take effect
 - Host mode: Select True for macvlan mode.
 - Scheduling scope: Node affinity and tolerations are used to limit the scheduling of [Cluster Agent] among fixed nodes, so as to reduce the number of nodes that need to enable network policies and reduce the attack surface.

1. Command installation

- On the Command Installation page, click Download Cluster Agent Image, select an appropriate architecture to download the image package (it is recommended to download the latest version of the image), upload the tar package to the server, and run the following command to push the image to the image repository:

```
docker load -i hiveagent-x86_64.tar
docker tag hiveagent-x86_64:version repo/cluster-link-x86_64:version
docker push repo/cluster-link-x86_64:version
```

- Click the "Generate Command" button and copy the command, then execute the command on the machine to download the relevant yaml file to the machine, and then perform the following steps.
- Kubernetes environment installation

(1) Create a namespace (if you have already created a namespace, you can skip this step); Run the command on the CLI terminal to create a namespace for deploying resources related to the cluster connection component, and the namespace name must be the same as that of the console, which is set to hivesec by default.

```
kubectl create namespace hivesec
```

(2) Create a secret of the image repository so that the image can be pulled from the remote image repository normally when starting the container (if the secret of the image repository has been created, you can skip this step): please replace the name and password with the correct username and password; The namespace name must be the same as in step (1), and docker-server must be replaced with the address of the repository where the related images are stored.

```
kubectl create secret docker-registry hivesec-secret --namespace=hivesec \
--docker-server=registry.test.cn/hive \
--docker-username='name' \
--docker-password='password'
```

Example:

```
kubectl create secret docker-registry hivesec-secret --namespace=hivesec \
--docker-server=registry.test.cn/hive \
--docker-username='admin' \
--docker-password='123456'
```

(3) Run the hivesec_rbac.yaml and cluster-link.yaml files in order to create RBAC authentication,

Deployment, Configmaps, and Service resources of the Cluster Agent

```
kubectl apply -f hivesec_rbac.yaml
kubectl apply -f cluster-link.yaml
```

After you perform the preceding operations, you can view the running status on the Agent

Management -> Running Monitor -> Agent ->Cluster Agent page.

2. Install the yaml file

The steps are the same as "Cluster Agent - Kubernetes Command Installation", note that after downloading the yaml file directly to the local computer, you need to upload the yaml file to the machine first, and then complete the installation of the Kubernetes environment.

Upgrade

- Method 1: In Agent Management -> Running Monitor -> Agent , click the Cluster Agent tab, find the Cluster Agent you want to upgrade, select it, and click Upgrade in the More Operations column.
- Method 2: In Agent Management -> Running Monitor -> Agent , click the Cluster Agent tab, click Create Management Task, click Cluster Agent, select Upgrade as the task type, configure the corresponding parameters, and execute the command.
- Method 3: In Agent Management -> Running Monitor -> Agent , click the Cluster Agent tab, select Cluster Details, and click Operation and Maintenance - Upgrade.

Note: You can only Upgrade the online Cluster Agent, and after submitting the Upgrade operation, you need to wait for a while to confirm whether the Upgrade operation is successful based on the version of the Cluster Agent in the foreground.

Uninstall

(1) Online uninstallation

- Method 1: Go to Agent Management -> Running Monitor -> Agent , click the Cluster Agent tab, find the Cluster Agent you want to Uninstall, select it, and click Uninstall in the More Operations column.
- Method 2: In Agent Management -> Running Monitor -> Agent , click the Cluster Agent tab, click Create Management Task, click Cluster Agent, select Uninstall as the task type, configure the corresponding parameters, and execute the task.

- Method 3: In Agent Management -> Running Monitor -> Agent , click the Cluster Agent tab, select Cluster Details, and click Operation and Maintenances - Uninstall.

Note: If you Uninstall the Cluster Agent online, the Cluster Agent will be uninstalled at the same time, and the service data will be cleaned up after the component is Uninstalld.

(2) Command line uninstallation

- Log in to the master node of the cluster and query the Deployment resource name of the cluster connection component:

```
kubectl get deployment -n hivesec # Replace 'hivesec' with the actual namespace where the Cluster Agent is located
```

- To Uninstall the resources related to the cluster connection component:

```
kubectl delete deployment cluster-link -n hivesec  
# Replace 'cluster-link', 'hivesec' with the Cluster Agent's actual Deployment resource name and the Cluster Agent's actual namespace
```

```
kubectl delete configmap cluster-link-config -n hivesec
```

```
kubectl delete secret cluster-link-userkey -n hivesec
```

11.1.1.2.2. Cluster Agent--Openshift

Supporting Environment

- Mainstream orchestration tool versions are supported

Cluster type	Supported versions
Openshift	3.9 ~ 3.11、4.7

- The rest of the environment requirements are the same as "Cluster Agent - Kubernetes".

Installation:

On the Agent Management -> Installation ->Agent page, click the Cluster Agent ->Openshift tab,

and select Command Installation or yaml File Installation to configure the parameters.

The parameter description is the same as that of Cluster Agent - Kubernetes.

1. Command installation

The rest of the steps are the same as "Cluster Agent - Kubernetes".

The steps to install the Openshift environment are as follows:

- Log in with the admin account

```
oc login -u system:admin
```

- Create a namespace (if you have already created a namespace, you can skip this step):

Run the command on the command line terminal to create a namespace for deploying resources related to the cluster connection component, and the namespace name must be the same as that of the console, which is Hivesec by default.

```
oc create namespace hivesec
```

- Create a secret of the image repository so that you can pull the image from the remote image repository normally when starting the container (if you have already created the secret of the image repository, you can skip this step):

Please replace name and password with the correct username and password; The namespace name is the same as in step (2), and docker-server is replaced by the repository where the related images are stored.

```
oc create secret docker-registry hivesec-secret --namespace=hivesec \
--docker-server=registry.test.cn/hive \
--docker-username='name' \
--docker-password='password'
```

Example:

```
oc create secret docker-registry hivesec-secret --namespace=hivesec \
--docker-server=registry.test.cn/hive \
--docker-username='admin' \
--docker-password='123456'
```

- Run the hivesec_rbac.yaml, hivesec_scc.yaml, and cluster-link.yaml files to create RBAC authentication, Deployment, Configmaps, and Service resources of the Cluster Agent.

```
oc apply -f hivesec_rbac.yaml
oc apply -f hivesec_scc.yaml
oc adm policy add-scc-to-user hivesec-scc system:serviceaccount:hivesec:hivesec-central-sa
oc adm policy add-scc-to-user hivesec-scc system:serviceaccount:hivesec:hivesec-agent-sa
#Replace 'hivesec' with the actual namespace where the Cluster Agent is located
oc apply -f cluster-link.yaml
```

After you perform the preceding operations, you can view the running status on the Agent

Management -> Running Monitor -> Agent ->Cluster Agent page.

2. Installation package installation

The steps are the same as "Cluster Agent - Openshift Command Installation", note that after downloading the yaml file directly to the local computer, you need to upload the yaml file to the machine first, and then run the Openshift environment installation.

Upgrade

Same as "Cluster Agent - Kubernetes".

Note: You can only Upgrade the online Cluster Agent, and after submitting the Upgrade operation, you need to wait for a while to confirm whether the Upgrade operation is successful based on the version of the Cluster Agent in the foreground.

Uninstall

(1) Online uninstallation

Same as "Cluster Agent - Kubernetes".

Note: If you Uninstall the Cluster Agent online, the Cluster Agent will be uninstalled at the same time,

and the service data will be cleaned up after the component is Uninstalld.

(2) Command line uninstallation

- Log in to the master node of the cluster and query the Deployment resource name of the cluster connection component:

```
oc get deployment -n hivesec # Replace 'hivesec' with the actual namespace where the Cluster Agent is located
```

- To Uninstall the resources of the cluster agent:

```
oc delete deployment cluster-link -n hivesec  
# Replace 'cluster-link', 'hivesec' with the Cluster Agent's actual Deployment resource name and the Cluster Agent's actual namespace  
  
oc delete configmap cluster-link-config -n hivesec  
  
oc delete secret cluster-link-userkey -n hivesec
```

11.1.1.2.3. Others

1. Help Center

The Help Center at the upper right corner of the main page of "Agent Management -> Installation -> Cluster Agent" provides:

- Steps to install the Cluster Agent for different environments
- Cluster audit log collection

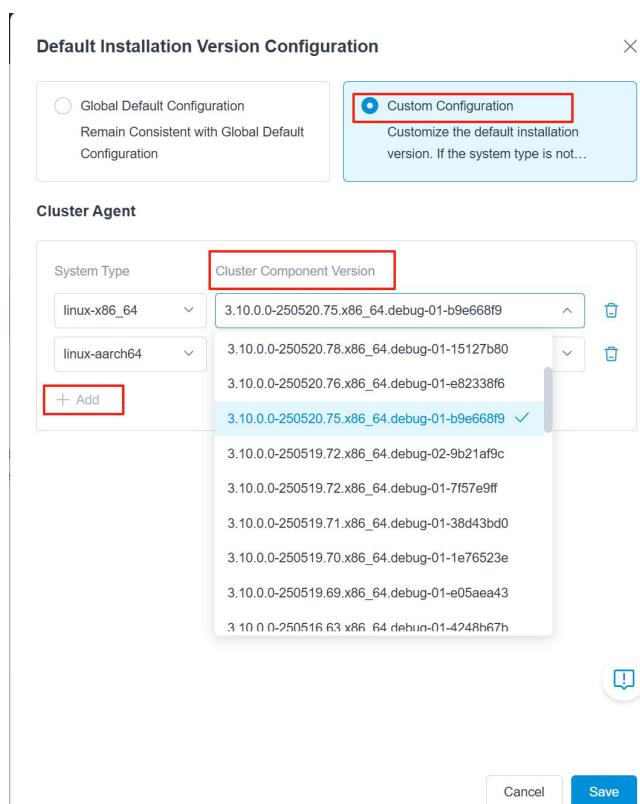
2. Installation records

In the upper right corner of the main page of Agent Management -> Installation -> Cluster Agent, you can view whether the Cluster Agent was successfully installed, the installation time, and the basic information of the Cluster Agent. Supports statistics on installations, including the total number of installs, the number of new additions added yesterday, and the number of decreases added yesterday.

3. Default installation version configuration

In the upper right corner of the main page of Agent Management -> Installation -> Cluster Agent, you can configure the default installed probe version for different system types of Cluster Agents.

- Global Default Configuration: This parameter is the same as the global default configuration and does not allow custom selection
- Custom configuration: The default installation version of the custom configuration is the same as the global default configuration for system types that are not customized
- Tenant administrators can upload different versions of probe installation packages and configure the global default probe installation version



11.1.1.3. Installation Credential Management

Manages the generated installation commands and activation codes, supporting the display of information such as whether they are valid, creation time, last used time, expiration time, remaining

days/total valid days, remaining uses/total usage count, etc.

- **Expiration Logic:** If the usage count is exhausted or the validity period expires, the credential is considered invalid and can no longer be used.
- **Configuration:** Supports clicking to configure and modify its usage count and validity period. If an existing configuration is cleared, it means the corresponding restriction is canceled.
- **Delete:** After deletion, the command will become invalid and cannot be restored.

Install Credential Management

<input type="checkbox"/> command	Is it effective	Command crea...	Command Last U...	Command expi...	Remaining days, eff...	Operation
<input type="checkbox"/>	Effective	2025-12-26 16:05:21	2025-12-26 16:06:05	-	-	Configuration Delete
<input type="checkbox"/>	Effective	2025-12-26 14:54:45	2025-12-26 14:55:39	-	-	Configuration Delete
<input type="checkbox"/>	Effective	2025-12-25 18:38:34	2025-12-25 19:06:46	-	-	Configuration Delete
<input type="checkbox"/>	Effective	2025-12-25 15:43:36	2025-12-25 15:44:12	-	-	Configuration Delete
<input type="checkbox"/>	Effective	2025-12-25 10:07:21	2025-12-25 10:08:11	-	-	Configuration Delete
<input type="checkbox"/>	Effective	2025-12-24 08:26:20	2025-12-24 08:32:15	-	-	Configuration Delete
<input type="checkbox"/>	Effective	2025-12-23 17:24:58	2025-12-23 17:25:53	-	-	Configuration Delete

11.1.1.4. Connection Address Configuration

The connection address is the network address where the Agent connects to the server. You can configure the connection address as needed to ensure normal communication between the Agent and the server.

11.1.1.4.1. List

The connection address configuration list displays the existing configurations, which can be edited or deleted. **Note:** After editing the connection address configuration that has already been used by the Agent, you need to reissue the "Configure Connection Address" task to the Agent or restart the Agent for it to take effect.

11.1.1.4.2. Create a new connection address

Parameter filling instructions:

- Basic information: Fill in the name and description of the new connection configuration.
- Connection method:
 - Communication protocols: Select based on the network protocol you are using.
- Connection address: The address for connecting to the server. Multiple addresses can be filled in. The newly installed Agent will randomly select an available address from the filling list to connect to the server.

The screenshot shows the 'Connection Configuration' section of the Agent management interface. On the left, there is a table listing two existing connection configurations: '12.16FC地址' and 'Default connection address'. The 'Default connection address' row shows 'Agent connection server default address' and 'IPv4'. On the right, there is a 'Basic Information' form with fields for 'Config...' (placeholder: 'Please enter config name') and 'Description' (placeholder: 'Please enter a description'). Below this is a 'Connection Method' section with radio buttons for 'IPv4' (selected) and 'IPv6'. At the bottom is a 'Connection address' section containing a table with columns 'Connect IP/Domain name' and 'Port'. A text input field for 'Please enter the connection IP address/Domain name' is followed by a placeholder 'Please enter the port'. There is also a '+ Add' button and a trash icon. At the very bottom are 'Cancel' and 'Save' buttons.

11.1.1.2. Security Integration

A capability module that can extend the basic capabilities of the agent and requires users to manage and control it separately is defined as "security integration".

1. System monitoring

Bash plugin: applies to Linux hosts and audits the security of commands executed in Bash programs by monitoring the command execution behavior in them.

DNS plugin: Applicable to Linux hosts, it audits DNS domain name resolution behavior by monitoring DNS domain name resolution in the system.

CMD plugin: This plugin is applicable to Windows hosts and audits the security of commands executed in CMD by monitoring the command execution behavior in CMD.

Powershell plugin: applies to Windows hosts and audits the security of commands executed in Powershell by monitoring the command execution behavior in Powershell.

Sysmon plugin: applicable to Windows host, is an event collection tool provided by Microsoft, process events, registry events, pipeline events and other types of events rely on the plugin for audit operations.

Driver switch: The system kernel dynamically loads the corresponding driver module to expand the agent's protection capabilities, including agent self-protection, malicious program blocking, and device control.

audit: an audit service on Linux that provides more fields and types of event sources.

eBPF: is an advanced event source that can be used in later kernel versions. This event source can accurately capture various events in multiple locations of the kernel with very low overhead without modifying the kernel code, and can efficiently transmit event information to user-space programs to support real-time monitoring and analysis.

Driver event source: It is an advanced event source that can obtain all event sources and have certain protection capabilities. Therefore, if you need protection capabilities such as anti-ransomware and automatic intrusion blocking, you can enable the driving event source. The driver event source will install drivers in the kernel and have certain requirements for the operating system version.

Network Concurrent Monitoring: When firewall rules are written to a Linux host, the connection tracking kernel module (conntrack module) is activated. If the number of concurrent connections is too high, network connections may be rejected. Therefore, it is necessary to monitor the counters of the connection tracking module. Once the limit may be reached, risks can be mitigated by

automatically adjusting the limit or generating alert information.

2. Safety components

Local anti-virus engine: This component integrates multiple virus detection engines to provide local file scanning and disk detection capabilities, and realizes real-time alarm and proactive blocking of host viruses and malicious programs.

3. Cloud native

Kubernetes: The Cluster Agent works with the Kubernetes Agent to collect cluster assets, manage node agents, and collect cluster audit logs by calling cluster APIs.

Openshift: The Cluster Agent works with the Kubernetes Agent to collect cluster assets, manage node agents, and collect cluster audit logs by calling cluster APIs.

Cluster audit logs: You can collect audit logs from clusters in the log backend and WebHook backend mode.

4. Network Connectivity

Dante Proxy: Provides secure and controllable SOCKS proxy services, supporting encrypted traffic forwarding, fine-grained access control, and network isolation penetration, thereby enhancing host communication security and flexibility.

CDN Acceleration: CDN (Content Delivery Network) is a technical service that distributes content from origin servers to global edge nodes, enabling users to access it from nearby locations. This enhances access speed and stability while saving bandwidth.

Note: When the above functions are needed, click the card to jump to the detail page for installation.

11.2. Integration Management

This feature provides a **dedicated management interface** for specific security integrations.

You can access it directly here, or navigate to it from:

- The **Security Integration page**, or
- The **Agent Details page > Security Integration section**.

11.2.1. Plugins

The page displays the current total number of hosts, statistics on installed and uninstalled plugins, as well as the plugin installation status of hosts within the system.

General Search: Enter the plugin details page and you can filter based on the conditions related to the host and the plugins.

List display: Show the system host information and the status of the plugin on the host, the version of the plugin, etc.

Plugins

5 items

Bash Plugin	Reported Events Description
Applicable Platforms: Host - Linux Agent	
Applicable OS: CentOS 5.3 and above, Ubuntu 12.04 and above (excluding 20.04)	
Function: The Bash plugin audits the security of commands executed within the Bash program by monitoring command execution behavior.	
Introduction:	
DNS Plugin	Reported Events Description
Applicable Platforms: Host - Linux Agent	
Applicable OS: CentOS 5.3 and above, Ubuntu 12.04 and above (excluding 20.04)	
Function: The DNS plugin audits DNS domain name resolution behavior by monitoring the system's DNS domain name resolution.	
Introduction:	
CMD Audit Plugin	Reported Events Description
Applicable Platforms: Host - Windows Agent	
Applicable OS: Windows 7 SP1 and above or Windows Server 2008 R2 and above	
Function: The CMD audit plugin monitors command execution behavior in the CMD and audits the security of the commands executed within it.	
Introduction:	
PowerShell Audit Plugin	Reported Events Description
Applicable Platforms: Host - Windows Agent	
Applicable OS: Windows 7 SP1 and above or Windows Server 2008 R2 and above(The kernel version must be greater than 6.0)	
Function: The PowerShell auditing plugin works by monitoring command execution behavior within PowerShell to audit the security of the commands executed.	
Introduction:	
Sysmon Plugin	Reported Events Description
Applicable Platforms: Host - Windows Agent	
Applicable OS: Windows 7 SP1 and above or Windows Server 2008 R2 and above(The kernel version must be greater than 6.0)	
Function: The Sysmon plugin is an event collection tool provided by Microsoft, which is used for auditing operations such as process events, registry events, and pipe events, among various other types of events.	
Introduction:	

11.2.1.1. List of plugins

Click the corresponding plugin to jump to the installation details page, which displays the applicable probes, application scope, latest version, total number of agents, number of uninstalled plugins, number of normal running devices, and number of abnormal running devices.

The list displays information such as the agent ID, host, plugin status, plugin version, and execution time.

Agent ID	Host	Plugin Status	Plugin Version	Last Execution Time	Last Execution Time	Installation Time	Operation
a1	Host - Linux ...	Not Installed	-	-	-	-	Install
●	Host - Linux ...	Not Installed	-	-	-	-	Install
●	Host - Linux ...	Not Installed	-	Uninstallation	2025-05-08 10:27:30	-	Install

11.2.1.2. Plugin Installation

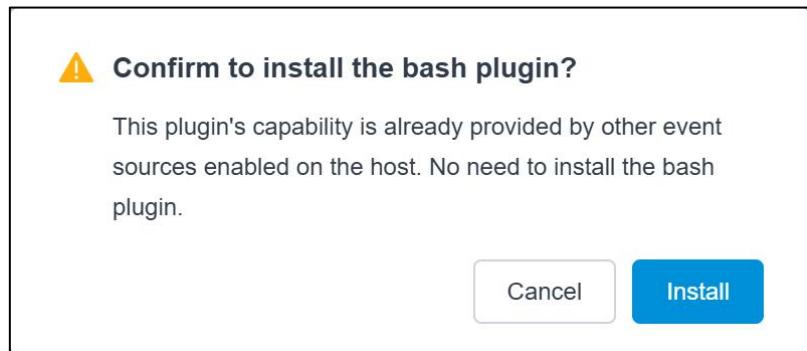
Method 1: Install it separately

Select a host and click Install in the operation bar to install the plugin on the current host agent.

Agent ID	Host	Plugin Stat...	Plugin ...	Operation
a1	Host - Linux ...	Not Installed	-	Install
●	Host - Linux ...	Not Installed	-	Install

Note: In Linux, plugins are used to provide certain special events, and subsequent ebpf and drivers also offer these events. Due to the high intrusiveness of plugins, when users have enabled the driver event source or ebpf event source and the information required for the current function can be met, a prompt indicating that **Bash plugins** and **DNS plugins** do not need to be installed will be given. **Users can choose to continue installing the plugin or use the provided event source by themselves.** In

addition, some system types do not support the installation of bash plugins and will also give prompts.



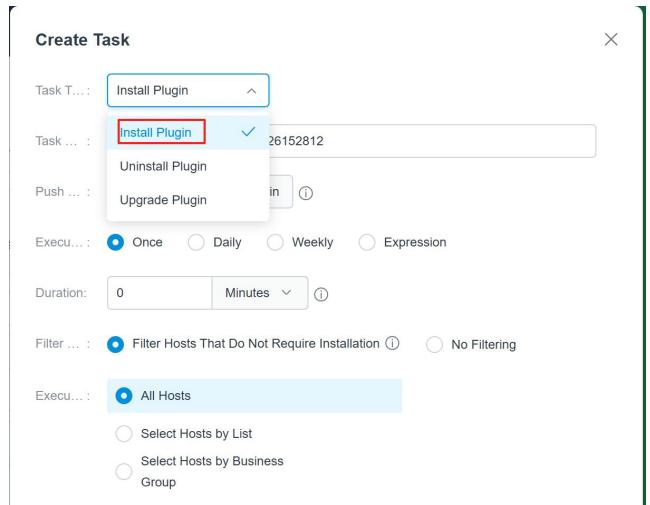
Method 2: Batch installation

Click the check box on the left side of the list to select one or more hosts, and click Install to install the plugin on the selected host agent.

Please Select Filtering Content		Uninstall		Upgrade		Install	
2/32 selected							
Agent ID	Host	Plugin Stat...	Plugin ...	Operation			
<input checked="" type="checkbox"/> 1	172.17.0.1	Not Installed	-	Install			
<input checked="" type="checkbox"/> 9	172.17.0.2	Not Installed	-	Install			
<input type="checkbox"/> 10	172.17.0.3	Not supported	-	Install			

Method 3: Create a task

Click **Create Task**, select Install Plugin, configure other parameters, and execute the task. You can go to Task Management to view the task execution results and execution records.



11.2.1.3. Plugin Upgrade

The steps are the same as "plugin installation".

11.2.1.4. Plugin uninstallation

The steps are the same as "plugin installation".

11.2.2. Event Sources

The correlation analysis of business data requires the collection support of various data sources, which can be divided into different event sources according to different detection mechanisms, and this function supports configuring the enablement/disabling of various event sources. All hosts enable the detection capability of basic event sources.

11.2.2.1. List of Event Sources

On the Integration Management - > Event Sources page, you can view the agent ID, event source type, and enabled event source information in the event source list. The system provides a search box for users to query the event source configuration information of a specified host.

Event Source Management

[Create Task](#)

Linux operating system environment supports four types of event sources: basic event source, ebpf event source, audit event source, and driver event source. Windows operating system environment supports two types of event sources: basic event source and driver event source; multiple event sources can be enabled simultaneously, and after enabling multiple event sources, the Agent will automatically select the appropriate event source based on the actual environment. [View more details](#)

Please Select Filtering Content								Batch Configuration
Agent ID	Host	Enable Event Sour...	Audit S...	Driver S...	eb	Operation		
● [REDACTED]	Microsoft Edge [REDACTED]	Bas... Total 2 items	Unsupported	Enabled		Details Configura		
● [REDACTED]	Apache [REDACTED]	Bas... Total 4 items	Prohibited ...	Disabled		Details Configura		
● [REDACTED]	Microsoft Edge [REDACTED]	Bas... Total 2 items	Unsupported	Enabled		Details Configura		
● [REDACTED]	Apache [REDACTED]	Bas... Total 4 items	-	Disabled		Details Configura		

Click Details under the Operation column of the event source list to view the event collection mechanism and collect events.

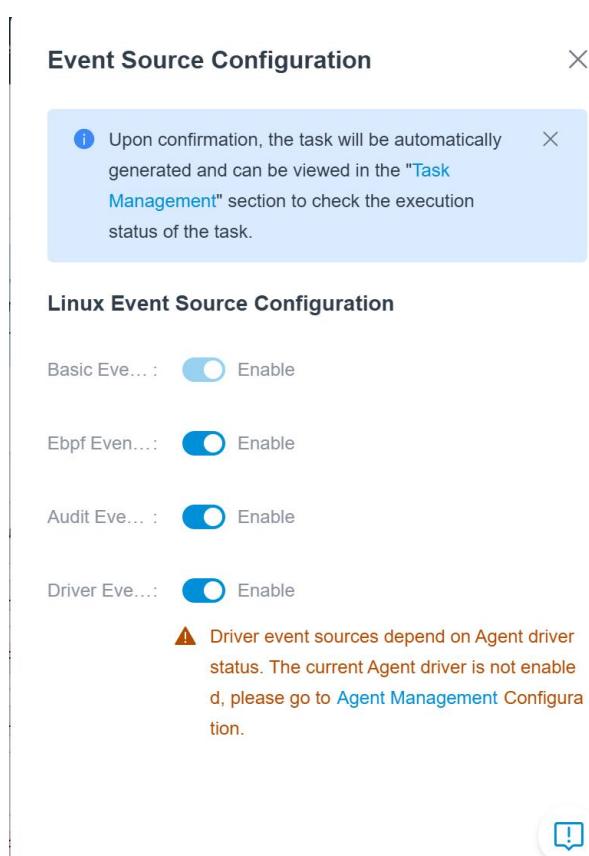
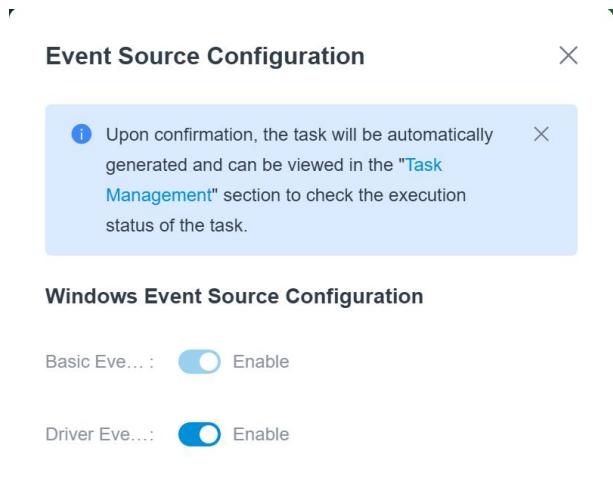
- The event collection mechanism refers to the collection method of events, including basic, ebpf, audit, and driver event collection in the Linux system. The Windows system includes basic and driver event collection.

11.2.2. Event Source Configuration

By default, the system enables basic event sources and cannot be disabled. If you need to enable other event sources due to other functions, you can change the default configuration or enable different event sources for a specified host.

Method 1: Configure the configuration separately

Select a host in the list and click Configure in the operation bar to edit the switches of various event sources for the host.



Method 2: Configure in batches

Click the checkbox on the left side of the event list to select one or more hosts, click Batch Configuration, and fill in the relevant parameters.

Please Select Filtering Content							Batch Configuration
2/42 selected							
Agent ID	Host	Enable Event Sour...	Audit S...	Driver S...	eb	Operation	
<input checked="" type="checkbox"/> S...	Windows Server 2012	Bas...	Total 2 items	Unsupported	Enabled	Details	Configura
<input checked="" type="checkbox"/> S...	Windows Server 2016	Bas...	Total 4 items	Prohibited ...	Disabled	Details	Configura
<input type="checkbox"/>	Windows Server 2008	Bas...	Total 2 items	Unsupported	Enabled	Details	Configura

11.2.2.3. Default Configuration

Click  on the Integration Management -> Event Sources page to modify the default event source configuration, which will be used by default for newly installed agents.

11.2.3. Anti-Virus Engines

The Anti-virus engine is a program provided by the system for local virus detection and removal services, which is used to detect local files and remove viruses. Users can install plugins and engines on the basis of the Agent to collect and audit the domain name resolution and command execution behaviors accessed by the host, promptly discover security issues, scan and remove viruses, and ensure the security of user information.

The page displays the current total number of hosts, statistics on installed and uninstalled antivirus engines, as well as the engine installation status of hosts within the system.

General Search: Enter the engine details page and you can filter based on the conditions related to the host and the engine.

List display: Display system host information, virus database version, virus database status and other information.

The screenshot shows the Sentry CWPP interface. At the top, there's a message: "To ensure the antivirus engine runs properly on Linux hosts, please upgrade the glibc version to 2.12 or higher." Below this are six status metrics: Total Hosts (42), Not Installed (34), Pending Upgrade (7), Latest Version (0), Installing (1), and Upgrading (0). A search bar and various navigation buttons are also present. The main area displays a table of 42 items, each row representing a host with columns for Run Mode, AgentID, Host, Operating System, Host Type, and Current Virus Database.

Run Mode	AgentID	Host	Operating System	Host Type	Current Virus Database
Host	Microsoft Windows 10 企业版 (build 19045)	PC	2025-05-21 08:18:44
Host	Microsoft Windows 8 专业版 (build 9200)	PC	2025-05-21 08:18:44
Host	Microsoft Windows 8.1 企业版 (build 9600)	PC	2025-05-14 07:46:40

11.2.3.1. Anti-Virus Engine Installation

Method 1: Install it separately

Select the host and click the "Install" button under the "Operation" column to complete the installation of the local Anti-Virus engine.

This screenshot shows a list of hosts with their operating systems, host types, and current virus database versions. The "Operation" column includes links for Install, Upgrade, and Uninstall. The "Install" link for the first host is highlighted with a red box.

Operating System	Host Type	Current Virus Database Versi...	Virus Definition ...	Operation
Microsoft Windows Server 2016 Datacenter (bu...)	PC	--	not installed	Install Upgrade Uninstall
Microsoft Windows 10 专业版 (build 18362)	PC	--	not installed	Install Upgrade Uninstall

Method 2: Batch installation

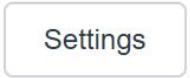
Select one or more hosts in the list and click Install under More Operations to complete the batch installation.

This screenshot shows a list of hosts with checkboxes in the "Run Mode" column. Three checkboxes are checked for the first three hosts. An "Install" button is highlighted with a red box above the host list. The "More" button is also highlighted with a red box.

Run Mode	AgentID	Host	Operating System	Host Type	Current Virus Database
<input checked="" type="checkbox"/>	Host	...	Microsoft Windows Server 2016 Datacenter (bu...)	PC	--
<input checked="" type="checkbox"/>	Host	...	Microsoft Windows 10 专业版 (build 18362)	PC	--
<input checked="" type="checkbox"/>	POD	...	CentOS Linux release 7.9.2009 (Core)	Server	--
<input type="checkbox"/>	Docker	...	Alpine Linux v3.13	Server	--

Note: The "Upgrade, Uninstall" and "Install" steps for the Anti-Virus engine are the same.

11.2.3.2. Anti-Virus Engine Settings

 Settings

You can enable "automatic installation" and "automatic Upgrade" in , and when the host goes online, the system will automatically install the local Anti-Virus engine and automatically Upgrade.

11.2.4. Network Concurrent Monitoring

Network Concurrent Monitoring is a security monitoring function for the connection tracking kernel module (conntrack module) in the Linux environment. Its core purpose is to mitigate the risk of network connection rejection caused by excessive concurrent connections. Users can obtain concurrent volume evaluation results to assist in security operation decisions, set the module's maximum value (with the system calculating risk thresholds accordingly), view periodic status data displayed on the page, receive threshold-exceeding alarms, and configure whether to automatically adjust the module's maximum value via a switch.

- The page displays statistical data of risk-free/risky hosts and monitored/unmonitored hosts.
- **Risky Hosts:** The number of hosts whose current concurrent volume exceeds the risk threshold.

General Search: Upon entering the Network Concurrent Monitoring page, users can filter hosts based on host-related criteria and Network Concurrent Monitoring-related criteria.

List Display: The list shows the monitoring status of Linux hosts, concurrent connection details (current count, historical maximum count, upper limit, risk threshold), and module status.

The screenshot shows the 'Network Concurrent Monitoring' section of the Sentry CWPP interface. At the top, there are four status boxes: 'No-Risk Hosts' (71), 'Risky Hosts' (0), 'Monitored Hosts' (49), and 'Unmonitored Hosts' (22). Below this is a search bar and a 'Batch Configuration' button. The main area displays a table with 71 items, each row representing a host configuration. The columns include: Monitoring Status, Agent ID, Host, Business Group, Connection Concurrency, Peak Time, Module, and Operation. Each row also contains a small thumbnail image of the host's network interface. The table includes sorting and filtering options at the top.

11.2.4.1. Connection Tracking Protection Configuration

After writing rules such as intrusion blocking and micro-segmentation blocking in the firewall, to prevent connection tracking counts from exceeding the upper limit, preset configurations will be applied first, followed by monitoring and automatic adjustment of the upper limit.

Method 1: Individual Configuration

Select a host, click the "Connection Tracking Protection Configuration" button in the "Operations" column to view the "Connection Tracking Upper Limit" and "Historical Maximum Count". Configure parameters such as "Monitoring Switch", "Preset Upper Limit Configuration", and "Auto-adjust Upper Limit", then click "Save".

Description of Connection Tracking Parameters:

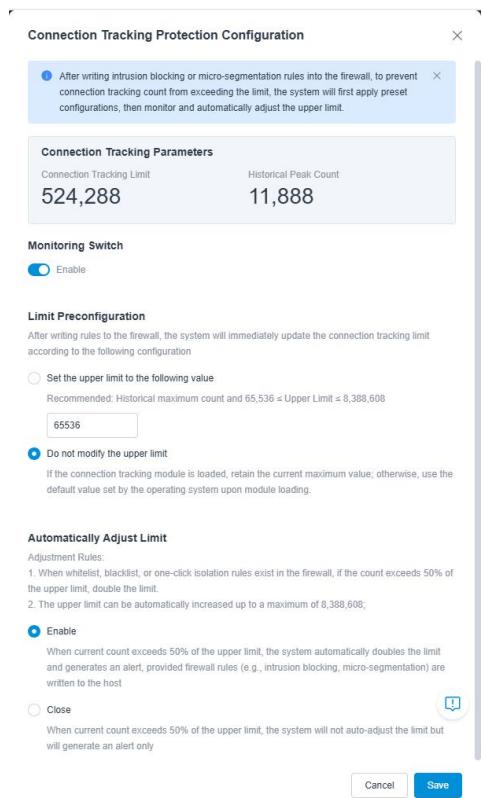
- Connection Tracking Upper Limit:** Displays the current upper limit of connection tracking. If the connection tracking module is not loaded, the current upper limit cannot be obtained. The value shown is from the last time the module was loaded and can be used as a reference for the preset upper limit.

- Historical Maximum Count**

Configuration Instructions:

- **Monitoring Switch:** Enabled by default. Only when enabled will the connection tracking module be monitored, and support for preset upper limit configuration and auto-adjust upper limit configuration be activated.
- **Preset Upper Limit Configuration:**
 - - If preset upper limit is supported: After writing rules (e.g., intrusion blocking, micro-segmentation blocking) to the firewall, the system will immediately modify the connection tracking upper limit according to the configuration. Recommended range for upper limit: Historical Maximum Count and $65,536 \leq \text{Upper Limit} \leq 8,388,608$.
 - If upper limit is not modified: If the connection tracking module is loaded, the current upper limit will be retained; if the module is not loaded, the default value specified by the operating system after module loading will be used.
- **Auto-adjust Upper Limit Configuration:**
 - - Enabled by default.
 - Adjustment rules: When the firewall contains whitelist, blacklist, or one-click isolation rules, if the count exceeds 50% of the upper limit, the upper limit will be doubled; the maximum auto-expanded upper limit is 8,388,608.
 - If enabled: When the current count exceeds 50% of the upper limit, the system will automatically adjust the upper limit (double it) and generate an alarm, provided that firewall rules (e.g., intrusion blocking, micro-segmentation blocking) have been written to the host.
 - If disabled: When the current count exceeds 50% of the upper limit, the system will not

automatically adjust the upper limit and will only generate an alarm.



Method 2: Batch Configuration

Select one or more hosts in the list, click the "Batch Configuration" button on the page, configure parameters such as "Monitoring Switch" and "Setting Selection", then click "Save".

Method 3: Create Task

Click the "Create Task" button on the page, configure parameters such as "Task Name", "Monitoring Switch", and "Setting Selection", then click "Save".

11.2.4.2. Network Concurrent Monitoring Message Notifications

Each time a host performs a concurrent connection count check, if the current count of the host's concurrent connections exceeds the risk threshold, an alarm will be triggered.

Supported notification methods include in-site messages, emails, robots, and SMS.

11.2.5. Dante Proxy Management

11.2.5.1. Dante Proxy Management List

Dante Proxy can provide secure and controllable SOCKS proxy services, supporting encrypted traffic forwarding, fine-grained access control, and network isolation penetration, thereby enhancing host communication security and flexibility.

Dante Proxy Management offers automated and visual proxy operation and maintenance capabilities through the Agent, along with continuous monitoring of service health, ensuring the continuity and stability of proxy services. Note: The proxy service must be manually assigned to specific nodes, and corresponding nodes must have the Agent installed to be incorporated into this system for management.

- **Feature Access:** Jump to this feature by clicking the "Dante Proxy" card on the "Security Integration" page; or navigate via the "Integration Management - Dante Proxy Management" menu.
- **Install Proxy:** Click "Install Proxy" in the upper-right corner of the interface, fill in the corresponding parameters to deploy Dante on a single node with one click. High availability deployment currently does not support one-click installation via the interface; it requires following the instructions in the help center documentation for operation.
- **Configure Proxy Service:** This section manages the proxy addresses reported by the Agent's actual connections, representing the proxy data that is actually configured and in use.
 - Click the "**Configure**" button for the selected proxy data, and configure basic proxy information and designate the node where the proxy service resides based on the actual situation.
 - **Single Node Deployment:** Select the node where the Dante service is located.

- **High Availability Deployment:** Select the node(s) where Keepalived, HAProxy, and the Dante daemon process reside; you can choose one or multiple machines.
- Only after the proxy service nodes are designated can the monitoring switch be turned on, after which proxy details and the process status of various components can be viewed. Simultaneously, CPU, memory, and other status monitoring data for the proxy service can be viewed in the system monitoring information.
- **General Search:** On the Dante Proxy Management page, you can filter based on conditions related to Dante proxies.
- **List Display:** This table displays the monitoring status, deployment mode, proxy name, proxy service node(s), proxy address, proxy service status, current connection count, number of associated Agents, number of associated Cluster Agents, etc., for Dante proxies.
 - **Proxy Service Status:**
 - **Single Node Deployment**
 - **Normal:** Process is in Running state.
 - **Abnormal:** Process is in Stopped state.
 - **Unknown:** Process does not exist or the Agent has not reported the process status.
 - **High Availability Deployment**
 - **Normal:** The process status for all three types of components is Running.
 - **Abnormal:** Any one of the three component types has a process status of Stopped.

- **Unknown:** Any one of the three component types has an unknown process status.
- **Number of Associated Agents:** This statistic represents the number of Agents configured with this proxy that are online / total number.
- **Number of Associated Cluster Agents:** This statistic represents the number of Agents configured with this proxy that are online / total number.
- **View Details:** After monitoring is enabled, you can click the "View Details" button to check the status monitoring of the overall proxy service and its various components.
- **Log Download:** When the Agent on the host of the component node is online, downloading logs for each component is supported.
- **Enable/Disable Monitoring:** Supports batch operations to enable or disable monitoring. Corresponding operations can be viewed for task details and execution records in the "Task Management" module.
- **Edit:** When monitoring is disabled, editing the configured proxy service information is supported.

Dante Proxy Management

This feature delivers automated, visual proxy operations and continuous health monitoring via Agent—ensuring proxy service continuity and stability. Supports one-click Dante deployment. Click [View Supported Systems](#)
Note: The proxy service must be manually assigned to a node, and the corresponding node must have the Agent installed to be managed by this system. Click [Install Now](#)

Please select filter content									<input type="checkbox"/> Select All	Enable Monitoring	Disable Monitoring
Proxy Name	Proxy Service Node	Proxy Addr...	Proxy Servic...	Current Co...	Associate...	Operation					
single_ins...	246代理-new	⚠️ [REDACTED]	unknown	3	0/2	View Details Configuration					
-	210集群	⚠️ Not Configured	unknown	0	0/4	View Details Configuration					
-	zili.chen-new	⚠️ Not Configured	unknown	0	0/0	View Details Configuration					

3 items

< 1 > 50 Item/Page

11.2.5.2. Install Proxy This description applies to the Dante single-node deployment method.

11.2.5.2.1. Supported Operating Systems

Operating System	Operating System Version	Kernel Version	System Architecture
CentOS	8.5.2111/9	4.18.0-348.7.1.el8_5.x86_64	x86/arm64
CTyunOS	2.24.07	4.19.90-2102.2.0.0076.ctl2.x86_64	x86/arm64
openEuler	22.03	5.10.0-216.0.0.115.oe2203sp4.x86_64	x86/arm64
Rocky	8/9.1 (Blue Onyx)	5.14.0-162.6.1.el9_1.x86_64	x86/arm64
SUSE	12-SP5 12.5	4.12.14-122.183-default	x86/arm64
Ubuntu	22.04	5.15.0-25-generic	x86/arm64
UOS	V20	4.19.0-server-amd64/4.19.90-2106.3.0.0095.up2.uel20.aarch64	x86/arm64
kylin	kylin v10	4.19.90-24.4.v2101.ky10.x86_64	x86/arm64

11.2.5.2.2. Resource Configuration Requirements

In a production environment, the corresponding requirements between Dante server configuration and the number of supported Agents are as follows:

Number of Agents	Server Configuration	Average Network Bandwidth	Peak Network Bandwidth
6000	8 cores, 16 GB RAM	1.2 Mbps	4.8 Mbps
3000	4 cores, 8 GB RAM	600 Kbps	1.2 Mbps
1000	4 cores, 8 GB RAM	200 Kbps	800 Kbps

11.2.5.2.3. Deployment Method

On the "Agent Management -> Integration Management -> Dante Proxy Management" page, click the "Install Proxy" button to jump to the "Install Proxy" page for parameter configuration.

The installation parameter descriptions are as follows:

Network Interface

- **Internal Listen Address:** Required. Specifies the internal network address the server listens on. Only IPv4 protocol is supported.
- **Internal Listen Port:** Required. Sets the port on which the server listens for connections on the internal network.

Authentication Method

- **SOCKS Client Authentication:** Single choice. Controls the authentication method for clients connecting to the SOCKS server. Options are **PAM Authentication** (based on system user authentication) and **No Authentication** (not recommended, lower security). When PAM Authentication is selected, the corresponding username and password must be configured.
- **Username:** When PAM Authentication is selected, set the account name used for client authentication. Clients must provide this username for identity verification when connecting.
- **Password:** When PAM Authentication is selected, set the password used for client

authentication. Clients must enter the correct password to pass authentication.

Access Control

- **Allowed Connection Ranges:** Required. Specifies the IP addresses or network segments allowed to access this proxy service. Only IPv4 protocol is supported. Please use CIDR notation, and separate multiple values with line breaks. By default, all connections are denied; only IPs or network segments configured within this range can successfully connect to the proxy service.

After configuring the parameters, click the "**Generate Installation Command**" button. Open a Linux terminal, right-click in the root directory to paste the generated command, press Enter to execute it. Dante will then install automatically. The appearance of the message "**Danted installation and configuration completed successfully!**" indicates a successful installation.

The screenshot shows the 'Install Proxy' configuration interface. It includes fields for 'Internal Listening ...' (IP address), 'Authentication Method' (selected PAM Authentication), and an 'Access Control' section. The 'Access Control' section contains a 'Allowed Connect...' field with an example of CIDR notation (192.168.1.0/24) and a 'Generate Installation Command' button.

11.2.6. CDN Management

11.2.6.1. CDN Management List

CDN (Content Delivery Network) is a technical service that distributes content from origin servers to global edge nodes, enabling users to access it from nearby locations. This enhances access speed and stability while saving bandwidth.

CDN Management provides automated and visual CDN management capabilities through the Agent, along with continuous monitoring of service health, ensuring the continuity and stability of CDN services. Note: The CDN service must be manually assigned to specific nodes, and corresponding nodes must have the Agent installed to be incorporated into this system for management.

- **Feature Access:** Jump to this feature by clicking the "CDN Acceleration" card on the "Security Integration" page; or navigate via the "Integration Management - CDN Management" menu.
- **Deploy CDN:** Click "Deploy CDN" in the upper-right corner of the interface, fill in the corresponding parameters to deploy with one click.
- **Configure CDN Service:**
 - Select CDN data and click the "Configure" button to configure basic CDN information and designate the node where the CDN service resides based on the actual situation.
 - Only after the CDN service nodes are designated can the monitoring switch be turned on.
- **General Search:** On the CDN Management page, you can filter based on conditions related to CDN.
- **List Display:** This table displays the monitoring status, access address, node location, process status, associated Agent(s), etc., for the CDN service.
 - **CDN Process Status:**
 - **Normal:** Process is in Running state.
 - **Abnormal:** Process is in Stopped state.
 - **Unknown:** Process does not exist or the Agent has not reported the process status.
 - **Number of Associated Agents:** This statistic represents the number of Agents

configured with this CDN access address that are online / total number.

- **Log Download:** When the Agent on the host of the CDN service node is online, downloading logs is supported.
- **Enable/Disable Monitoring:** Supports batch operations to enable or disable monitoring. Corresponding operations can be viewed for task details and execution records in the "Task Management" module.
- **Edit:** When monitoring is disabled, editing the configured CDN service information is supported.

CDN Management

This screenshot shows the CDN Management interface. At the top, there's a note about automated management via Agent and continuous monitoring for service health. Below is a search bar and filter options. The main area displays a table with two items. The columns are: Monitoring Status (with a switch icon), Node Name, CDN Access URL, CDN Service Node (with a progress bar and value 172), CDN Process Status (with a warning icon and text 'Not Configured'), Associated Agents (with a value of 0/2), and Operation (with a 'Download logs' link and 'Edit' button). The table has a header row with sorting icons. At the bottom right, there are navigation arrows and a '50 Item/Page' dropdown.

Monitoring Status	Node Name	CDN Access URL	CDN Service Node	CDN Process Status	Associated Agents	Operation
<input checked="" type="checkbox"/>	246节点-new	https://172...	172	unknown	1/4	Download logs Edit
<input checked="" type="checkbox"/>	cdn-https://172...	https://172...	Not Configured	unknown	0/2	Download logs Edit

11.2.6.2. Deploy CDN

11.2.6.2.1. Supported Operating Systems

Operating System	Operating System Version	Kernel Version	System Architecture
CentOS	8.5.2111	4.18.0-348.7.1.el8_5.x86_64	x86/arm64
Ubuntu	22.04	5.15.0-25-generic	x86/arm64
SUSE	12-SP5 12.5	4.12.14-122.183-default	x86/arm64
Kylin	kylin v10	4.19.90-24.4.v2101.ky10.x86_64	x86/arm64

UOS	V20	4.19.0-server-amd64	x86
UOS	V20	4.19.90-2106.3.0.0095.up2.uel20.aarch64 arm64	
openEuler	22.03	5.10.0-216.0.0.115.oe2203sp4.x86_64	x86/arm64
Rocky	9.1 (Blue Onyx)	5.14.0-162.6.1.el9_1.x86_64	x86/arm64
CTyunOS	2 24.07	4.19.90-2102.2.0.0076.ctl2.x86_64	x86_64

11.2.6.2.2. Hardware Requirements

Please mount the data disk to the /data directory.

Hardware Type	Hardware Requirements
cpu	4C
Memory	8G
Disk	100GB

11.2.6.2.3. Network Policy

All firewall policies for connecting to the service end must be met.

Port	Description
8443	Service communication port, default is 8443; if modified, please open accordingly based on actual settings.

11.2.6.2.4. Deployment Method

Click the "**Deploy CDN**" button on the page to jump to the "**Deploy CDN**" page. You can refer to the help documentation in the "**Help Center**" to fill in the required parameters (CDN Domain/IP, CDN Port, Server IP, Server Port) and optionally upload a certificate. Then, click the "**Generate Installation Command**" button and execute it locally to complete the CDN deployment.

- **CDN Domain/IP:** Required. Used to specify the network identifier for the CDN service. You can fill in a domain name or IP address to provide the location basis for accessing the CDN service.
- **CDN Port:** Required. The network port used by the CDN service to establish network connections.
- **Server IP:** Required. The network IP address of the Qingteng Shenrui 5.0 system server. Separate multiple values with English commas.
- **Server Port:** Required. The network port of the Qingteng Shenrui 5.0 system server.
- **Certificate:** Optional. A digital certificate used to secure communication between the CDN service and the server. Uploading it is recommended. The format should be a .tar.gz compressed package containing only the certificate and private key files.

After configuring the parameters, click the "**Generate Installation Command**" button. Open a Linux terminal, right-click in the root directory to paste the generated command, and press Enter to execute it. The CDN will then deploy automatically. The appearance of the message "**Nginx installation and configuration completed successfully!**" indicates a successful deployment.

Deploy CDN

* CDN Domain/IP: https:// is included by default; enter only the domain/IP

* CDN Port:

* Server IP:

* Server Port:

Certificate: Please upload a .tar.gz package containing only certificate and private key files.

11.3. Local Client

11.3.1. Product Installation

You can contact the administrator to install the product either via the command - line method or by downloading the installation package. After the installation is complete, you need to configure it through administrator review or password input to use it normally. This is to prevent the installation package from being leaked and avoid unauthorized installations that waste licenses.

11.3.1.1. Administrator Review Method

After the installation is finished, start the application. A pop - up window will appear for you to fill in the review information.



After filling in the information, click "Apply to Join" and wait for the administrator's approval.



11.3.1.2. Password Verification Method

After the installation is complete, start the application. A pop - up window will prompt you to enter the password.



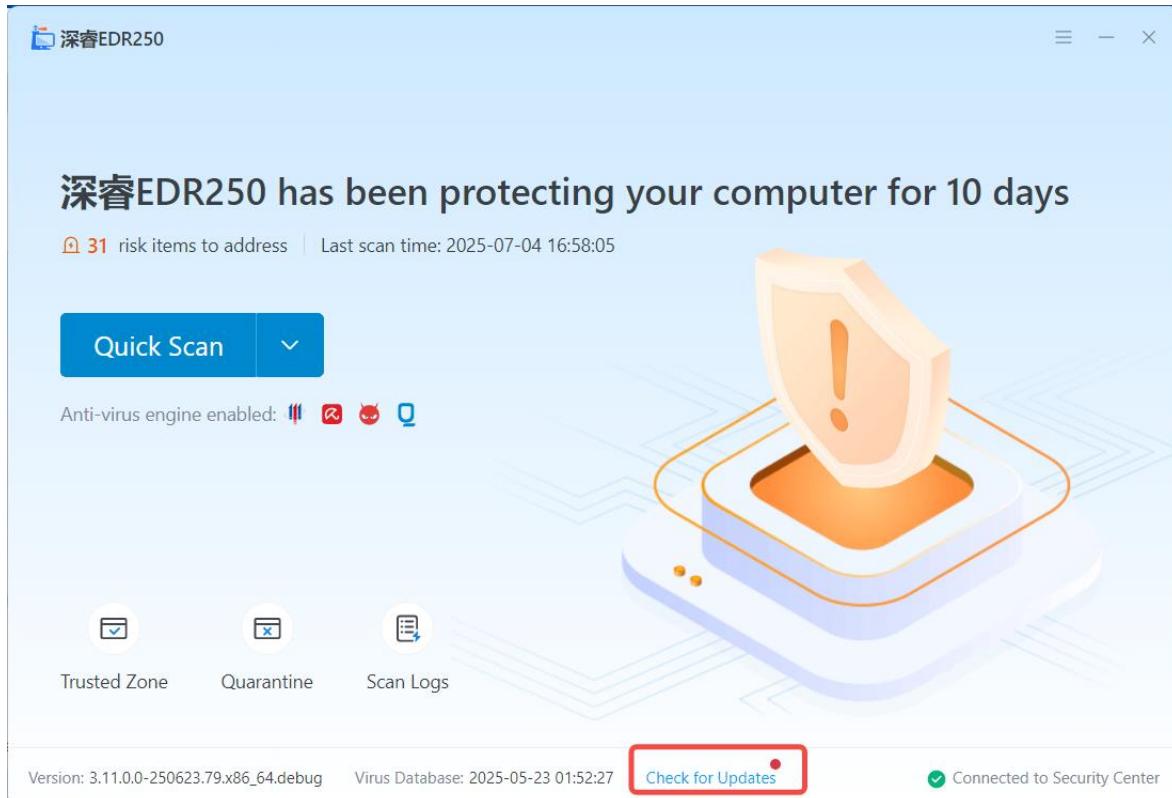
11.3.2. Exit and Uninstallation

If the administrator has enabled anti - uninstallation in the background, clicking the uninstall program will pop up a window prompting you to enter the password.



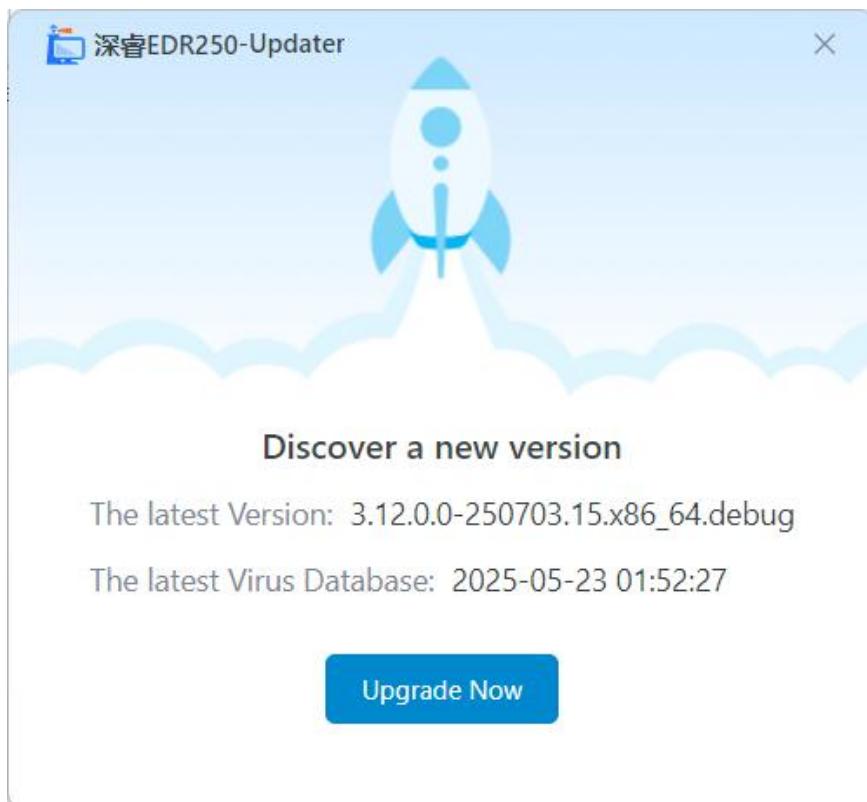
11.3.3. Update and Upgrade

You can click the "Check for Updates" button on the home page.



If the system detects a version update or a virus database update, a pop - up window will appear.

You can click "Upgrade Now".



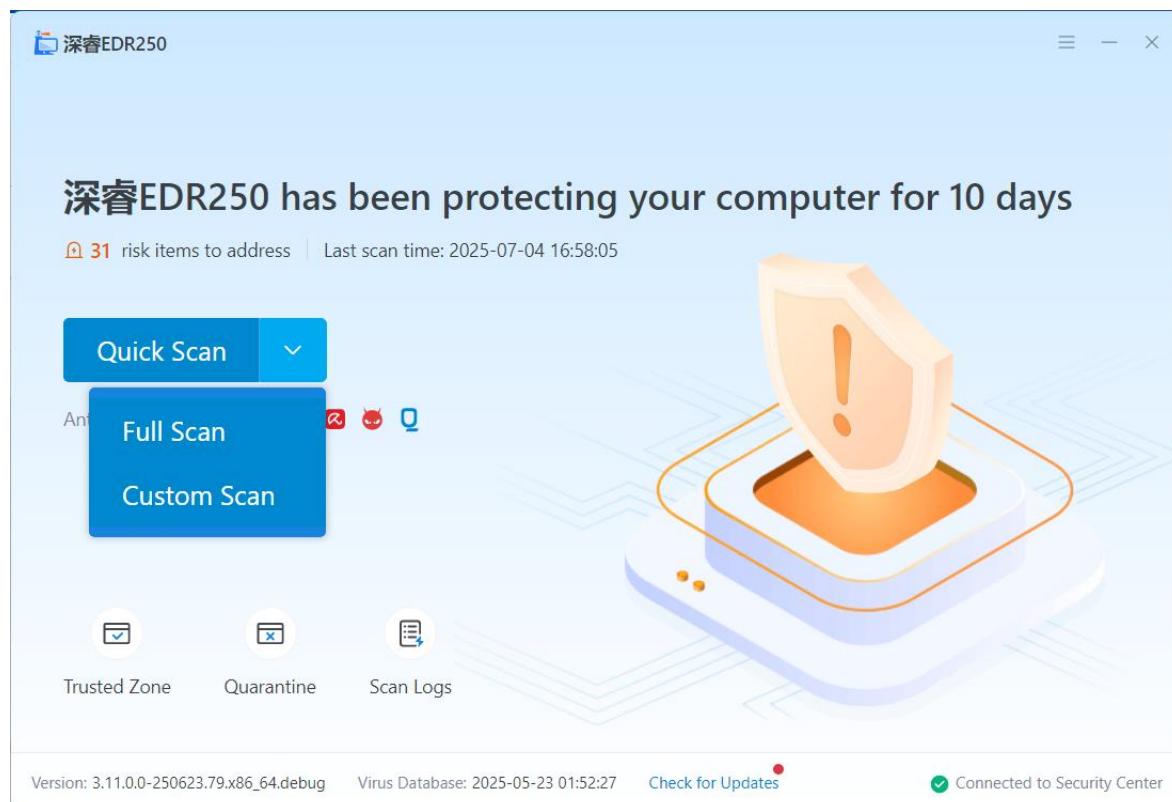
11.3.4. Scanning Task

The scanning task can be executed either by the client user or the administrator.

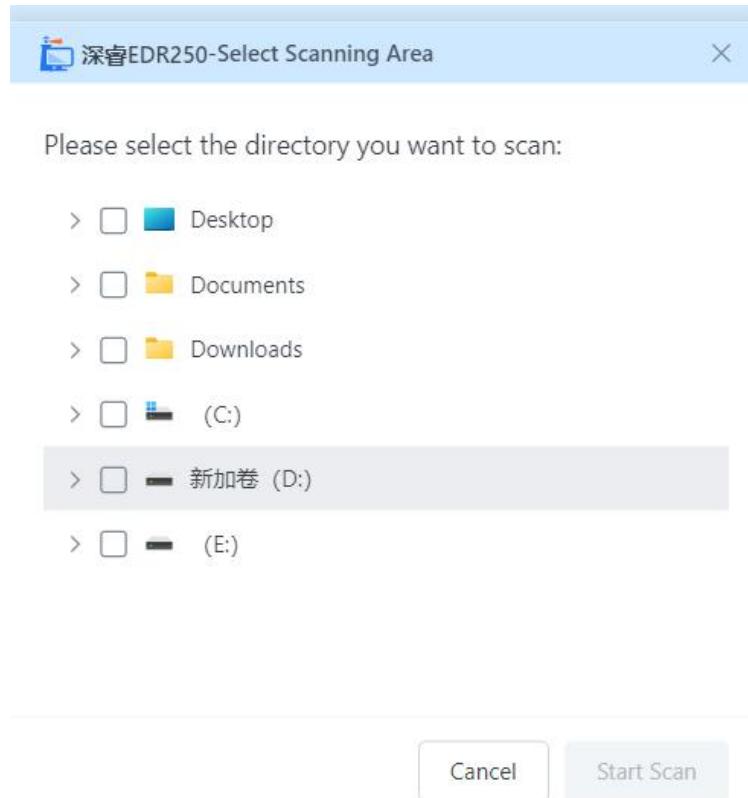
(1) Execution by Client User

- You can perform a security scan on the relevant directories of the host to detect and report risk items. The scanning tasks are divided into quick scan, full - disk scan, and custom scan.

The quick scan will scan the key directories, and the full - disk scan will scan all directories.



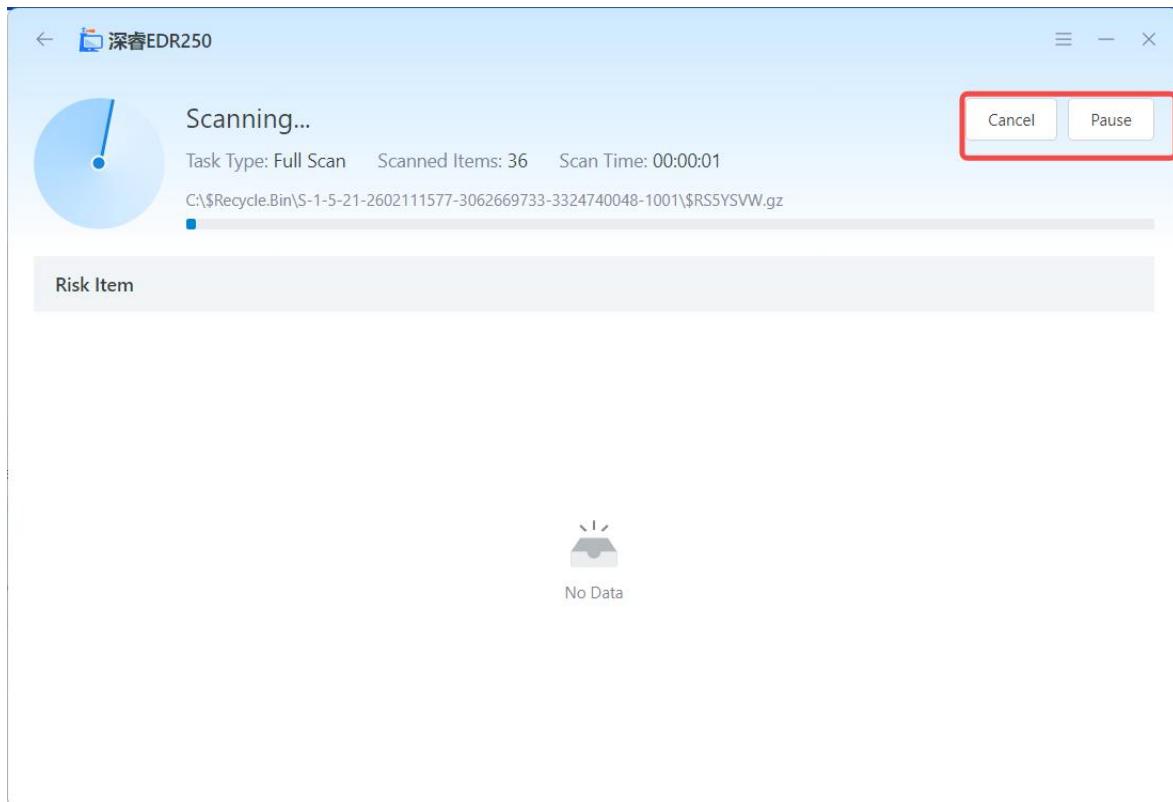
- If you choose the custom scan, you can manually select the directories to be scanned for security.



- You can select a file/directory or multiple files/directories to right-click and click to use Qingteng Cloud Security to kill viruses and enter the scan page.

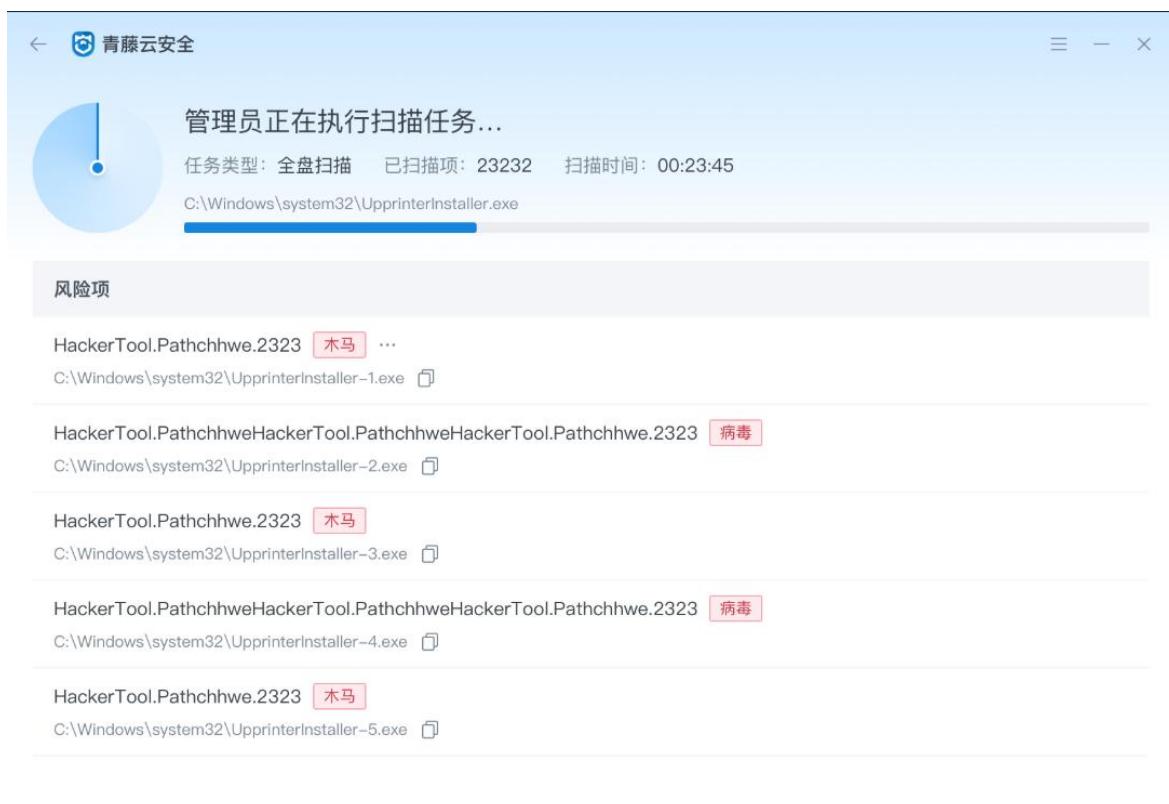


- If you need to interrupt the scanning task due to special reasons, you can cancel or pause it.



(2) Execution by Administrator

The system will automatically execute the scanning tasks issued by the administrator.



11.3.5. Risk Handling

If risks are detected during the scan, you can choose to handle them immediately or temporarily ignore them. For each risk item, you can view the details, add it to the trust zone, or quarantine it.

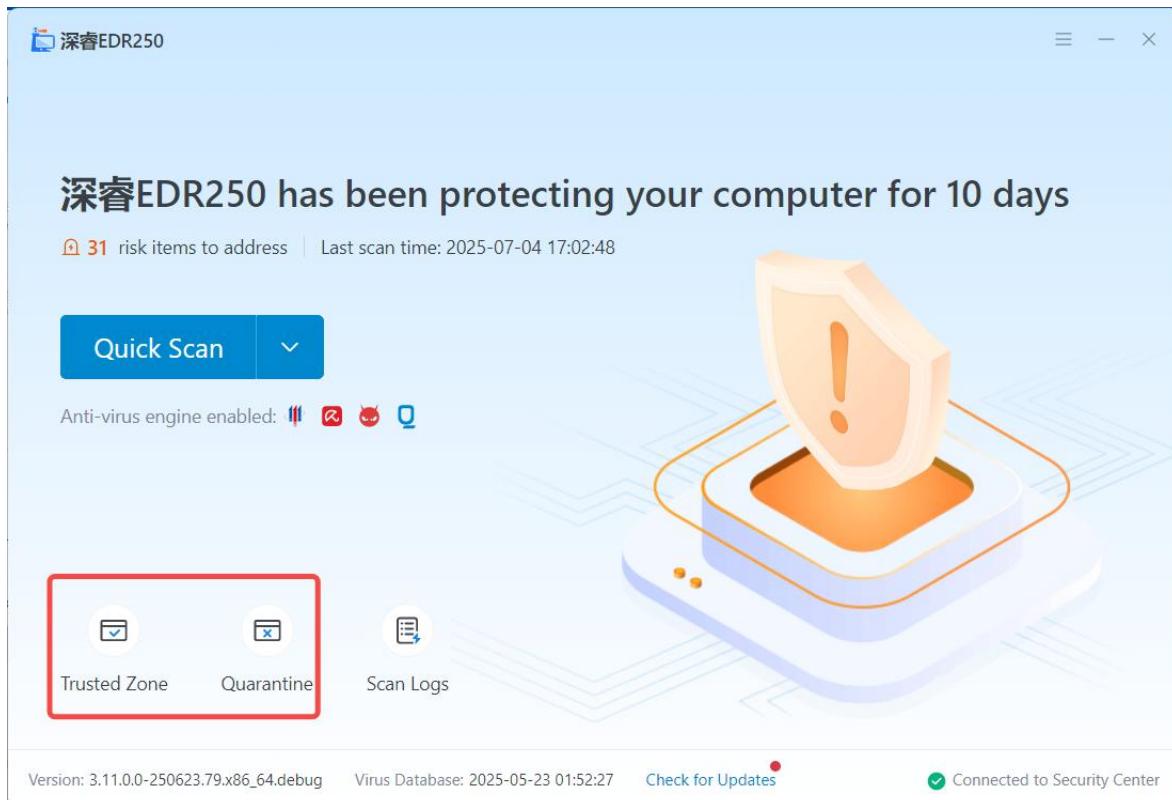
If you choose to add it to the trust zone, the system will no longer detect it.

If you choose to add it to the quarantine zone, the system will quarantine the file.

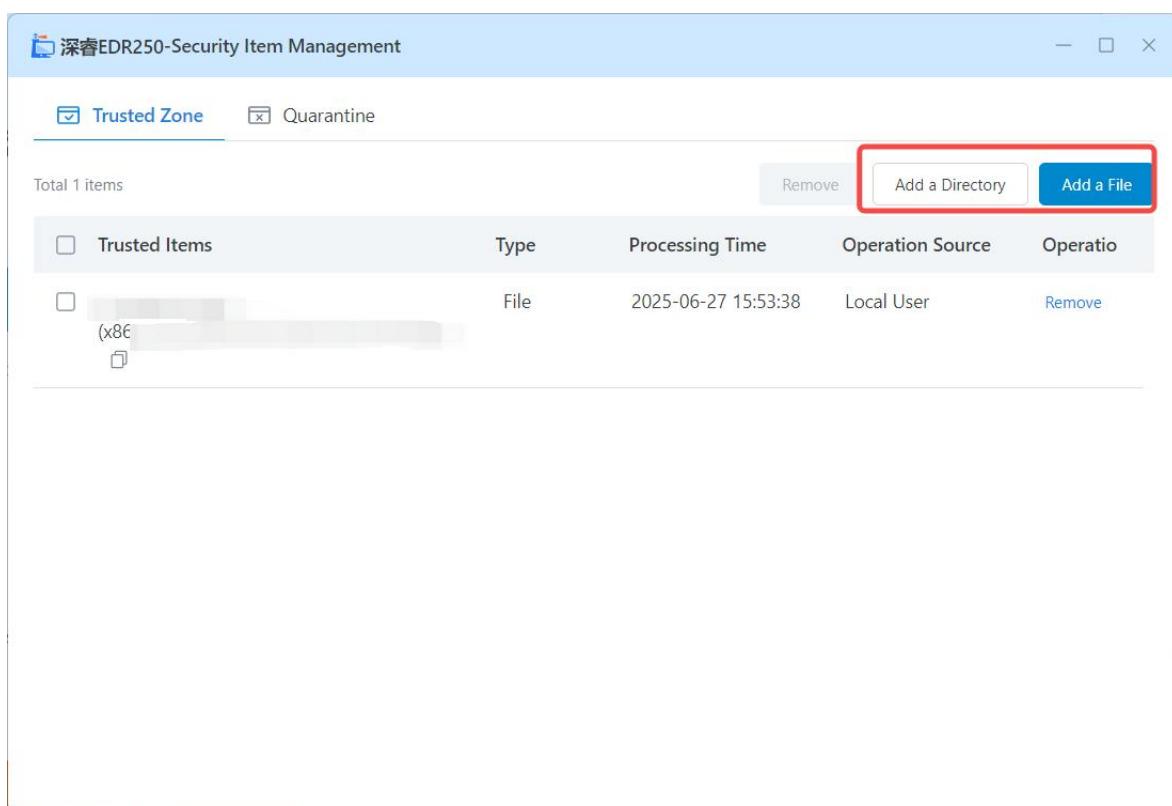
The screenshot shows a software interface titled "深睿EDR250". A message at the top states "Scan canceled, 2 risk items need to be handled". Below this, task details are shown: "Task Type: Full Scan", "Scanned Items: 15863", and "Scan Time: 00:05:20". A progress bar indicates the scan was canceled. The main area displays two risk items under the heading "Risk Item". Each item has a checkbox, a name ("Trojan.PE.A!"), a path ("C:\Program Files\WindowsApps\AppUp.IntelArcSoftware_25.22.1502.0_x64_8j3eq9eme6ctt\VFS\ProgramFilesX64\Intel\Intel Graphics Software\IntelGraphicsSoftware.Service.dll"), and three operation buttons: "Details", "Trust", and "Quarantine".

11.3.6. Security Item Management

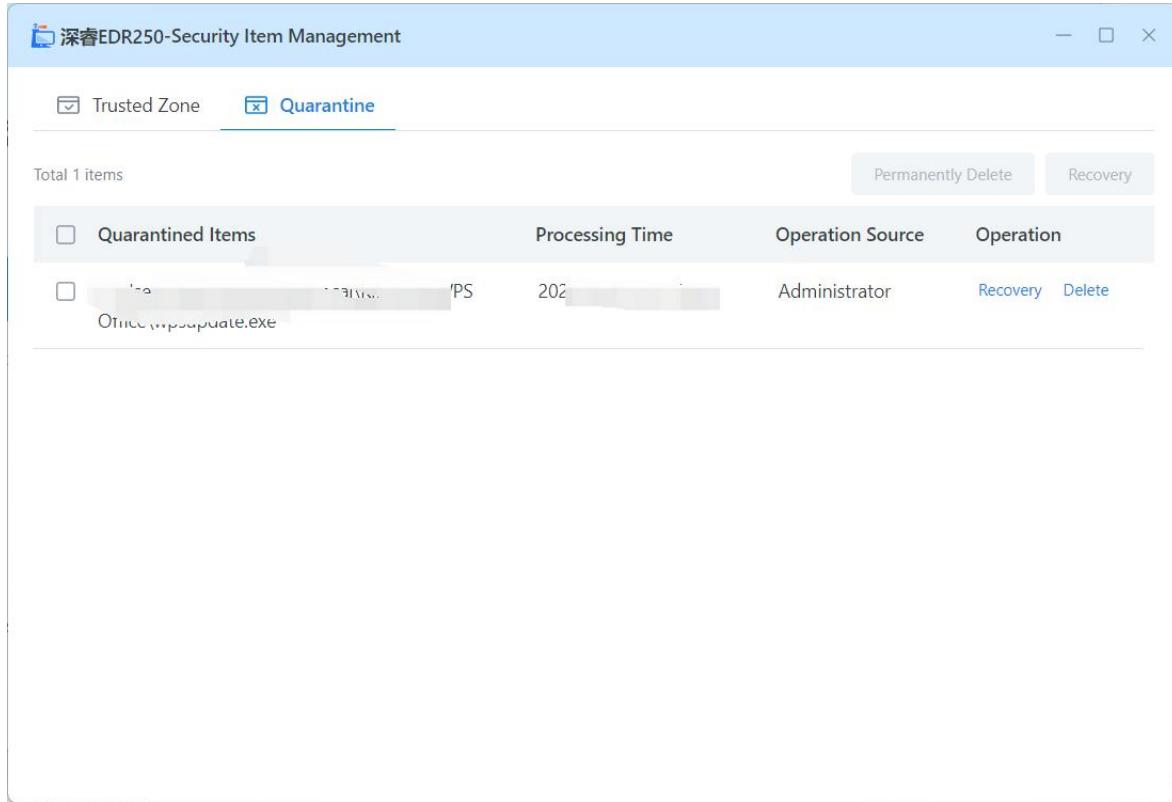
You can click "Trusted Zone/Quarantine Zone" on the home page to enter the security item management page.



In the trust zone, you can manually add trusted directories or files, and the system will no longer scan them in the future.

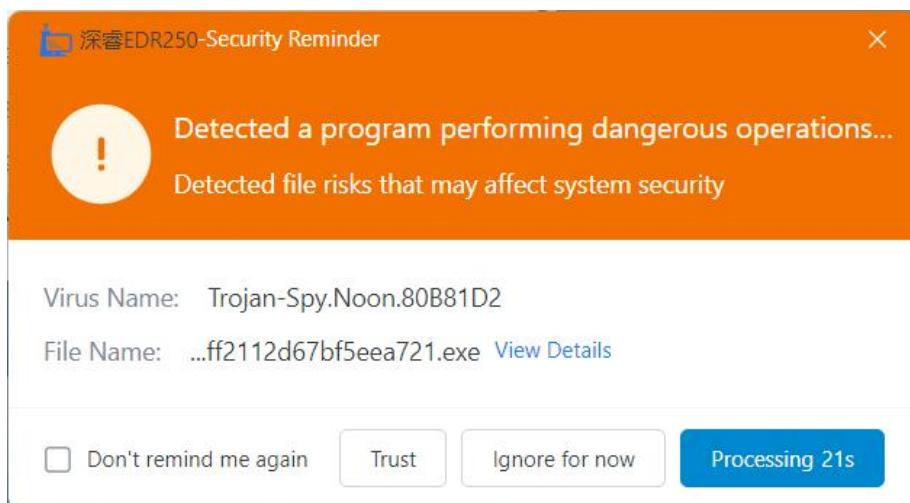


In the quarantine zone, you can delete or restore the quarantined items.



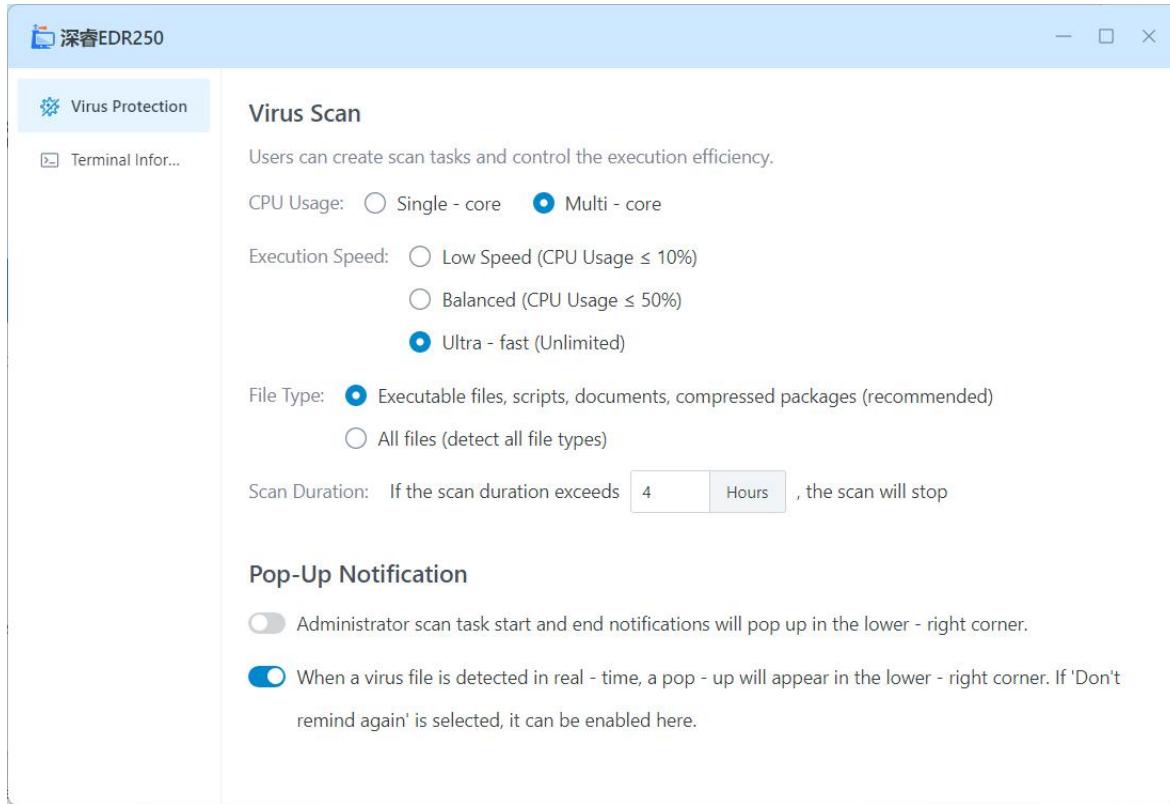
11.3.7. Real - time Detection

The system continuously monitors the security status of the terminal. If a malicious file is detected being written to the disk, a pop - up window will appear. Clicking "Trust" will add it to the trust zone, and clicking "Handle Immediately" will add it to the quarantine zone.

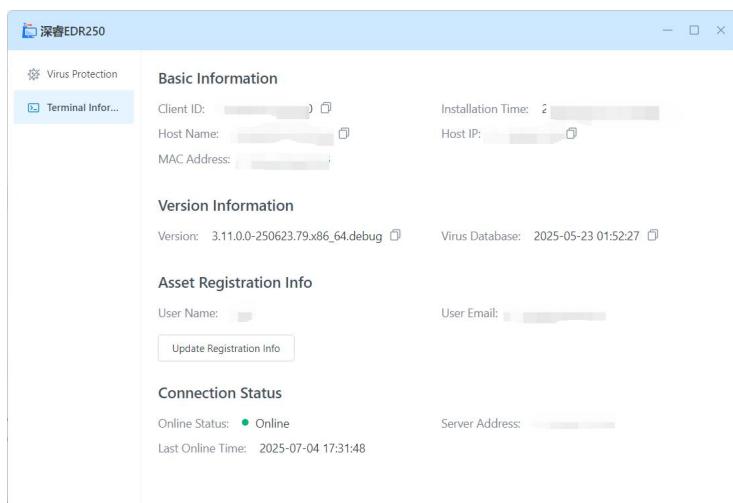


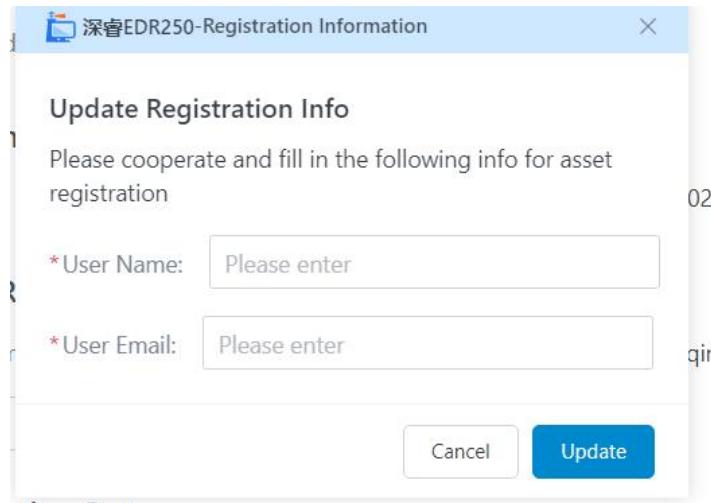
11.3.8. Settings Center

- **Virus Protection:** You can configure virus scanning configurations and pop-up alerts.



- **Terminal Information:** You can view basic information, version information, asset registration information, and connection status here. You can also update the asset registration information.





11.3.9. Log Center

You can view the virus - killing logs, file logs, and specific product update information here.

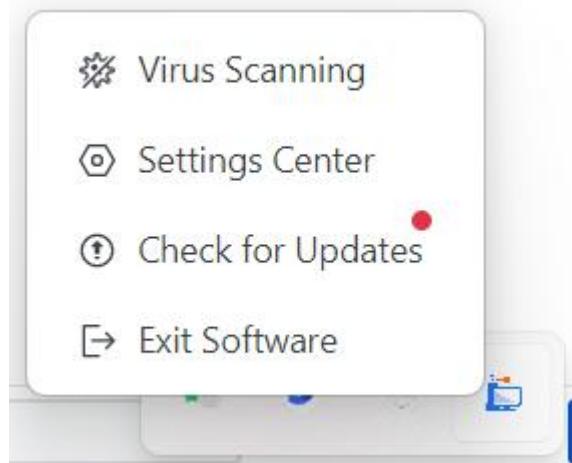
The screenshot shows the Sentry application interface with the "File Logs" tab selected. The main area displays a table of log entries. The columns are: Operation Time, Operation Type, Status, File or Directory Path, and Operation Source. The "Status" column uses colored circles to indicate success (green) or failure (red). A red box highlights the "Status" column. The log entries are:

Operation Time	Operation Type	Status	File or Directory Path	Operation Source
2025-11-24 12:25:29	Delete Isolated File	成功	[REDACTED]	Local User
2025-11-24 12:24:40	Restore Isolated File	失败	[REDACTED]	Local User
2025-11-24 12:24:11	Isolate File	成功	[REDACTED]	Local User
2025-11-24 12:23:26	Delete Isolated File	成功	[REDACTED]	Local User
2025-11-24 12:17:49	Isolate File	成功	[REDACTED]	Local User
2025-11-24 12:17:05	Isolate File	失败	[REDACTED]	Local User
2025-11-24 12:16:19	Remove Trust File	成功	[REDACTED]	Local User

11.3.10. Tray Menu

- Clicking "Virus Scan" will open the home page.
- Clicking "Settings Center" will open the settings center page.
- Clicking "Check for Updates" will open the "Check for Updates" pop - up window on the home page.

- Clicking "Exit Software" will close the application.



11.4. Agent - APP Grayscale Upgrade

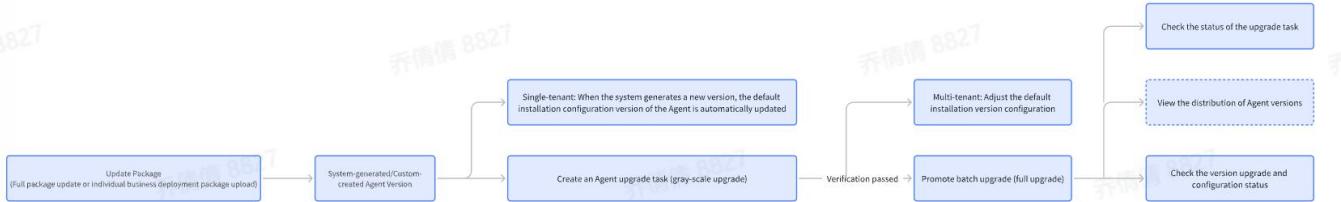
When the system version is upgraded, hotfix upgraded, rollbacked, or an app is installed, a small-scale agent is usually specified for grayscale testing, and the scope of operation can be expanded after the agent version is verified to be running stably.

[Concept Description]

- Agent main program version: the version of the agent client
- Application APP Version: The version of various business APPs, such as the asset inventory APP version, the risk discovery APP version, etc
- Agent version: The version composed of the version of the main program of the agent and the version of each APP on the application side, in the format: version number of the main program of the agent - self-increasing serial number - short hash of the APP collection, followed by the version description of the APP contained in it, and the self-increasing serial number is incremented from 00. For example: 3.6.0.0-250207.15.x86_64-00-d5eghs8s6 ⓘ

[Procedure]

The following is an example of an agent probe (the process of cluster component probes is similar):



11.4.1. Update packages

- You can upload various deployment packages on the Deployment - Application Management page, or you can upload the main agent package separately on the Agent Package Management page.

Package Management page

System Management > Deployment > Application Management

Application Management

Currently deployed product	Recently Updated Applications	Recent Update Time	Number of System Applications	Number of Business Applications
Sentry (5.1.1.0)	Micro Segmentation	2025-07-04 09:35:24	3	18

Please select filter content

Application	Type	Version	Recent Update Time
Micro Segmentation	Business Application	v0.0.2-20250703.1743	2025-07-04 09:35:24
Probe Management	System Application	v3.12.0-20250703.1646	2025-07-03 19:03:17
Compliance Baseline	Business Application	v1.16.0-20250630.1744	2025-07-01 00:34:57
Intrusion Detection and Response	Business Application	v2.11.0-20250630.1829	2025-07-01 00:34:30
Vulnerable	Business Application	v1.17.0-20250630.1746	2025-07-01 00:33:17
Asset Inventory	Business Application	v2.18.0-20250630.1752	2025-07-01 00:28:57
Connection Manager	System Application	v1.3.0-20250627.0935	2025-07-01 00:28:24
Local Engine Management	Business Application	v2.2.0-20250630.1530	2025-07-01 00:27:46
edr_ui	Business Application	v1.4.0-20250630.1635	2025-07-01 00:27:16

11.4.2. The system generates or creates an agent version

- The system automatically generates an agent version:** When the server fully updates the entire package or uploads the package on the Deployment Management - Application Management page, the system automatically generates a set of the latest combined agent versions (one for each system type)
 - For multi-tenant, the global default installation version is not updated and needs to be manually modified by the user. For a single tenant, the global default installation

version is automatically updated every time the agent version is updated

- b. For the version that has not been used by the user, the system will automatically update the version to the latest when there is an update; If the user has already used the version, the system automatically creates a new version

- **User-created agent versions:** On the Deployment Management - Application Management - Agent Version Management page, you can view all agent versions that are generated by the system or created by the user.
 - New Version: You can select the probe type and system type, and specify the version of the main agent program and each APP version to produce a custom agent version
 - Deleting and Editing Versions: Deletion and editing of unconfigured and used custom versions can be supported
 - Copy Version: You can copy a version and make quick adjustments to create a new version
 - Version comparison: You can select two probes of the same type and the same system type for comparison. Highlight version differences.

System Management > Deployment > Application Management > Agent Packages > Agent Version Management

Agent Version Management

Please Select Filtering Content							<input type="text"/>	<input type="button" value="Delete"/>	<input type="button" value="View Comparison"/>	<input type="button" value="New Version"/>																																																																								
282 Items							<table border="1"> <thead> <tr> <th>Probe Type</th><th>System Type</th><th>Probe Version</th><th>Version creation ...</th><th>Update Time</th><th>Operation</th></tr> </thead> <tbody> <tr><td>Agent</td><td>Linux loongarch64</td><td>3.12.0... (1) up-to-date</td><td>Default Installation</td><td>2025-07-03 19:03:15</td><td>copy</td></tr> <tr><td>Agent</td><td>Windows x86_64</td><td>3.12.0... (1) up-to-date</td><td>Default Installation</td><td>2025-07-03 19:03:15</td><td>copy</td></tr> <tr><td>Agent</td><td>Linux x86_64</td><td>3.12.0... (1) up-to-date</td><td>Default Installation</td><td>2025-07-03 19:03:15</td><td>copy</td></tr> <tr><td>Agent</td><td>Linux aarch64</td><td>3.12.0... (1) up-to-date</td><td>Default Installation</td><td>2025-07-03 19:03:15</td><td>copy</td></tr> <tr><td>Cluster Agent</td><td>Linux aarch64</td><td>3.12.0... (1) up-to-date</td><td>Default Installation</td><td>2025-07-03 19:03:15</td><td>copy</td></tr> <tr><td>Agent</td><td>Linux sw_64</td><td>3.12.0... (1) up-to-date</td><td>Default Installation</td><td>2025-07-03 19:03:15</td><td>copy</td></tr> <tr><td>Agent</td><td>Linux loongarch64d</td><td>3.12.0... (1) up-to-date</td><td>Default Installation</td><td>2025-07-03 19:03:15</td><td>copy</td></tr> <tr><td>Cluster Agent</td><td>Linux x86_64</td><td>3.12.0... (1) up-to-date</td><td>Default Installation</td><td>2025-07-03 19:03:15</td><td>copy</td></tr> <tr><td>Agent</td><td>Windows x86_64</td><td>3.12.0.0-250701.8.x... (1)</td><td>Default Installation</td><td>2025-07-01 10:05:31</td><td>copy</td></tr> <tr><td>Agent</td><td>Linux x86_64</td><td>3.12.0.0-250701.8.x... (1)</td><td>Default Installation</td><td>2025-07-01 10:05:31</td><td>copy</td></tr> <tr><td>Agent</td><td>Linux sw_64</td><td>3.12.0.0-250701.8.s... (1)</td><td>Default Installation</td><td>2025-07-01 00:32:10</td><td>copy</td></tr> </tbody> </table>	Probe Type	System Type	Probe Version	Version creation ...	Update Time	Operation	Agent	Linux loongarch64	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy	Agent	Windows x86_64	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy	Agent	Linux x86_64	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy	Agent	Linux aarch64	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy	Cluster Agent	Linux aarch64	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy	Agent	Linux sw_64	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy	Agent	Linux loongarch64d	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy	Cluster Agent	Linux x86_64	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy	Agent	Windows x86_64	3.12.0.0-250701.8.x... (1)	Default Installation	2025-07-01 10:05:31	copy	Agent	Linux x86_64	3.12.0.0-250701.8.x... (1)	Default Installation	2025-07-01 10:05:31	copy	Agent	Linux sw_64	3.12.0.0-250701.8.s... (1)	Default Installation	2025-07-01 00:32:10	copy	<input type="button" value="Delete"/>	<input type="button" value="View Comparison"/>	<input type="button" value="New Version"/>
Probe Type	System Type	Probe Version	Version creation ...	Update Time	Operation																																																																													
Agent	Linux loongarch64	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy																																																																													
Agent	Windows x86_64	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy																																																																													
Agent	Linux x86_64	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy																																																																													
Agent	Linux aarch64	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy																																																																													
Cluster Agent	Linux aarch64	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy																																																																													
Agent	Linux sw_64	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy																																																																													
Agent	Linux loongarch64d	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy																																																																													
Cluster Agent	Linux x86_64	3.12.0... (1) up-to-date	Default Installation	2025-07-03 19:03:15	copy																																																																													
Agent	Windows x86_64	3.12.0.0-250701.8.x... (1)	Default Installation	2025-07-01 10:05:31	copy																																																																													
Agent	Linux x86_64	3.12.0.0-250701.8.x... (1)	Default Installation	2025-07-01 10:05:31	copy																																																																													
Agent	Linux sw_64	3.12.0.0-250701.8.s... (1)	Default Installation	2025-07-01 00:32:10	copy																																																																													
282 Items							1 2 3 4 5 6 >	50 Item/Page																																																																										

11.4.3. Creating an Agent Upgrade Task (Grayscale Upgrade)

Tenant administrators can create upgrade tasks on the Tenant Management-Agent-Agent Tasks page.

A standard account can create an upgrade task on the Agent Management-Running Monitor-Agent page.

Note: For the installation of a new product APP, you need to ensure that the corresponding agent has obtained the authorization of the corresponding product (the authorization can be adjusted in the 'Agent-Operation Management-Authorization Configuration' function), and then upgrade before the installation can be successful.

11.4.4. Promote batch upgrades

The grayscale upgrade verification version runs stably, and upgrade tasks can be created in batches to complete the full upgrade.

In System Management, Deployment Management, Application Management, and Agent Version Management, set the global default installation version to the current verification version.

11.4.5. View the status of the upgrade task

Tenant administrators can view task execution records on the Tenant Management - Agent - Agent Tasks page.

For a standard account, you can view tasks and execution records on the Agent Management-Task Management page.

11.4.6. Check the distribution of agent versions

Go to System Management - Deployment Management - Application Management - Agent Package

Management - Agent Version Distribution to view the number and status of agent versions of different versions in each tenant as the basis for upgrade troubleshooting.

Agent Version Distribution

This function supports viewing the distribution of installed Agents by version for the tenant, and updates the data every 5 minutes.

Please Select Filtering Content								
90 items								
Tenant Na...	System T...	Running ...	Agent Version	Total Agent ...	Agent Onlin...	Number of A...	Number of A...	
kewitest	Linux x86_64	Host	3.10.0.0-250522.84.x86_64-01...	1	8	7	0	0
default	Windows x86_64	Host	3.11.0.0... ⓘ Default Installation	6	6	0	0	
ztest	Linux x86_64	Host	3.12.0.0-250630.3.x86_64.deb...	1	8	6	0	0
default	Linux x86_64	Host	3.11.0.0-250612.59.x86_64.de...	1	10	5	0	0
default	Windows x86_64	Host	3.11.0.0-250619.71.x86_64.de...	1	4	3	0	0
default	Windows x86_64	Host	3.11.0.0-250603.26.x86_64.de...	1	4	2	0	0
zwh	Linux aarch64	Host	3.11.0.0... ⓘ Default Installation	2	2	0	0	
autotest	Linux x86_64	POD	3.12.0.0... ⓘ Default Installation	2	2	0	0	
idsautotest	Linux x86_64	Host	3.10.0.0-250521.82.x86_64.de...	1	2	2	0	0
default	Linux aarch64	Host	3.11.0.0-250603.26.aarch64.de...	1	1	1	0	0

90 items

11.4.7. Check the version upgrade and configuration

In Tenant Management - Agent - Agent Runtime, you can view the distribution of agent types and quantities in each tenant, and click View Details to check whether the agent master program version and app version of the tenant are consistent with the configuration, which can be used to troubleshoot upgrade failures.

Version Detail								
Agent Cluster Agent								
Please Select Filtering Content								
11 items								
Agent ID	Host	Actual version of probe main...	Probe main program configu...	Is the main ...	Actual version of APP	Operation		
dd1cb45bcd720089	10.108.109.203 titan	3.11.0.0-250614.81.x86_64.debug	3.11.0.0-250614.81.x86_64.debug	Yes	Asset Inventory: v2.17.0-20250612... Local Engine Management: v2.1.0-... Compliance Baseline: v1.15.0-202... Event Collect: v2.7.0-202505823.1651 Intrusion Detection and Response: v. Micro Segmentation: v0.0.2-20250... Security Control: v1.4.0-20250906... Vulnerable: v1.16.0-20250907.2028	Download... Download the operati...		
a87915cb21a017	172.16.22.13 localhost.localdomain	3.12.0.0-250703.16.x86_64.debug	3.12.0.0-250703.16.x86_64.debug	Yes	Asset Inventory: v2.18.0-20250630... Local Engine Management: v2.2.0-... Compliance Baseline: v1.16.0-202... Event Collect: v2.8.0-20250630.1804 Intrusion Detection and Response: v. Micro Segmentation: v0.0.2-20250...	Download... Download the operati...		

11 items

12. General Features

12.1. Probes

12.1.1. Running Monitor

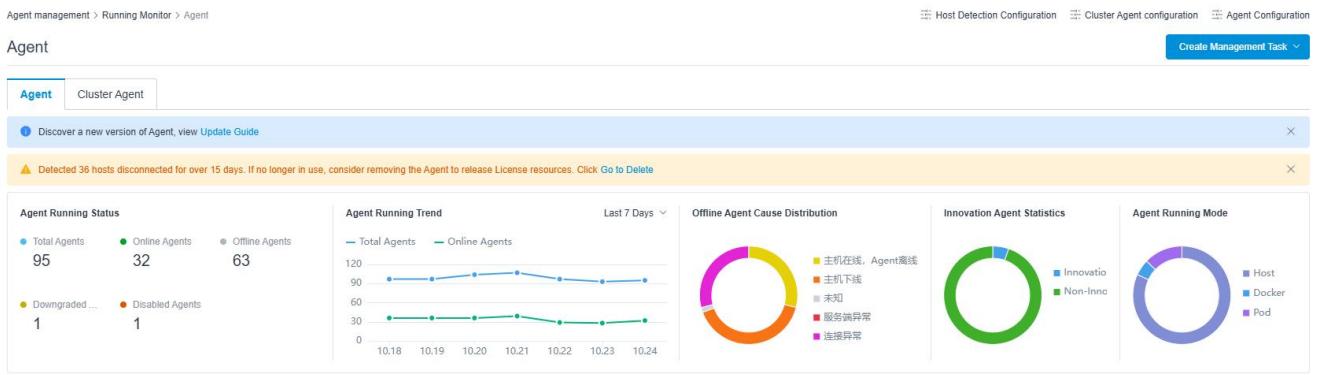
12.1.1.1. Agent

The agent management function can help you overview the running status of the agent on the machine, display the basic agent information, probe configuration information, and performance parameter information of each machine, support users to create and restart, Upgrade, Uninstall, drive start/stop and other Operation and Maintenances of the agent, and configure the agent's performance, reclamation policy, and security protection policy, so as to achieve comprehensive management of the agent.

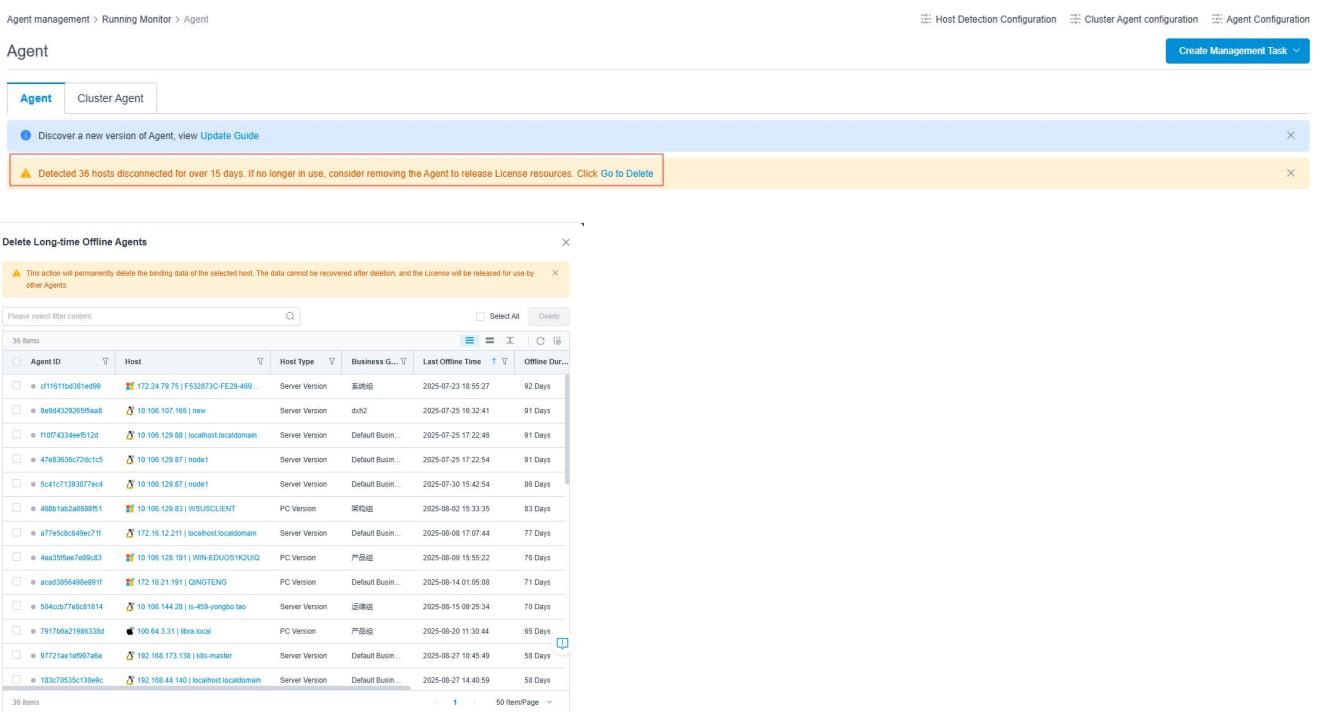
12.1.1.1.1. Agent

12.1.1.1.1.1. Agent list

This function provides visual statistics on the different running states of the agent, the running trend of the agent in the last 7 days, 15 days, and 30 days, the Offline Agent Cause Distribution, the information of China-specific agent, and the distribution of the agent running mode.



If there are hosts disconnected for more than 15 days, a prompt will appear: "Found x hosts disconnected for more than 15 days. If they are no longer in use, it is recommended to delete the Agent to release license resources. Click to delete." Clicking "Click to delete" will pop up the "Delete Long-Term Offline Agents" drawer, allowing for batch deletion.



The agent list displays details such as the running mode, agent ID, host, host type, agent version, running level, integrated modules, and offline status. It supports batch filtering by Agent ID or IP, where multiple input values can be separated by "|".

Please Select Filtering Content						More Operations	Upgrade	Uninstall	Restart
43 items						Up	C	Uninstall	Restart
Runnin...	Agent ID	Host	Host Type	Agent Version	Operation				
<input type="checkbox"/> POD	● [REDACTED]	● [REDACTED]	Server	3.10.0.0-250521.82.x86_6 4.debug-02-217ed399	Details Download I... Download t...				
<input type="checkbox"/> POD	● [REDACTED]	● [REDACTED]	Server	3.10.0.0-250521.82.x86_6 4.debug-02-217ed399	Details Download I... Download t...				
<input type="checkbox"/> Host	● [REDACTED]	● [REDACTED]	PC	3.10.0.0-250520.75.x86_6 4.debug-01-9731d1a6	Details Download I... Download t...				

12.1.1.1.1.2. Details

Click Agent ID or Operation - > Details to view the Details, including basic information, security integration, authorization functions, and deploy application.

- Basic Information: displays the agent configuration and online status, and displays the file installation path of the probe. You can set the run level, log level, edit the performance configuration, and download the run report and logs (so that you can understand the details of the agent run). Provides Operation and Maintenances to restart, uninstall, upgrade, and enable drivers for the agent/disable drivers for the agent.
- Security integration: displays the integrated and non-integrated modules of the Agent, along with key configuration and status information of the integrations. Clicking on an integration card will redirect to its dedicated management interface for troubleshooting and management.
- Authorization Function: displays the authorization information of the agent, including the host type, authorization status, and authorization function.
- Deploy Application: displays the applications that have been deployed by the agent and their respective versions.

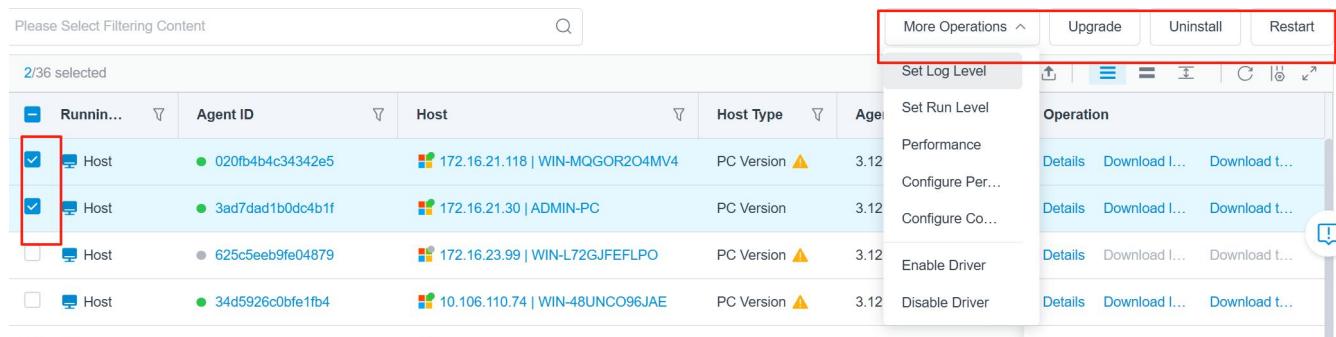
12.1.1.1.3. Agent Operation and Maintenance

Method 1: List operation

Select one or more agents in the list and click Upgrade, Uninstall, Restart, and More to perform

Operation and Maintenances on the current agent.

After the operation is completed, a task is automatically created, and you can view the task execution result and execution records in the Task Management function.

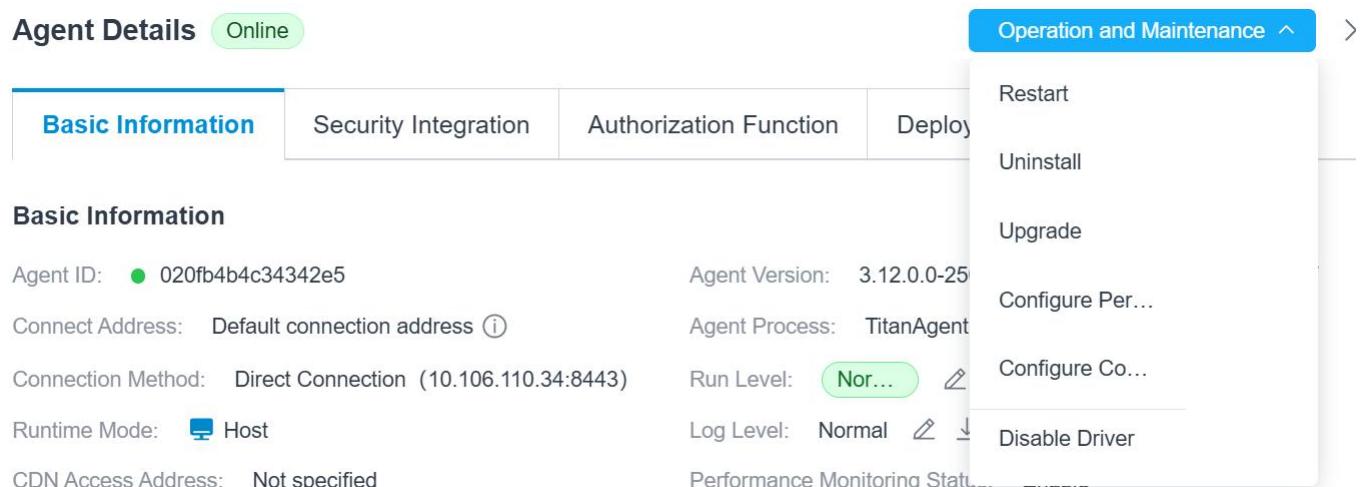


Please Select Filtering Content					More Operations	Upgrade	Uninstall	Restart
2/36 selected					Set Log Level			
Running...	Agent ID	Host	Host Type	Agent Version	Set Run Level	Operation		
<input checked="" type="checkbox"/> Host	020fb4b4c34342e5	172.16.21.118 WIN-MQGOR2O4MV4	PC Version	3.12	Performance	Details	Download I...	Download t...
<input checked="" type="checkbox"/> Host	3ad7dad1b0dc4b1f	172.16.21.30 ADMIN-PC	PC Version	3.12	Configure Per...	Details	Download I...	Download t...
<input type="checkbox"/> Host	625c5eeb9fe04879	172.16.23.99 WIN-L72GJFEFLPO	PC Version	3.12	Configure Co...	Details	Download I...	Download t...
<input type="checkbox"/> Host	34d5926c0bfe1fb4	10.106.110.74 WIN-48UNCO96JAE	PC Version	3.12	Enable Driver	Details	Download I...	Download t...
<input type="checkbox"/> Host					Disable Driver	Details	Download I...	Download t...

Method 2: Create an agent from the details page

Go to the Details and click O&M to select the corresponding task type.

After the operation is completed, a task is automatically created, and you can view the task execution result and execution records in Task Management.



Agent Details Online

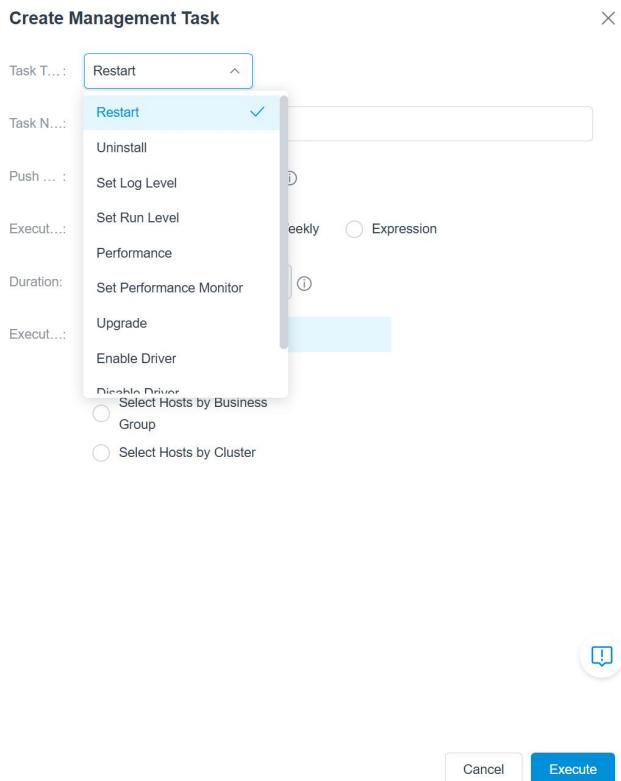
Operation and Maintenance

Basic Information	Security Integration	Authorization Function	Deployment
Basic Information <p>Agent ID: 020fb4b4c34342e5</p> <p>Connect Address: Default connection address (i)</p> <p>Connection Method: Direct Connection (10.106.110.34:8443)</p> <p>Runtime Mode: Host</p> <p>CDN Access Address: Not specified</p>	<p>Agent Version: 3.12.0.0-25</p> <p>Agent Process: TitanAgent</p> <p>Run Level: Normal</p> <p>Log Level: Normal</p> <p>Performance Monitoring Status: Normal</p>	<p>Restart</p> <p>Uninstall</p> <p>Upgrade</p> <p>Configure Per...</p> <p>Configure Co...</p> <p>Disable Driver</p>	

Method 3: Create an administrative task

Go to the Running Monitor -> Agent page, click Create Management Task, choose Agent, configure parameters

such as Task Type, Task Name, and Push Speed to execute the task. You can go to Task Management to view the task execution results and execution records.



The parameters are described as follows:

- Task Type:
 - Set log level: The agent runs in normal mode by default, and the Debug mode is set to make the logging more detailed and the accuracy of the audit logs improved.
 - Set run level: The agent is enabled after installation, and if it is disabled, the agent retains only the most basic communication functions with the server.
 - Performance configuration: If the agent occupies too many system resources, the system cannot run effectively. You can set an agent demotion threshold to restrict the agent's running or even kill the agent process when the resources occupied by the agent reach a certain value.
 - Set performance monitor: When the Agent occupies too many system resources, it will

cause the system to fail to run effectively. The Agent degradation threshold can be set.

When the resources occupied by the Agent reach a certain value, its operation can be restricted or even the Agent process can be directly killed.

- Enable/Disable Driver: Indicates whether the host is allowed to gain the ability to control the driver, which is enabled by default. After deactivation, the host is unable to perform operations on the driver.
- Configure connection address: The connection address refers to the address at which the Agent connects to the server. By default, it is the "default connection address" configured by the system and can be changed.
- Push speed: up to 600 units per minute. If the value is 0, the default configuration is used.
- Execution Period: You can select "Once", "Daily", or "Weekly", or you can customize the settings.
- Duration: If the value is 0 or empty, no limit is required.
- Execution scope: You can select hosts in different filtering methods, such as By list, by business group, and by cluster.

12.1.1.1.4. Agent configuration

Click  Agent Configuration on the Running Monitor -> Agent page to configure the agent recycling, security protection, and function switches.

1. Configure the recycling policy

If the agent is offline for a long time, we recommend that you revoke the authorization of the host to prevent the waste of authorized points. By default, the system requires users to manually reclaim the data by themselves, and you can choose to set an offline duration threshold, and the system will automatically collect it according to the threshold standard.

2. Security protection configuration

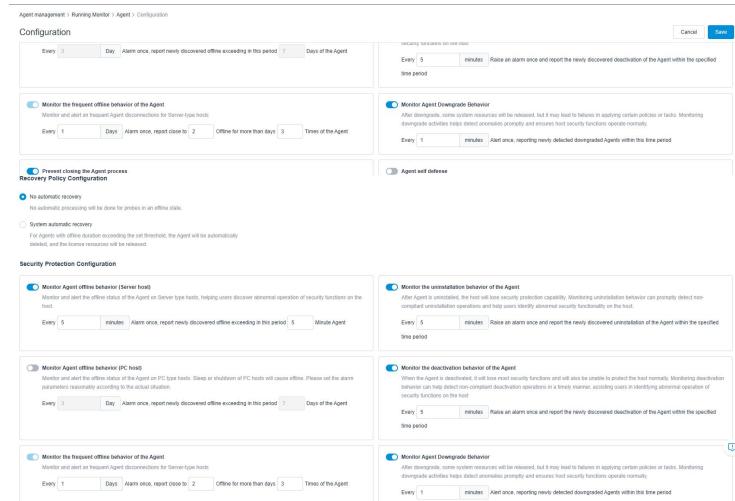
If the host is severely attacked, the agent may be offline, uninstalled, or so on. To prevent the host agent from being attacked and the host loses its ability to protect itself, you can monitor the running status of the agent and report an alarm if abnormal behavior occurs.

- By default, the system enables monitoring of the offline, unmounted, disabled, and frequently offline behaviors of the agent, and prevents the agent process from being shut down. The ability to monitor the agent's frequently offline behavior cannot be disabled.
- The alarm frequency can be set for each configuration
- Prevent the agent process from being disabled: This configuration takes effect only on Linux hosts and depends on the Bash plugin, which you need to install on the plugin management page.
- Agent self-protection: This function depends on the driver, and after the protection is enabled, the agent program exits and the terminal is uninstalled, and the protection password needs to be verified before it can be executed. You can view self-protection interception records.

3. Function switch configuration

Drive Status:

After this switch is enabled, you can see the description of the driver-related detection capabilities and enable the driver to enable the function of the dependent driver. Driver operation will cause a certain burden on performance, so please turn it on with caution.



12.1.1.1.5. Agent Offline Probing

Agent offline probing can quickly check the offline status of hosts and accurately identify machines where "the host is alive but the agent is offline", ensuring the agent coverage and survival rate.

Method 1: Host Detection Configuration - Supports configuring scheduled offline detection.

On the "Running Monitor-> Agent" page, click  to configure host detection. Host detection helps analyze the cause of host offline status by checking network connectivity. It should be noted that detection results are for reference only (If you want to obtain accurate detection results: 1. Try logging in to the cloud host directly; 2. If login is possible, try pinging the server's domain name/IP from the cloud host. 3. If ping is successful, use telnet/netcat/ssh -v -p to check connectivity to port 7788 on the server's Java connection layer. In theory, the Agent remains online if it can access port 7788.); Detection methods include: Agent liveness detection within the same subnet, and server-side liveness detection; Liveness detection is not supported for hosts with only IPv6 addresses; Agent proxy connections only support Agent-based liveness detection, and at least one other Agent must be active within the same subnet.

On this page, the following settings can be made:

- Detection method: You can select "Agent Liveness" or "Server Liveness" to determine the

specific way to detect the network connectivity of offline hosts.

- **Detection mode:** There are two options: "Ping scan" and "Nmap scan" to scan the network status of the host.
- **Automatic detection operation:** You can select "Disable auto-probing". At this time, no automatic processing is performed on hosts in offline status, and only host offline data is recorded in the list. You can also select "Enable auto-probing". The system will scan the host regularly according to the rules. For hosts whose offline duration exceeds the set threshold, it will automatically detect their network connectivity and record the detection results.
- **Max packets per second:** You can set the maximum number of detection packets sent per second, which affects the detection efficiency and network load.

After all configurations are completed, click the "Save" button to take effect. If you want to cancel the configuration, click the "Cancel" button.

Agent Management > Runtime Monitoring > Runtime Monitoring > Agent Management > Host Detection Configuration

Host Detection Configuration

Host detection helps analyze the cause of host offline status by checking network connectivity.
Note: 1. Detection results are for reference only. Click to view [Accurate Detection Method](#).
2. Detection methods include: Agent liveness detection within the same subnet, and server-side liveness detection.
3. Liveness detection is not supported for hosts with only IPv6 addresses.
4. Agent proxy connections only support Agent-based liveness detection, and at least one other Agent must be active within the same subnet.

*Detection Met...: Agent Liveness Server Liveness

*Detection Mode: Ping Scan
 Nmap Scan

Automatic Detect...:
 Disable Auto-Probing
No automatic actions are taken for offline hosts; only offline records are kept in the list.
 Enable Auto-Probing
The system periodically scans hosts based on rules. For hosts offline longer than the configured threshold, it automatically probes network connectivity and records the results.

Max Packets p...:

[Import](#)

[Cancel](#) [Save](#)

Method 2: Manual Detection - Trigger Immediate Execution

[Detect Now](#)

On the "Running Monitor-> Agent" page, click the [Detect Now](#) button directly. By default, this operation will check the network connectivity of all offline hosts in the list. If you first select one or

Detect Now

more Agents that need to be operated on in the list and then click the **Detect Now** button, this operation will check the network connectivity of the selected offline hosts. After execution, a pop-up window will appear in the upper right corner showing "Host Discovery Completed". You can view the detection results (including fields such as host connectivity, last detection time, and last offline reason) in the Agent list on the "Running Monitor-> Agent" page.

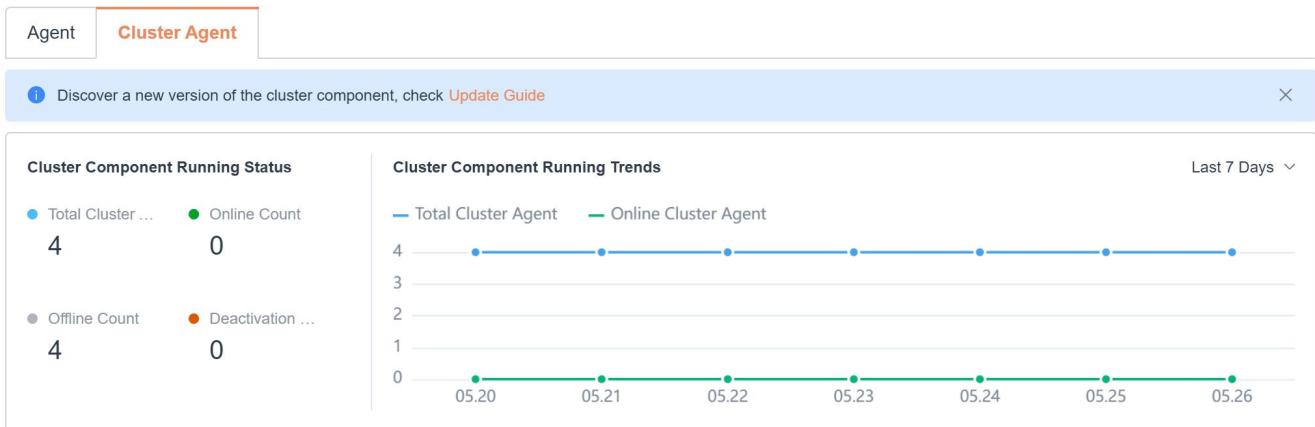
Running...	Agent ID	Host	Host Connectivity	Host Type	Business...	Agent Version	Operation
<input type="checkbox"/> Docker	a0540cb26f35fbe1	10.106.110.181 localhost.localdomain	Connected	Server Version	-	3.13.0-250910.167.x8...	Details Download
<input type="checkbox"/> Docker	933b9eb7ca047722	10.106.110.106 crack-4c8g	Connected	Server Version	-	3.13.0-250910.167.x8...	Details Download

Running...	Integrated Modules	Latest Online Time	Last Offline Time	Last Detection Time	Last Offline Reason	Frequent Offline	Operation
Normal	eBPF +2 items	2025-09-15 11:26:11	-	-	-	Normal	Details Download
Normal	eBPF +2 items	2025-09-15 11:25:54	-	-	-	Normal	Details Download

12.1.1.1.2. Cluster Agent

12.1.1.1.2.1. List of Cluster Agents

This feature displays graphical statistics on the running trends of Cluster Agents in different running states and the last 7 days, 15 days, and 30 days.



The Cluster Agent list displays details such as the Agent ID, cluster name, node, agent version, running level, integrated modules, and offline status of the Cluster Agent.

Please Select Filtering Content		Q	More Operations	Upgrade	Uninstall	Restart
4 items						
<input type="checkbox"/> Cluster Comp...	Cluster Name	Node	Cluster Co...	Operation		
<input type="checkbox"/>	● [REDACTED]	● [REDACTED] 1 [REDACTED]	3.9.0.0-2504...	D... Download log	load the operation re	
<input type="checkbox"/>	● [REDACTED]	● [REDACTED] 1 [REDACTED]	3.9.0.0-2504...	D... Download log	load the operation re	
<input type="checkbox"/>	● [REDACTED]	● [REDACTED]	3.9.0.0-2504...	D... Download log	load the operation re	

12.1.1.1.2.2. Cluster Details

Click Cluster Agent ID or Operation -> Details to view the details of the Cluster Agent, including basic information, security integration, and deploy application.

- **Basic Information:** displays the basic information, component configurations, and performance configurations of the Cluster Agent, allows you to configure the running level and log level, and downloads the running reports and logs (to help you understand the running status of the Cluster Agent).
- **Security Integration:** displays the integrated and non-integrated modules of the Agent, along with key configuration and status information of the integrations. Clicking on an integration card will redirect to its dedicated management interface for troubleshooting and management.

- Deploy Application: displays the applications that have been deployed by the Cluster Agent and their corresponding versions.

12.1.1.2.3. Cluster Agent Operation and Maintenance

Method 1: List operation

Select one or more clusters in the list and click Upgrade, Uninstall, Restart, and More to perform Operation and Maintenances on the current cluster agent. After the operation is completed, a task is automatically created, and you can view the task execution result and execution records in the Task Management function.

The screenshot shows a table of cluster components. The columns are: Cluster Comp..., Cluster Name, Node, Cluster Co..., and Operation. The first row has a checked checkbox in the first column. The 'Operation' column contains buttons for More Operations, Upgrade, Uninstall, and Restart, with 'More Operations' highlighted with a red box. A search bar at the top right says 'Please Select Filtering Content'.

Cluster Comp...	Cluster Name	Node	Cluster Co...	Operation
<input checked="" type="checkbox"/> d16c3f59fa62008e	● [redacted]	⚠ [redacted]	3.9.0.0-2504...	D... Download log/upload the operation re
<input type="checkbox"/> d3fe32a280397b94	● [redacted]	⚠ [redacted]	3.9.0.0-2504...	D... Download log/upload the operation re

Method 2: Create a Cluster Agent from the Cluster Details page

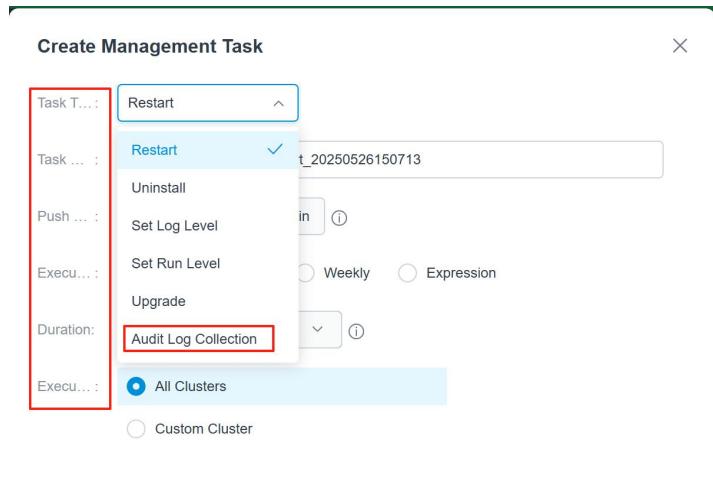
Go to the Details and click O&M to select the corresponding task type. After the operation is completed, a task is automatically created, and you can view the task execution result and execution records in Task Management.

The screenshot shows the 'Cluster Component Details' page. It includes tabs for Basic Information, Security Integration, and Deploy Application. On the right, a 'Operation and Maintenance' dropdown menu is open, containing options: Restart, Uninstall, Upgrade, Audit Log Collection, and an ellipsis (...). The 'Operation and Maintenance' button is highlighted with a red box.

Method 3: Create an administrative task

Go to the Running Monitor -> Agent page, click Create Management Task, choose Cluster Agent, configure parameters such as Task Type, Task Name, and Push Speed to execute the task. You can go to Task

Management to view the task execution results and execution records.



The parameters are described as follows:

- Task Type:
 - Set log level: The agent runs in normal mode by default, and the Debug mode is set to make the logging more detailed and the accuracy of the audit logs improved.
 - Set run level: The agent is enabled after installation, and if it is disabled, the agent retains only the most basic communication functions with the server.
 - Set performance monitor: When the Agent occupies too many system resources, it will cause the system to fail to run effectively. The Agent degradation threshold can be set. When the resources occupied by the Agent reach a certain value, its operation can be restricted or even the Agent process can be directly killed.
- Configure connection address: The connection address refers to the address at which the Agent connects to the server. By default, it is the "default connection address" configured by the system and can be changed.
- Audit log collection: Cluster audit logs are set to "Not Collected" by default. If "Collected" is selected, the system can automatically identify the Log/Webhook backend collection methods and monitor the collection status, which is used to detect

abnormal behaviors of the cluster. In addition, audit log collection supports refined audit log collection in high-availability cluster environments. It can collect audit logs from all apiserver nodes in the cluster at one time, achieving full coverage of node logs.

- Execution Scope: You can select a cluster by filtering methods.

The other parameters are the same as those in Agent Operation and Maintenance - > Create Management Task.

12.1.1.2.4. Cluster Agent Configuration

Click  on Running Monitor -> Agent to configure the recycling and security protection of the Cluster Agent.

1. Configure the recycling policy

For cluster agents that have been offline for a long time, you can revoke the authorization to prevent the waste of authorized points. You can choose to set a threshold and the system automatically recycles it according to the threshold standard, or the user manually recycles it by yourself.

2. Security protection configuration

To prevent the Cluster Agent from being unusable due to an attack on the host, you can monitor the offline and uninstallation of the Cluster Agent. Users can set an alarm period to understand the offline Uninstalling situation in real time, and report the alarm once abnormal behavior occurs.

- By default, the system enables monitoring of offline, unmounted, disabled, and frequent offline behaviors of the cluster agent, and prevents the cluster agent process from being shut down. The ability to monitor the frequently offline behavior of the cluster agent cannot be disabled.
- For different abnormal behaviors, you can set an alarm period to understand the abnormal

conditions of the Cluster Agent in real time.

Configuration

[Cancel](#) [Save](#)

Recovery Policy Configuration

No automatic recovery

No automatic processing will be done for probes in an offline state.

System automatic recovery

For probes with offline duration exceeding the set threshold, probes will be automatically deleted.

Security Protection Configuration

<p><input checked="" type="checkbox"/> Monitor offline behavior of Cluster Agent</p> <p>Every <input type="text" value="5"/> minutes Alert once, report newly discovered offline exceeding in this period</p> <p><input type="text" value="5"/> Minute cluster component</p>	<p><input checked="" type="checkbox"/> Monitor deactivation behavior of Cluster Agent</p> <p>When Cluster Agent are deactivated, the corresponding security functions will be lost, and normal host protection will also be impossible. Monitoring deactivation behavior can promptly detect non-compliant deactivation operations, helping users discover abnormal operation of security functions on the host.</p> <p>Every <input type="text" value="5"/> minutes Alert once, report newly discovered deactivation of Cluster Agent in this time period</p>
<p><input checked="" type="checkbox"/> Monitor uninstallation behavior of Cluster Agent</p> <p>After uninstalling the Cluster Agent, the host will lose the corresponding security protection capabilities. Monitoring uninstallation behavior can promptly detect non-compliant uninstallation operations, helping users discover abnormal operation of security functions on the host.</p> <p>Every <input type="text" value="5"/> minutes Alert once, report newly discovered uninstallation of Cluster Agent in this time period</p>	<p><input checked="" type="checkbox"/> Monitor frequent offline behavior of Cluster Agent</p> <p>Alert for Cluster Agent with frequent offline anomalies</p> <p>Every <input type="text" value="1"/> Days Alert once, report close to <input type="text" value="2"/> Offline for more than days</p> <p><input type="text" value="3"/> Cluster component of the time</p>

12.1.1.2. Equipment Approval

12.1.1.2.1. Equipment audit configuration

Administrators can set the review method for the installation and launch of Agents.

Click  on the upper right corner on the Running Monitor -> Equipment

Approval page to enable agent terminal review or agent installation password.

Equipment Approval Configuration

[Cancel](#) [Save](#)

Agent terminal audit

After enabling the audit, Agent, the online request needs to pass the server-side audit before it can be executed

*Equipment type: Server version PC version

Agent installation password

After enabling installation protection, the agent needs to enter a password before going online

*Protection password: 

Note:

- If the agent terminal review is enabled, the agent online request needs to be filled in with management information, which can be executed only after the server review is passed, and

the administrator can see the relevant device information in Running Monitor - > Equipment Approval - Pending, and can approve or reject it.

- If you enable the agent installation password, the agent needs to enter the password before you can go online.

12.1.1.2.2. Equipment approval

The page displays pending/processed approvals, with detailed information including device name, device type, user, authorization module, etc.

Equipment Approval

Pending processing	Processed								
Please select filter content									
<input type="button" value="to examine"/>									
0 items									
<table><thead><tr><th>Equipment name</th><th>Equipment ...</th><th>User</th><th>IP, MAC address</th><th>Authorizati...</th><th>Application...</th><th>Applicat...</th><th>Operation</th></tr></thead></table>		Equipment name	Equipment ...	User	IP, MAC address	Authorizati...	Application...	Applicat...	Operation
Equipment name	Equipment ...	User	IP, MAC address	Authorizati...	Application...	Applicat...	Operation		
 No Data									

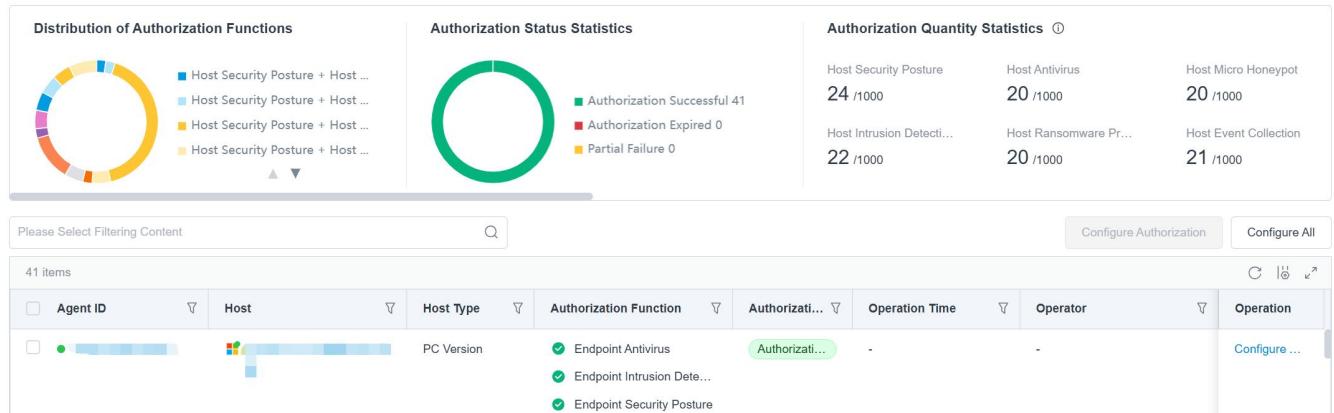
12.1.1.3. License

12.1.1.3.1. License List

This function visualizes the distribution and authorization status of the agent, counts the authorization quota and various authorization consumption obtained by the tenant, displays the authorization function type and authorization status of each agent, and supports modification of the authorization configuration of the agent.

The system provides a search box for users to query the specified host to view its authorization status.

License

[Update](#)

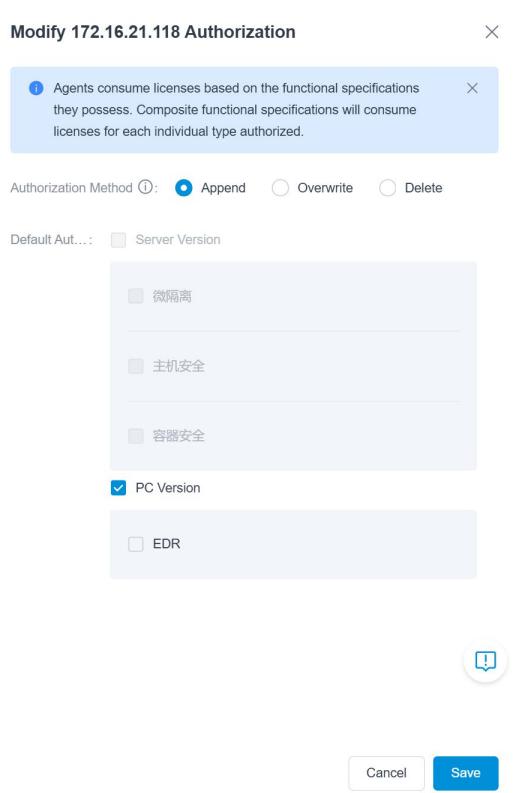
12.1.1.3.2. Configure License

Method 1: Configure the configuration separately

Select a host and click Configure Authorization in the operation bar of the list to configure authorization for the current host.

Authorization method description:

- New addition: On the basis of the original authorization of the host, add the selected authorization.
- Coverage: The original authorization functions of the host are completely replaced by the selected authorization. Data that does not match the selected host type will be filtered. It is recommended to configure the Server host and the PC host separately.
- Remove: On the basis of the original authorization of the host, remove the selected authorization



Method 2: Configure in batches

Click the checkbox on the left side of the list to select one or more hosts, and then click

Configure Authorization

to fill in the relevant parameters.

Method 3: Configure all the configurations

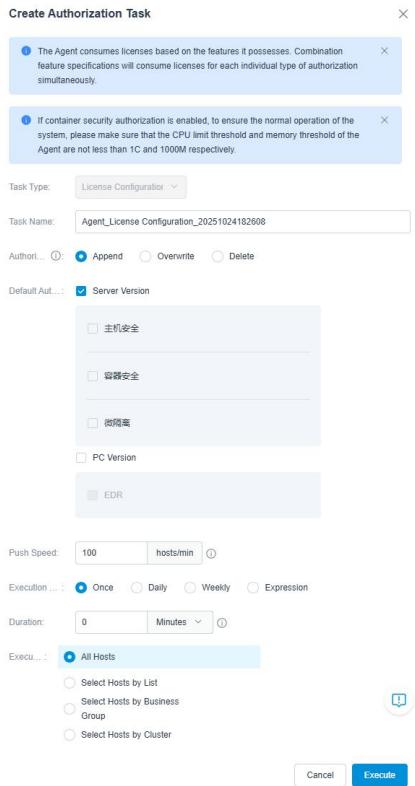
Configure All

Click **Configure All** to configure the filtered results of the list with one click.

Method 4: Create Configuration Task

Create Authorization Task

Click **Create Authorization Task** on the page, configure parameters such as "Task Name", "Authorization Method", "Default Authorization Function", "Push Speed", "Execution Cycle", "Duration", and "Execution Scope", then execute the task. You can view the task execution results and records in "Task Management".



Parameter Description:

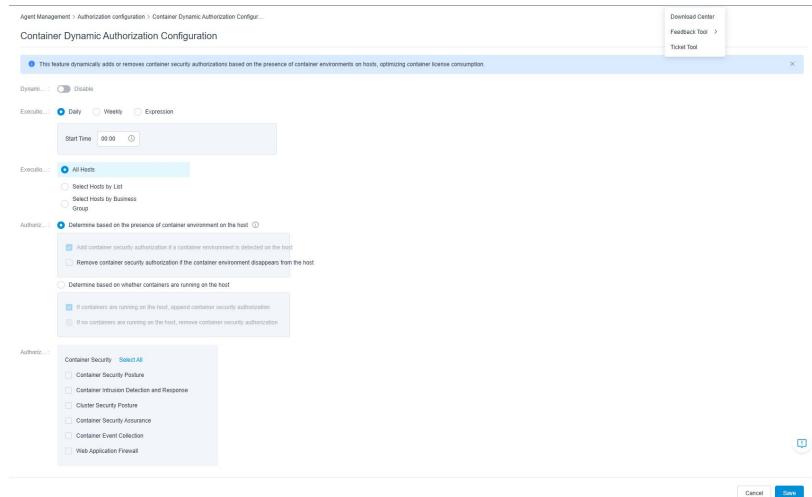
- **Task Type:** Authorization Configuration (fixed value).
- **Task Name:** Defaults to "Agent_AuthorizationConfig_Timestamp" and can be modified.
- **Authorization Method:** Options include "Add", "Overwrite", and "Remove" (single selection, with "Add" selected by default). Authorization can be configured separately for Server and PC hosts; data that does not match the selected host type will be filtered out.
 - **Add:** Append the selected authorization to the host's existing authorization.
 - **Overwrite:** Completely replace the host's existing authorized functions with the selected authorization.
 - **Remove:** Remove the selected authorization from the host's existing authorization.
- **Default Authorized Functions:** Configured separately for PCs and Servers, with each configuration taking effect independently (multiple selections allowed).
- **Push Speed:** Maximum 600 units per minute. A value of 0 indicates following the system's

default configuration.

- **Execution Cycle:** Optional options include "Once", "Daily", "Weekly", or custom settings.
- **Duration:** A value of 0 or an empty field indicates no limitation.
- **Execution Scope:** Provides various filtering methods to select hosts, such as "All", "By List", "By Business Group", and "By Cluster".

12.1.1.3.3. Container Dynamic Authorization Configuration

Click  on the page to dynamically add or remove container security authorizations based on the survival status of container environments on the host, so as to reasonably consume the number of container authorizations.



Parameter Description:

- **Dynamic Authorization:** Disabled by default.
- **Execution Cycle:** Daily, Weekly, or Expression.
- **Execution Scope:** All hosts, Select hosts by list (only Linux hosts are displayed), or Select hosts by business group.
- **Authorization Action:** Required, single selection.
 - **Judgment based on the existence of container environment on the host** (selected by default)

default):

- Judgment criterion: Whether there are container runtime processes on the host machine.
 - If a container environment is detected on the host, append container security authorization.
 - If the container environment on the host disappears, remove container security authorization.
- **Judgment based on the running status of containers on the host:**
 - If there are running containers on the host, append container security authorization.
 - If no running containers are detected on the host, remove container security authorization.
- **Authorized Functions:** Required, select at least one item. Supports one-click select all and one-click deselect all. Includes all authorized products under the container security category.

12.1.2. Task Management

Displays agent and cluster agent tasks, manages them, and views execution results and execution records.

12.1.2.1. Task List

In the task management list, you can display information such as the task name, task type, probe type, and execution data, and provide options to view the execution result, edit, and Uninstall the task.

The system sets up a general search box to support the search for specific tasks.

Task Management

Status		Task Name	Task Type	Probe T...	Total Exec...	Executor	Operation
<input type="checkbox"/>	<input checked="" type="checkbox"/> Disable	Agent_设置日志级别_20250526155335	Set Log Level	Agent	1	1	Execute... Edit Delete
<input type="checkbox"/>	<input checked="" type="checkbox"/> Disable	Agent_删除_20250526154833	Uninstall	Agent	1	1	Execute... Edit Delete
<input type="checkbox"/>	<input checked="" type="checkbox"/> Disable	Agent_设置日志级别_20250526154651	Set Log Level	Agent	1	1	Execute... Edit Delete
<input type="checkbox"/>	<input checked="" type="checkbox"/> Disable	Agent_设置运行级别_20250526154556	Set Run Level	Agent	1	1	Execute... Edit Delete

Click Execution Results to view the details of the execution result of the task, including the basic information of the task, execution statistics, and the execution result details of each probe.

Total Executions	Executed	Successes	Failures
1	1	1	0

Agent ID	Host	Execution Time	Execution Details
● [REDACTED]	[REDACTED]	2025-05-26 15:53:34	Success

12.1.2.2. Execution Records

Click Execution Records to view the status of each execution batch of the task.

There are three types of execution statuses: Executing, Partially Failed, or Completed.

- A task that is in progress cannot be re-executed.
- For partially failed tasks, click Re-execute to take effect only for probes that failed in the last execution, and probes that have been successfully executed will not be executed repeatedly.

Execution Records

Please Select Filtering Content							<input type="button" value="Re-execute"/>
287 items							
<input type="checkbox"/>	Start Time	End Time	Task Na...	Task Type	Probe T...	Executio...	Operation
<input type="checkbox"/>	2025-05-26 15:53:34	2025-05-26 15:53:37	Agent_设置日...	Set Log Level	Agent	Completed	Re-execute Details
<input type="checkbox"/>	2025-05-26 15:48:32	2025-05-26 15:48:33	Agent_删除_2...	Uninstall	Agent	Completed	Re-execute Details
<input type="checkbox"/>	2025-05-26 15:46:50	2025-05-26 15:46:59	Agent_设置日...	Set Log Level	Agent	Completed	Re-execute Details
<input type="checkbox"/>	2025-05-26 15:45:55	2025-05-26 15:45:57	Agent_设置运...	Set Run Level	Agent	Completed	Re-execute Details

12.1.3. Security Tools

12.1.3.1. Tool Center

The function provides various security gadgets, such as file query, network tools, process query, web query, account control, security detection, etc., which can help users quickly and easily perform query analysis or response processing.

Tool Center

This feature provides various security tools such as file queries, network tools, process queries, web queries, account control, security detection, etc. It can help users quickly and conveniently perform query analysis or response processing.

<input type="text" value="Search Tool Type"/>	<input type="text" value="Please enter filter options"/>	<input type="button" value=""/>
All Types 69		
Process Inquiry 12	Get the system's timestamp and timezone   1111	Tool Type Security Tools Update Time 2025-05-20 10:05:40
Network Tools 6	Find logs in the log file for the specified time period  Find logs in the log file for the specified time period	Tool Type Document Query Update Time 2025-04-24 17:09:40
Document Query 23	File upload  <output>. Upload the input file path to minio	Tool Type Document Query Update Time 2025-03-21 09:57:43
Security Tools 9	[File Query] Specify start and end offsets to obtain specified...   Input start and end offsets to view the content of any specified line in the text file	Tool Type Document Query Update Time 2025-04-18 10:43:53
Others 1	Clean up redundant files in the 3.x and 5.0 migrations   Clean up redundant files in the 3.x and 5.0 migrations	Tool Type Agent Operations Update Time 2025-03-13 15:14:28
Web query 9		
Agent Operations 9		

12.1.3.1.1. View tool details



Click a tool or

view its details, including basic information, tool introduction, risk warnings,

execution results examples and so on.

Clean up redundant files in the 3.x and 5.0 migrations[Create Tool Task](#)**Basic Information**

Tool ID: 8c38555f-4c51-4fa0-a481-5d22296af054

Tool Type: Agent Operations

Applicable Environment: Linux Windows

Online Time: 2025-03-03 15:44:46

Update Time: 2025-03-13 15:14:28

Tool Introduction

Clean up redundant files in the 3.x and 5.0 migrations

Risk Warning

No risk whatsoever

Execution Result Example

execute result	Execution result prompt information
success	-

12.1.3.1.2. Create a tool task

Click or create a tool task in the Tool Details. After the parameter configuration is completed, the task can be executed, and the task execution record can be viewed in the Tool Task.

Create Tool Task-File upload

*Task N... : File upload_20250526161225

Input Pa...:

* File Path:
Please enter File Path
The absolute path of the file to be uploaded

Push Sp...: 100 hosts/min

Executio...: Once Daily Weekly Expression

timeout: 30 Seconds

Execut...: All Hosts

Select Hosts by List
 Select Hosts by Business Group

12.1.3.2. Tool Tasks

The page displays the status, task name, execution scope, and execution time of the created task.

A search bar is provided to filter tasks.

Tool Tasks						
Please Select Filtering Content				Actions		
<input type="checkbox"/>	Stat...	Task Name	Execution Scope	Recent Execution Time	Update Time	Operation
<input type="checkbox"/>	<input checked="" type="checkbox"/>	查询系统中的所有隐藏进程_20...	All Hosts	2025-04-24 09:59:05	2025-04-24 09:59:00	Recent Executi Edit Delete
<input type="checkbox"/>	<input checked="" type="checkbox"/>	获取系统的时间戳与时区_2025...	All Hosts	2025-04-24 09:51:21	2025-04-24 09:51:16	Recent Executi Edit Delete

12.1.3.2.1. Tool task management

Select a task from the list and view the recent execution results in the Actions column.

The recent execution result displays the basic information of the task, including the tool name, push speed, and execution cycle. Details of the most recent execution, including the total number of executions, the number of executions, the number of successes, and the number of failures (you can click "View Details" to view the reason for the failure); The list displays the details of the agent, including the agent ID, host, process pid, process name, and process path.

Recent Execution Results——查询系统中的所有隐藏进程_20250424095205 Partially Failed

Basic Information

Tool Name: 查询系统中的所有隐藏进程

Push Speed: 100 hosts/min

Execution Cycle: Once

Execution Scope: All Hosts

Start Time: 2025-04-24 09:59:00

Retry Time for Failed Hosts: -

End Time: 2025-04-24 10:04:08

Total Time: 5Minutes7Seconds

Details of the most recent execution

Total Executions ① 12	Executed 12	Successes 11	Failures 1	View Details
Please Select Filtering Content <input type="text"/>				
<input type="checkbox"/> Agent ID	Host	Process PID	Process Name	Process Path
<input type="checkbox"/>		-	-	-
<input type="checkbox"/>	1	-	-	-

Method 1: Separate management

Select a task and edit or Uninstall it in the Actions column.

Please Select Filtering Content <input type="text"/>	Disable	Enable	Delete
2 items			
<input type="checkbox"/> Stat...	Task Name	Execution Scope	Recent Execution Time
<input type="checkbox"/>	查询系统中的所有隐藏进程_20...	All Hosts	2025-04-24 09:59:05
<input type="checkbox"/>	获取系统的时间戳与时区_2025...	All Hosts	2025-04-24 09:51:21
2 items			
50 Item/Page			

Method 2: Batch management

After checking the task in the list, perform the Deactivate, Enable, and Uninstall actions.

Please Select Filtering Content <input type="text"/>	Disable	Enable	Delete
2/2 selected			
<input checked="" type="checkbox"/> Stat...	Task Name	Execution Scope	Recent Execution Time
<input checked="" type="checkbox"/>	查询系统中的所有隐藏进程_20...	All Hosts	2025-04-24 09:59:05
<input checked="" type="checkbox"/>	获取系统的时间戳与时区_2025...	All Hosts	2025-04-24 09:51:21

12.1.3.2.2. Execution Record

Displays the start time, execution status, and total number of executed tasks, and allows you

to re-execute the task (only for probes that fail to be executed, and probes that have been

successfully executed will not be executed repeatedly) and view the details of the execution result.

Execution Records

Please Select Filtering Content									
Start Time ▾ End Time ▾ Total Time Task Name Executed... Total Executed Successes Failures Operation									
<input type="checkbox"/>	2025-04-24 09:59:00	2025-04-24 10:04:08	5Minutes7Seconds	查询系统中的...	Partial fail...	12	11	1	Re-execute Details
<input type="checkbox"/>	2025-04-24 09:54:13	2025-04-24 09:54:18	5Seconds	查询系统中的...	Completed	10	10	0	Re-execute Details
<input type="checkbox"/>	2025-04-24 09:52:16	2025-04-24 09:52:22	5Seconds	查询系统中的...	Completed	11	11	0	Re-execute Details
<input type="checkbox"/>	2025-04-24 09:51:16	2025-04-24 09:51:21	5Seconds	获取系统的时...	Completed	14	14	0	Re-execute Details

12.2. Groups Management

12.2.1. Overview

The Object Overview page displays five types of management objects: hosts, containers, Pods, clusters, and images. Clicking on one of these management objects will display the corresponding list data.

- Host: List and display host information, including IP, corresponding business group, tag, responsible person, etc. Click to highlight to view detailed information. You can search for or click on the corresponding business group/tag on the left to view the host information within its range

Overview				
Host Container POD Cluster Image Update Data				
Business Group > <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> Please select filter content <input type="text"/> </div>				
<input type="checkbox"/> All	68	<input type="checkbox"/> Host	Business Group	Tags Owner
<input type="checkbox"/> Default Business Gr...	54	<input type="checkbox"/> 10.106.110.240 DESKTOP-RUV...	Default Business Group	-
<input type="checkbox"/> dxh	6	<input type="checkbox"/> 10.42.2.60 cdplugin-0	dxh	-
> 安全组1	0	<input type="checkbox"/> 10.42.1.99 cdplugin-1	dxh	dxh3 dong小慧-1.99-2
tjtest	0	<input type="checkbox"/> 10.42.0.96 cdplugin-2	dxh	-
梅娜	1	<input type="checkbox"/> 172.16.4.188 k8s-master	dxh3 (dxh/dxh2)	dxh1 dong小慧-匹配182-重复
-一级业务组	0	<input type="checkbox"/> 10.106.144.21 master-144-21	Default Business Group	-
test222	0	<input type="checkbox"/> 192.168.173.150 DESKTOP-ECE6...	Default Business Group	-
tjtest2	0	<input type="checkbox"/> 172.16.4.188 k8s-master	Default Business Group	-
ns_hivesec	0	<input type="checkbox"/> 172.16.4.188 k8s-master	Default Business Group	-
nstest1	0			
nstest2	0			
> 入侵一级业务组	5			

- Container: The list displays container information, including the container name, container status, and image used by the container. You can search for or click the corresponding cluster or namespace on the left to view the container information in the range.
- POD: The list displays the POD information, including the POD name, POD status, corresponding cluster, corresponding namespace, etc. You can search for or click the corresponding cluster/namespace on the left to view the POD information in the range.
- Cluster: The list displays information such as the cluster name, cluster-link ID, node name, and namespace.
- Image: displays the aggregate data of the local image, which can be associated with the node information and image information of the aggregate, or click the highlight to view the image details.

You can also export and update data about hosts, containers, PODs, clusters, and images as needed.

12.2.2. Business Groups

Business groups are a method for grouping and managing hosts hierarchically, allowing up to four levels of business groups.

12.2.2.1. Manage Groups

If you want to create a business group, the operation steps are as follows:

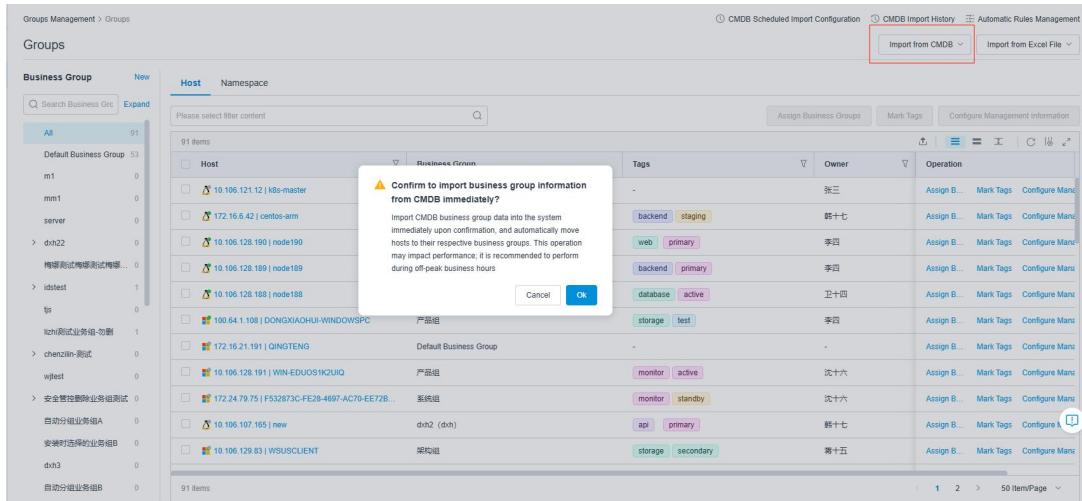
Creation Method 1: Click the "New" button to create a business group, and enter the business group name and description. Note that first-level business groups with the same name cannot be created to prevent duplication.

The dialog box is titled "Create Business Group". It contains two input fields: one for the business group name and another for its description. Both fields have placeholder text and validation icons. At the bottom are "Cancel" and "Confirm" buttons.

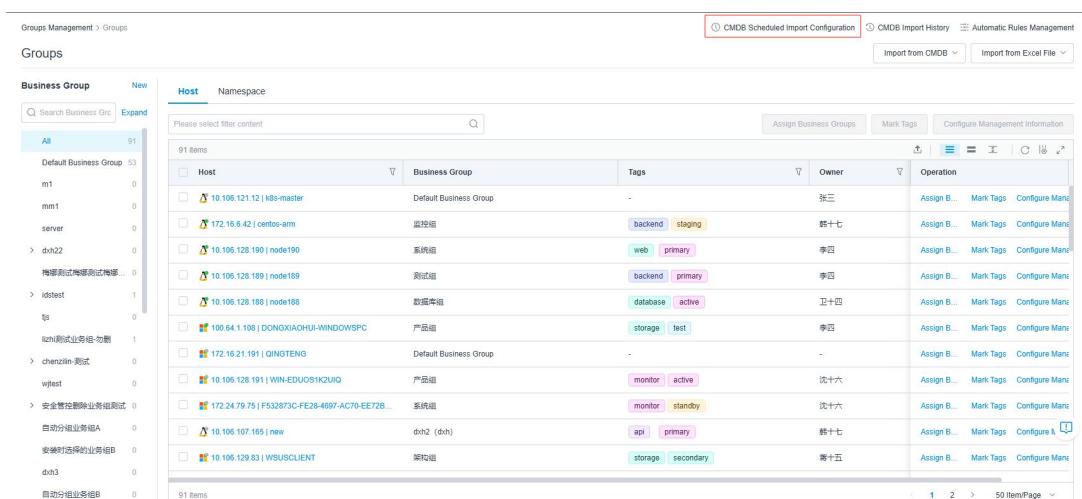
Creation Method 2: Click the "Import from Excel File" button, select a business group, and import directly from an external source. Note that the format of the imported Excel file must comply with the standards.

The dialog box is titled "Import Business Group". It shows a preview of an Excel file with columns for "Operation" and "Assign B...". A red box highlights the "Import from Excel File" button. The background shows a list of business groups and a CMDB interface.

Creation Method 3: First, complete the CMDB connection configuration (a customized function that requires configuring the "Unique Identifier Field", "Asset Field", and "Grouping Field" in the "Synchronization Field Mapping Configuration" under CMDB connection configuration). Click the "Import from CMDB" button, select a business group, and you can immediately import CMDB business group data into the system, which will automatically move the hosts to their respective business groups. CMDB import records can be viewed in the "CMDB Import Records" section at the top right corner of the page.



Creation Method 4: First, complete the CMDB connection configuration (a customized function that requires configuring the "Unique Identifier Field", "Asset Field", and "Grouping Field" in the "Synchronization Field Mapping Configuration" under CMDB connection configuration). Click "CMDB Scheduled Import Configuration" at the top right corner of the page and enable scheduled synchronization. The system will synchronize business group information to this system according to the custom synchronization cycle and automatically move the hosts to their respective business groups. CMDB import records can be viewed in the "CMDB Import Records" section at the top right corner of the page.



- Created business groups can be edited to modify their names.
- To add a sub-business group under an existing business group, click "Add Subgroup."

- You can also delete business groups. Here are the details:
 - If you delete a parent business group, all its subgroups will be deleted as well.
 - Batch deletion: Click "Batch Delete" to select multiple business groups for deletion at once. Note: If the deleted business group has a parent, all hosts under this business group will be transferred to the parent business group; if it has no parent, all hosts under this business group will be transferred to the unassigned business group.
- Please operate with caution.
- The business group sidebar can be resized by dragging to facilitate direct viewing of the full names of business groups.

12.2.2.2. Assign business groups to hosts

If you want to group and tag the hosts, you can assign business groups . At the same time, in order to help you quickly locate the host's position and the corresponding person in charge, the system supports configuring corresponding management information for each host.

Steps:

- Click the "Allocate Business Group" button and make a selection from the created business groups.
- Click the "Configuration Management Information" button and fill in the person in charge, the person in charge's email and the location of the computer room in the pop-up box.
- You can also perform operations such as batch export, batch allocation of business groups, and batch configuration of management information.

The screenshot shows the 'Groups Management > Groups' page. On the left, there's a sidebar with 'Overview', 'Groups', 'Tags', and 'IP Display Manager'. The main area has tabs for 'Business Group' (selected), 'Host' (highlighted in blue), and 'Namespace'. A search bar says 'Please select filter content'. Below is a table with columns: Host, Business Group, Tags, Owner, and Operation. The table lists various hosts like '10.240 | DESKTOP-R...', '10 | cdplugin-0', etc., each associated with a business group (e.g., 'Default Business Group', 'dxh', 'dxh3') and tags (e.g., 'dxh1', 'dxh3'). Buttons for 'Assign Business Groups', 'Mark Tags', and 'Configure Management Information' are at the top of the table. At the bottom, there are navigation buttons (1, 2, 3, 4, 50 items/page).

12.2.2.3. Import host information

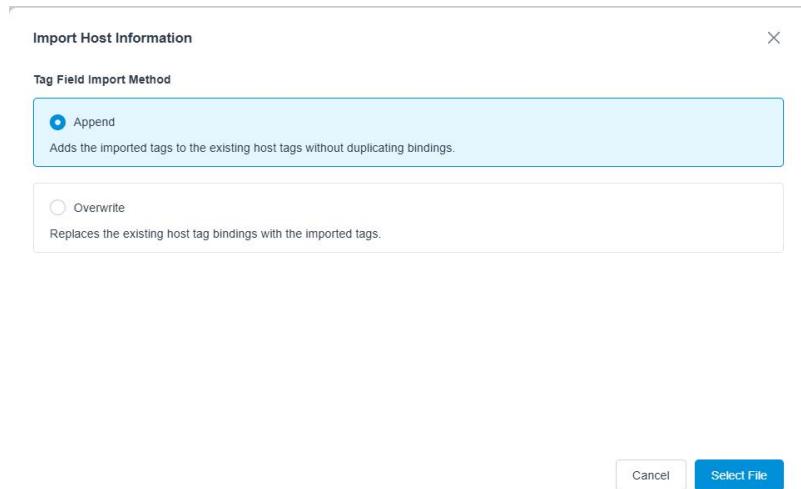
You can also import host-related information using three methods:

Method 1 -Import Data via File: Click the "Import from Excel File" button, select the host information, and import it directly from external sources. Note that you must ensure the imported Excel file complies with the standard format and correctly select the tag field import method.

Tag Field Import Method: Include Append and Overwrite, with Append selected by default.

- **Append:** On the basis of retaining the host's existing tag bindings, add bindings for the tags imported this time without duplicate bindings.
- **Overwrite:** On the basis of deleting the host's existing tag bindings, add bindings for the tags imported this time.

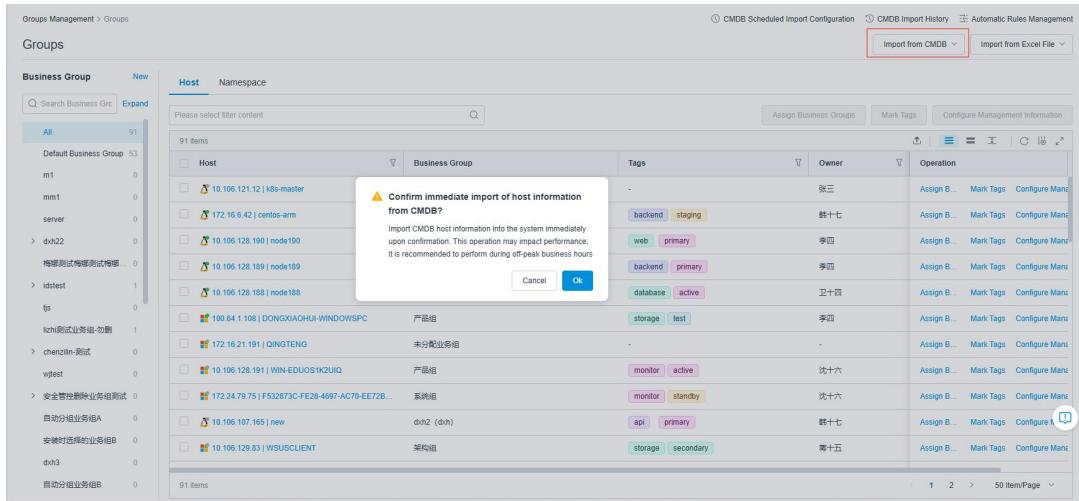
The screenshot shows the 'Import Host Information' dialog box overlaid on the 'Groups Management > Groups' page. The dialog box has a 'Feature Description' section with numbered points explaining the import function. It includes a note about AgentID being a required field in the Excel template. At the bottom are 'Cancel' and 'next step' buttons. The background shows the 'Groups' table with columns: Host, Business Group, Tags, Owner, and Operation. The 'Import from Excel File' button is highlighted in red in the top right corner of the dialog box.



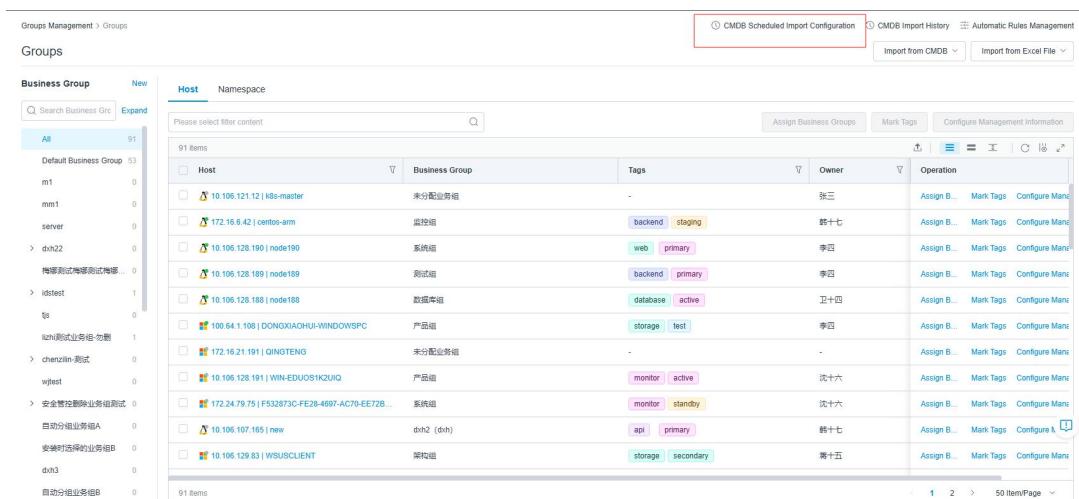
The "Excel File Import" method supports a "rollback" operation. Click the "Excel File Import" button, and you can choose "Rollback".

- Each time host information is imported via an Excel file, the system automatically backs up the original data of the modified information to a corresponding Excel file (file name format: Business Group Management_Excel Import Host Information Backup_Timestamp.xlsx).
- If you need to restore to the original version before the import, you can go to the "Download Center" to obtain the backup file and re-import it.

Method 2 - Manual Import of CMDB Data: First, complete the CMDB connection configuration (a customized function that requires configuring the "Unique Identifier Field" and "Asset Field" in the "Synchronization Field Mapping Configuration" under CMDB connection configuration). Click the "Import from CMDB" button, select the host information, and you can immediately import CMDB host information data into this system. CMDB import records can be viewed in the "CMDB Import Records" section at the top right corner of the page.



Method 3 - Scheduled Automatic Import of CMDB Data: First, complete the CMDB connection configuration (a customized function that requires configuring the "Unique Identifier Field" and "Asset Field" in the "Synchronization Field Mapping Configuration" under CMDB connection configuration). Click "CMDB Scheduled Import Configuration" at the top right corner of the page and enable scheduled synchronization. The system will synchronize host information from CMDB to this system according to the custom synchronization cycle. CMDB import records can be viewed in the "CMDB Import Records" section at the top right corner of the page.



12.2.2.4. Allocate business groups - namespaces

If you want to group and manage namespaces, you can assign business groups.

Assign Method 1: Click the "Assign Business Group" button and select from the created business

groups. You can also select clusters in batches and assign business groups.

The screenshot shows the 'Groups Management > Groups' page. On the left, there's a sidebar with 'Overview', 'Groups' (which is selected and highlighted in blue), 'Tags', and 'IP Display Manager'. The main area has tabs for 'Host' and 'Namespace', with 'Namespace' being active. A search bar says 'Please select filter content'. Below it is a table with three items:

Cluster	Cluster Agent ID	Node	Number of Namespaces
default-8a006d5e25349163	8a006d5e25349163	10.106.110.182 k8s-01	16/16

Under the cluster row, there's a sub-table for 'Namespaces' with columns: Namespace, Business Group, and Operation. One row in this sub-table has a red box around the 'Operation' column, which contains the link 'Assign Business Groups'.

Assign Method 2: If automatic assign rules are created and executed, the newly added namespaces will be automatically grouped according to the matched rules.

The screenshot shows the 'Groups Management > Groups > Auto Grouping Rules' page. On the left, there's a sidebar with 'Asset', 'Intrusion Detection', 'ransomware Protection', 'Risk Discovery', and 'More'. The main area shows a table of '15 items' with columns: Rule Status, Rule Name, Rule Scope, and Rule Content. A 'New Rule' dialog box is open on the right, divided into sections:

- Basic Information:** Contains fields for 'Rule Status' (Enable), 'Rule Name' (Please enter the rule name), and 'Rule descri...: Please enter a rule description'.
- Rule Scope:** Set to 'All Namespaces' (selected).
- Rule Content:** Contains conditions like 'If [Namespace] Equals All Clusters' and 'Then Perform Operation'.

Introduction to Automatic Grouping rules:

- Preset rules: Enabled by default, effective for newly added namespaces.
 - If other namespaces in the cluster belong to the same business group, the newly added namespace will be automatically added to that group.
 - If the Cluster namespace belongs to different business groups, join the business group specified during the installation of the Cluster Agent.

- If the specified business group does not exist, it will be classified as "ungrouped".
- Custom Rules: Custom rules can be created to move namespaces that meet specified conditions to a designated business group or a business group with the same name as the namespace.
 - Supported operations include adding, editing, deleting, enabling, and disabling rules.
 - Manual execution of rules is supported to move existing namespaces to the target business group.
- Rule priority:
 - - The rules are executed in the order of the list from top to bottom, with the rule at the top being executed first.
 - The priority of rules can be adjusted by moving them up or down.
 - If there is a conflict in the condition range of the rules, only the rule that hits the first one will be executed.

12.2.3. Tags

Tags are a method for marking managed objects to facilitate management and screening.

12.2.3.1. Create tags

Creation Method 1: Click the "New" button to create a new tag, enter the relevant basic information, and create tag values.

New Tag

(i) Tag names and tag values only support input of English letters (uppercase and lowercase), numbers, underscores (_), hyphens (-), Chinese characters, and Chinese and English parentheses.

Basic Information

* Tag Na... :

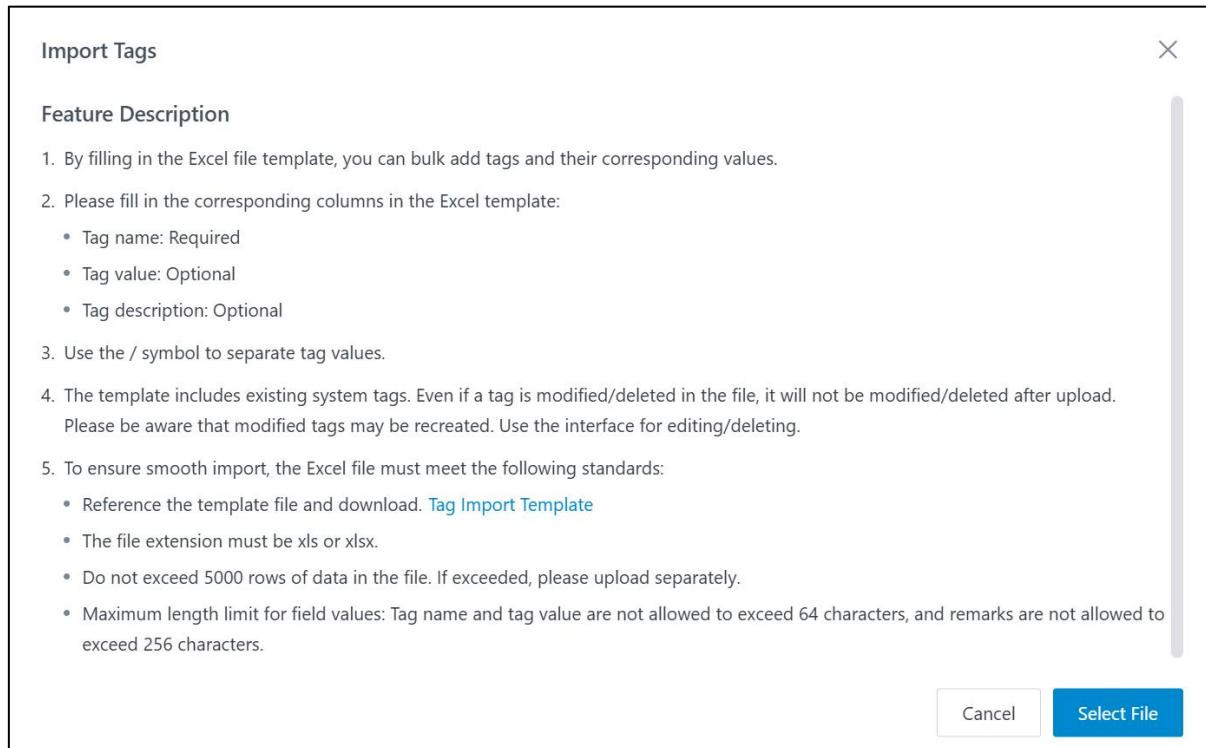
* Tag Color: 

Tag Desc...:

Tag Value *(i)*

+ New Tag Value

Creation Method 2: Click the "Import" button to import directly from an external source.



- For created tags, you can click the "Edit" button to modify tag values or the "Delete" button to delete tags.

12.2.3.2. Assign tags

On the Groups Management -Groups - Host page, click the "Mark Tags" button and select from the created labels. Tags can also be marked in batches

Business Group	New	Host	Namespace	Import
All	68	68 items		
Default Business Group	54	06.110.240 DESK...	Default Business Group	Assign B... Mark Tags Configure Manag...
dxh	6	2.2.60 cdplugin-0	dxh	Assign B... Mark Tags Configure Manag...
安全组1	0	2.1.99 cdplugin-1	dxh	Assign B... Mark Tags Configure Manag...
tjtest	0	2.0.96 cdplugin-2	dxh	Assign B... Mark Tags Configure Manag...
梅娜	1	16.4.188 k8s-master	dxh3 (dxh/dxh2)	Assign B... Mark Tags Configure Manag...
一级业务组	0	06.144.21 master-1...	Default Business Group	Assign B... Mark Tags Configure Manag...
test222	0	168.173.150 DESK...	Default Business Group	Assign B... Mark Tags Configure Manag...
tjtest2	0	16.4.188 k8s-master	Default Business Group	Assign B... Mark Tags Configure Manag...
ns_hivesec	0	16.4.188 k8s-master	Default Business Group	Assign B... Mark Tags Configure Manag...
ns1test1	0	16.4.188 k8s-master	Default Business Group	Assign B... Mark Tags Configure Manag...
nstest2	0	16.4.188 k8s-master	Default Business Group	Assign B... Mark Tags Configure Manag...
入侵一级业务组	5	16.4.188 k8s-master	Default Business Group	Assign B... Mark Tags Configure Manag...
合规基线测试	0	16.4.188 k8s-master	Default Business Group	Assign B... Mark Tags Configure Manag...

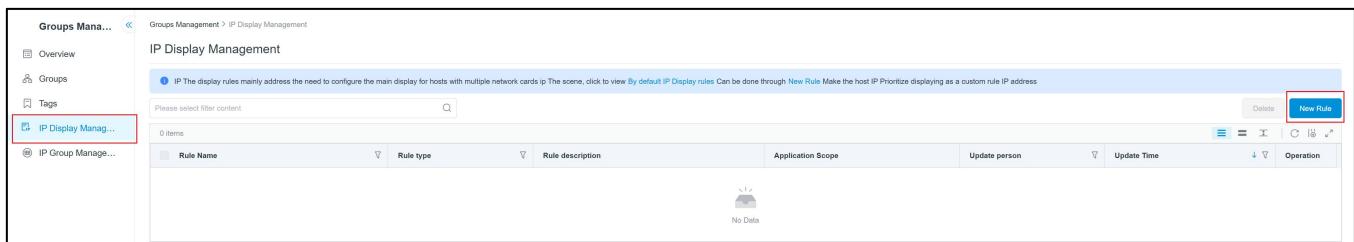
12.2.4. IP Display Management

When a client has multiple network adapters, the system will select an IP address as the primary IP according to the default rules. Other functional pages within the system will use this primary IP to search for and query the corresponding host and related data.

If you wish to manage the primary IP of a host, you can create a new rule to set the primary display IP for hosts within the specified range.

Operation Steps:

- Click the "Add Rule" button and enter the corresponding rule.



- Rule types include Display by IP Range and Display by Network Adapter.
 - Display by IP Range: IP addresses that fall within the input IP range will be prioritized as the primary IP for display.

newly build IP Display rules

* Rule N... : Please enter the rule name

Rule de... : Please enter a rule description

Rule type: IP Display
By setting ip The interval will satisfy ip Within the interval ip As the primary priority ip display

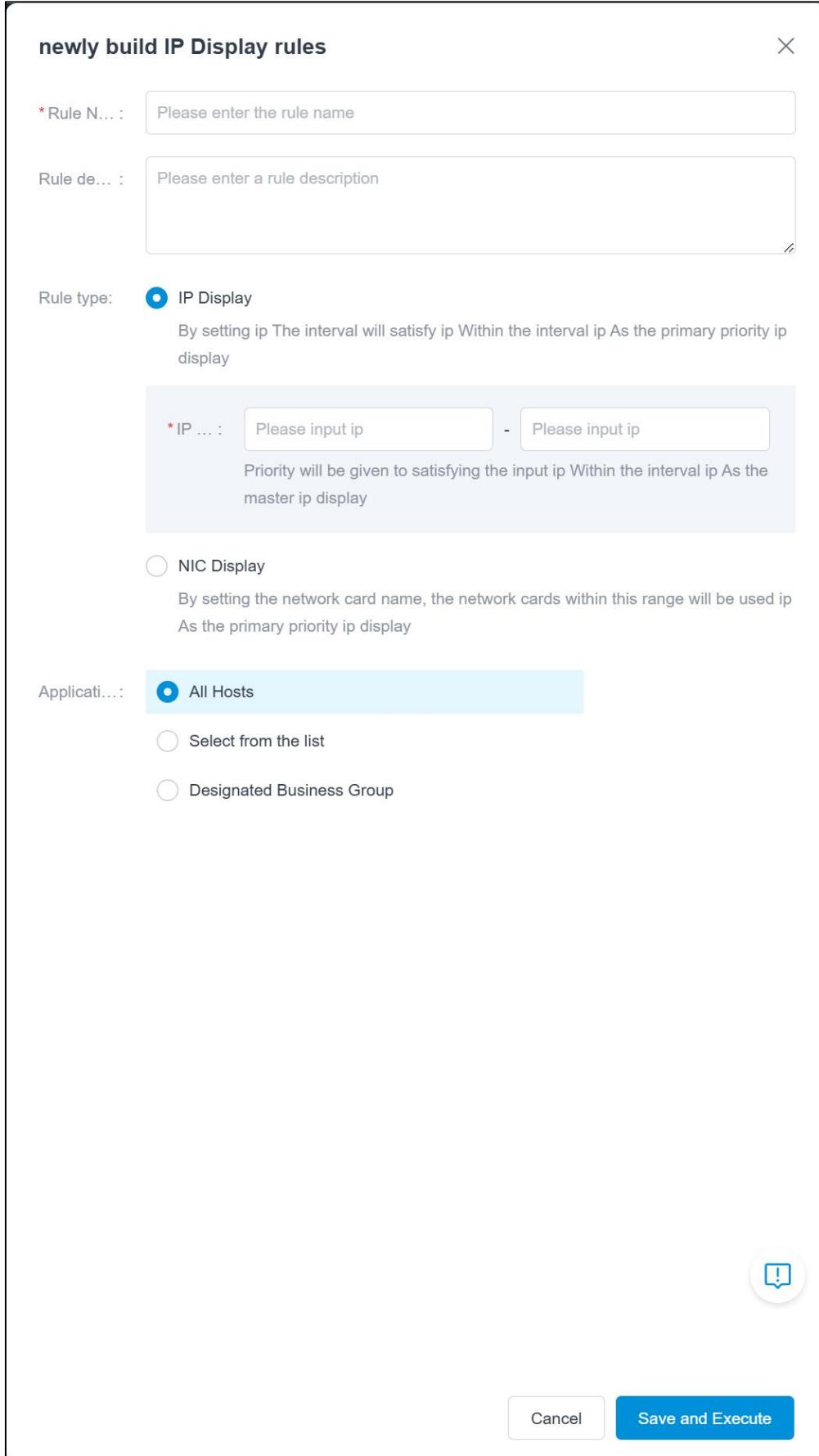
* IP ... : Please input ip - Please input ip
Priority will be given to satisfying the input ip Within the interval ip As the master ip display

NIC Display
By setting the network card name, the network cards within this range will be used ip As the primary priority ip display

Applicati...: All Hosts
 Select from the list
 Designated Business Group

!

Cancel Save and Execute



- Display by Network Adapter: By setting the network adapter name, IP addresses

associated with adapters within this range will be prioritized as the primary IP for display.

▪

Exact Match: Precisely matches the complete network adapter name with strict accuracy.

▪ Fuzzy Match: Uses the input network adapter name as a keyword for similarity-based matching, with lower precision.

newly build IP Display rules

* Rule N... : Please enter the rule name

Rule de... : Please enter a rule description

Rule type: IP Display
By setting ip The interval will satisfy ip Within the interval ip As the primary priority ip display

NIC Display
By setting the network card name, the network cards within this range will be used ip As the primary priority ip display

Matching m... : Strict matching
Strictly match accurately based on the complete network card name

Fuzzy matching
Using the input network card name as a keyword for similarity matching has low accuracy

* Match netw... : Please enter the network card name, supports multiple inputs, separated by commas in English

Those that match the above network card names ip Priority display as host ip Support entering multiple network card names separated by commas in English

Applicati...: All Hosts

Select from the list

Designated Business Group



Cancel **Save and Execute**

- Application Scope: Select the range of hosts to which the rule will apply. After clicking

"Save and Execute," the IP addresses of all hosts meeting the rule criteria will be updated.

12.2.5. IP Group Management

IP Group Management helps users define and manage internal and external IP address ranges within an enterprise.

In cases such as the misuse of public IP addresses for private purposes or the need to comply with technical requirements for network zoning under regulations like Classified Protection 2.0, you can configure IP address ranges in Internal IP Groups and External IP Groups to accurately identify internal assets (e.g., servers, office terminals) and external addresses, thereby avoiding misjudgments in security policies.

During product usage, the system prioritizes matching based on the ranges set in the Internal IP Group and External IP Group. IP addresses within the Internal IP Group range are identified as internal IPs, while those within the External IP Group range are identified as external IPs. If an IP address does not fall within either the Internal IP Group or the External IP Group, it is identified according to the following default rules:

- IPv4 Internal Network Identification Rules:
 - 10.0.0.0/8 - Class A private address
 - 172.16.0.0/12 - Class B private address
 - 192.168.0.0/16 - Class C private address
 - 169.254.0.0/16 - Link-local address
 - Excluding the loopback address 127.0.0.0/8 and 0.0.0.0
- IPv6 Internal Network Identification Rules:

- fc00::/7 - Unique local address
- fe80::/10 - Link-local address
- fec0::/10 - Site-local address

Operation Steps:

- Click "Internal IP Group" on the left, then click the "Add" button in the upper-right corner of the list.

The screenshot shows the 'IP Group Management' page under 'Groups Management > IP Group Management'. On the left, there's a sidebar with 'IP Group' and two buttons: 'Internal IP Group' (highlighted with a red box) and 'External IP Group'. The main area has a table titled 'IP or IP Range' with columns: IP or IP Range, Update person, Update Time, and Operation (with 'Edit' and 'Delete' buttons). The table contains seven entries, each with a checkbox next to it. At the top right of the table, there's a blue 'Add' button. Below the table, there are pagination controls showing '1' and '50 items/Page'.

IP or IP Range	Update person	Update Time	Operation
8.0.0.0	admin	2025-08-15 10:00:04	Edit Delete
2001:0:2851:b90::64	admin	2025-08-14 18:14:05	Edit Delete
8.8.8.8	admin	2025-08-14 18:39:05	Edit Delete
8.0.0.0-8.255.255.255	admin	2025-08-14 18:39:05	Edit Delete
8.0.0.0/8	admin	2025-08-14 18:39:05	Edit Delete
8.8.8.8	admin	2025-08-14 18:39:05	Edit Delete
8.0.0.0-8.255.255.255	admin	2025-08-14 18:39:05	Edit Delete

- Enter internal IP addresses or IP ranges. Supported formats include individual IPs, start-end IP ranges, and CIDR (e.g., 192.168.0.0/16). Separate multiple values by line breaks. After entering the values, click the "Save" button. The system will automatically split the entered IP ranges into multiple data entries.

The screenshot shows the IP Group Management section of the Sentry CWPP interface. On the left, there's a sidebar with navigation links like Asset, Intrusion Detection, Ransom Protection, Risk Discovery, Compliance, Event Collection, Security Control, DevSecOps, and Micro Segmentation. Under Groups Management, it says "IP Group Management". The main area has a header "IP Group" with a note: "Internal IP groups are used to identify public IP as internal IP." Below this is a search bar "Please enter IP group name" and a dropdown menu "Internal IP Group" with a count of 7 items. Another dropdown "External IP Group" shows 6 items. A table lists "IP or IP Range" entries with columns for "Update person" (admin), "Update Time" (e.g., 2025-08-15 10:00:04), and "IP or IP Range" values (e.g., 8.0.0.0, 2001::2851:b90::64). To the right, a modal window titled "Add IP or IP Range" is open, containing a "Format Description" section with instructions and examples, and a text input field with a red border containing the value "01 8.0.0.0\n02 2001::2851:b90::64\n03 8.8.8.8\n04 8.0.0.8-255.255.255\n05 2001:DAA8:0200::20c:29ff:fe4b:baec\n06 2001:DAA8:0200::2001:DAA8:baec:\n07 2001:DAA8:0200::/48\n08\n09\n10". At the bottom of the modal are "Cancel" and "Save" buttons.

- After the configuration is complete, you can view the corresponding identification results in the internal IP and external IP sections of the host details. After the configuration is complete, you can view the corresponding identification results in the internal IP and external IP sections of the host details.

The screenshot shows the "10.106.121.12 Details" page. On the left, there's a sidebar with "Groups Manager" and "Overview" selected. The main area has tabs for "Host", "Container", "POD", "Cluster", and "Image". It shows a tree view of business groups and hosts. A specific host entry "10.106.121.12 | k8s-master" is highlighted with a red box. The right side contains several sections: "Basic Information" (Hostname: k8s-master, Host IP: 10.106.121.12, Host Type: server), "Management Information" (Business Group: -, Tag: -, Remarks: -, Machine Room: -), "Host Assets" (Port: 22, Process: 64), "System Software" (SSH (Secure Shell): 1, OpenSSL: 1), "Accounts" (System Account: 38, Group: 58, Public Key: 4), "Hardware Assets" (graphics card: 1, motherboard: 1, Disk: 2, Network Interface Card: 5, Memory: 1, CPU: 1), and "Installation Packages" (RPM package: 514). At the top right, there are "Asset Comparison" and "Update Data" buttons.

12.2.6. CMDB Management

CMDB Connection Configuration is used to configure CMDB API and manage access credentials, helping users synchronize CMDB data with this platform. This function is a customized feature. If you have requirements, please contact the staff.

- If a customized API plug-in is installed, information such as API name, description, configuration status, number of environments, synchronization method, synchronization cycle, update time and latest modifier will be displayed on this page.
- Click the edit button in the upper right corner to fill in CMDB connection information. It includes CMDB API configuration, synchronization configuration, synchronization field mapping configuration and more parameters.

The screenshot shows the 'CMDB Management' section of the 'Groups Management' interface. It displays two environment configurations: 'Demo' and 'Demo2'. Each configuration card includes fields for Number, Sync Method, Sync Period, Update Time, and Recently. The 'Demo' card has a red border around its entire content area, while the 'Demo2' card does not. A blue banner at the top provides a note about the feature being a custom one.

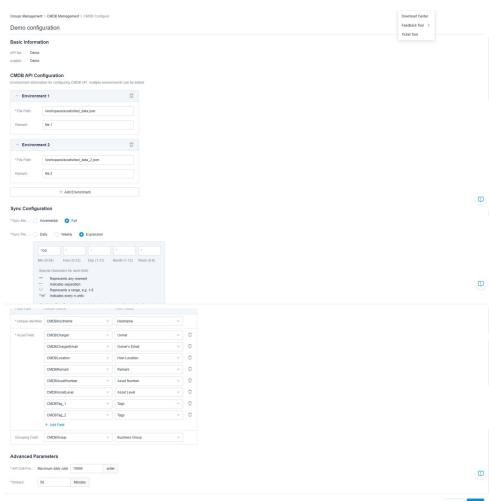
Environment	Number	Sync Method	Sync Period	Update Time	Recently
Demo	2	Full	*00 ****	2025-10-20 17:06:33	admin
Demo2	1	Full	Every day 00:00	2025-10-20 12:07:59	admin

The parameter description is as follows:

- **CMDB API Configuration:** The parameter information here is parsed from customized plug-ins. It is used to configure the environment information of the CMDB API, and multiple sets of environments can be added.
- **Synchronization Configuration:**
 - **Synchronization Method:** Incremental and full synchronization methods are

supported.

- **Synchronization Cycle:** Daily, weekly, and expression-based cycles are supported.
- **Synchronization Field Mapping Configuration:** It is used to configure the fields in the CMDB that need to be synchronized to this system, as well as the mapping relationship with the host fields of this system. The source fields and mapping relationships are parsed and populated from the customized plug-in by default, and manual addition and deletion are supported.
- **Unique Identification Field:** It is the field used to identify the uniqueness of data. You can select either the host IP or the host name, and only one option is allowed.
- **Asset Fields:** The asset fields that support synchronization include owner, owner's email, computer room location, remarks, asset number, asset level, and tags. Among them, tags can be selected and configured for mapping multiple times.
- **Group Field:** It corresponds to the business group field of this system. If you want to import the business group information of the host and move the host to the corresponding business group, this field must be configured.



Synchronized Data is used to display the data synchronized to this product after the CMDB is successfully connected. This data can be used for updating host information, comparing hosts without the Agent installed, verifying the reasons for Agent offline status, and calculating Agent

installation coverage.

- Click the "Synchronize Now" button in the upper right corner of the list to immediately synchronize CMDB data to this system.

This screenshot shows the 'CMDB Management' section under 'Groups Management'. It displays a table of 134 items (hosts) with columns for Host IP, Hostname, Business Group, Owner, Email, Host Location, Tags, and Last Sync Time. Each row includes a small icon and a 'Sync Now' button. At the top, there's a message about sync records and a 'Sync Now' button. The bottom right shows pagination controls.

Click the "Connection Synchronization Records" button in the upper right corner of the page to view connection synchronization records. This function supports downloading synchronization logs and terminating synchronization operations.

This screenshot shows the 'Connect Sync Records' section under 'Groups Management'. It lists 4429 items (sync records) with columns for Start Time, End Time, Duration, Sync Status, Total CMDB Data, Synchronized, Not Synchronized, Failed to Sync, and Operation. Each row includes a 'Download Sync Logs' link and a 'Terminate Sync' button. The bottom right shows pagination controls.

12.3. Report Center

The Report Center provides users with data visualization and analysis capabilities, supporting the statistical analysis of security event data through data components. It helps users quickly build

security data dashboards and manage components and dashboards uniformly.

12.3.1. Widget Management

Data widget, i.e., data visualization chart components, are the smallest units of data visualization that make up dashboards and reports. Widget management is used to manage both pre-configured and custom data components in the system.

12.3.1.1. View Widget

Steps:

- Enter the component management page. The left list displays component groups. Click on a group to view all components under that group.
- Supports searching for components by name.

The screenshot shows the 'Widget Management' page. On the left, there's a sidebar titled 'Widget Library' with a tree view. It has two main categories: 'All' (101 items) and 'Pre-set' (101 items). Under 'All', there are sub-categories: 'Custom' (0), 'My Custom' (0), and 'Pre-set' (101), which further includes '安全左移管理...' (10), '入侵检测与响应...' (40), '风险发现' (25), '资产清点' (13), and '探针管理' (13). To the right of the sidebar is a search bar with the placeholder 'Widget Name' and a magnifying glass icon. Below the search bar are three data cards: 'CI 镜像总览' (Total CI Image Scans: 7200, CI Compliance Rate: 89%), '仓库镜像总览' (Total Repository Image Scans: 2400, Repository Compliance Rate: 89.2%), and '验证通过率' (Validation Pass Rate: 93.2%). In the top right corner, there is a blue button labeled 'New Widget'.

12.3.1.2. Create New Widget

In addition to pre-configured data components, you can create custom data components by configuring the data source, dimensions, metrics, and style.

Notes:

- Creating components requires some understanding of data tables, data analysis, and data

visualization chart creation.

- Dimensions: Refers to the perspective from which data is viewed, such as this month (date dimension), risk level, business group, etc.
 - If the dimension field is of date type, the system supports setting the granularity of the date.

Time granularity	Description
Year-Month-Day	Statistically count data by day, and the display format of the data is: YYYY-MM-DD
Year-Month-Day-Hour-Minute-Second	To calculate data at the finest granularity of year, month, day, hour, minute, and second, the display format of the data is: YYYY-MM-DD HH:MM:SS
Month-Day	Daily statistics data, displayed in the following format: MM-DD
Year-Month	The data is calculated by year and month, and the display format of the data is: YYYY-MM
Year-Quarter	Statistically analyze data by year quarter, and display the data in the format of YYYY for the Nth quarter
Hour	Count data by hour, without distinguishing between year, month, and day

- Metrics: Refers to numerical data with clear business meanings, such as the number of new alerts this month, the number of management objects affected by weak passwords.

- Metrics are generated by selecting a field from the data table and combining it with a calculation method.

Field Type	Calculation Method
Numerical type	Deduce, count, sum, maximum value, minimum value, average value
Non-Numerical type	Deduce, count

Steps:

- Click the "Create New Component" button in the upper right corner of the page.
- Creating a new component involves two steps: setting the data source and configuring the chart.

12.3.1.3. Set Data Source

Steps:

- Select the data table to be analyzed from the left list. Supports searching by table name or group name.
- Preview the data in the selected table on the right.
- Set filter conditions for the data source above the right list.

应用	低危	中危	高危	危急	总计
containerd	0	3	2	0	5
docker	0	0	0	7	7
runc	0	0	3	0	3

12.3.1.4. Chart Configuration

Steps:

- Chart configuration includes three parts:
 - Select the chart type.
 - Configure data.
 - Configure style.
 - Advanced configuration: Includes component description, refresh frequency, and link settings.

(1) Select Chart Type

The screenshot shows the 'New Widget' configuration interface. Step 2, 'Chart Configuration', is active. On the left, a sidebar lists chart types: Summary, Detail Table, Line Chart, Bar Chart, Horizontal..., Pie Chart, Word Cloud, Heatmap, and Timeline. A red box highlights this sidebar. On the right, the 'Data' tab is selected in a configuration panel. This panel contains sections for 'Dimension' (with fields for Dimension and Display Name), 'Index' (with fields for Index, Calculation Method, and Display Name), and 'Sort'. To the right of the configuration panel is a table titled 'Unnamed Components' with two columns: '应用' (Application) and '应用' (Application). The table lists components: runc, docker, and containerd, each with a value of 1. At the bottom right are 'Cancel', 'Export', and 'Save' buttons.

Supported Chart Types:

- **Summary Table:** Displays summarized data grouped by dimensions.

TOP 10 Host High Frequency Patch			
1		CentOS 7 : kernel (CESA-2024: 0346)	507
2		CentOS 7 : linux-firmware (CES A-2024:0753)	505
3		CentOS 7 : kernel (CESA-2023: 5622)	501
4		CentOS 7 : kernel (CESA-2023: 0399)	500
5		CentOS 7 : kernel (CESA-2023: 1091)	500

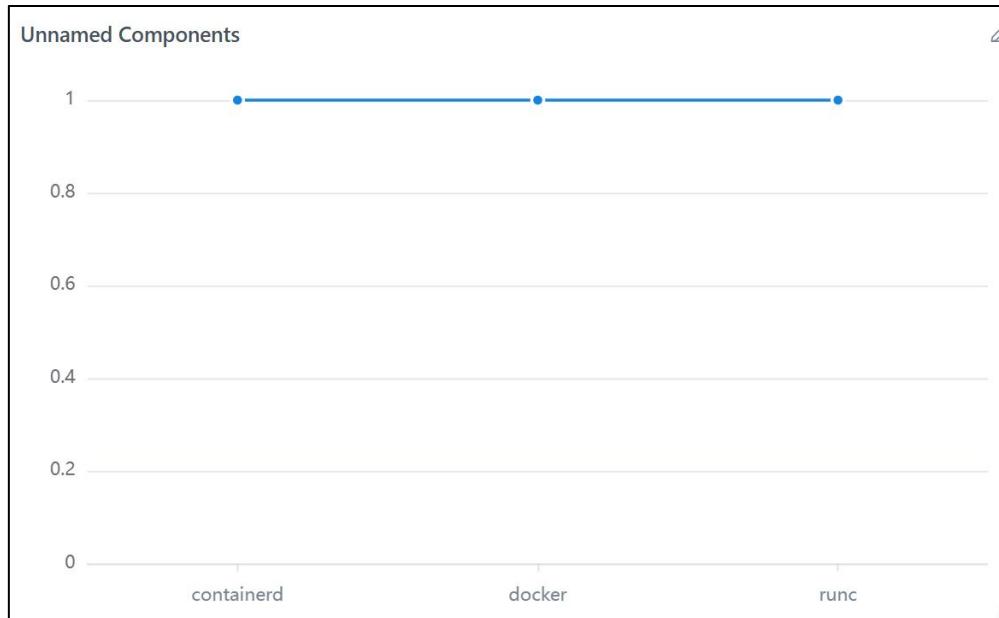
- **Detail Table:** Displays the most detailed data from the data source without grouping.

Unnamed Components	
TaskID	ExecuteRecordID
a8d33308-1c4b-44e6-bc66-26829c5400c3	98f950f1-825f-4d87-a5d5-8d49b9eb49cd

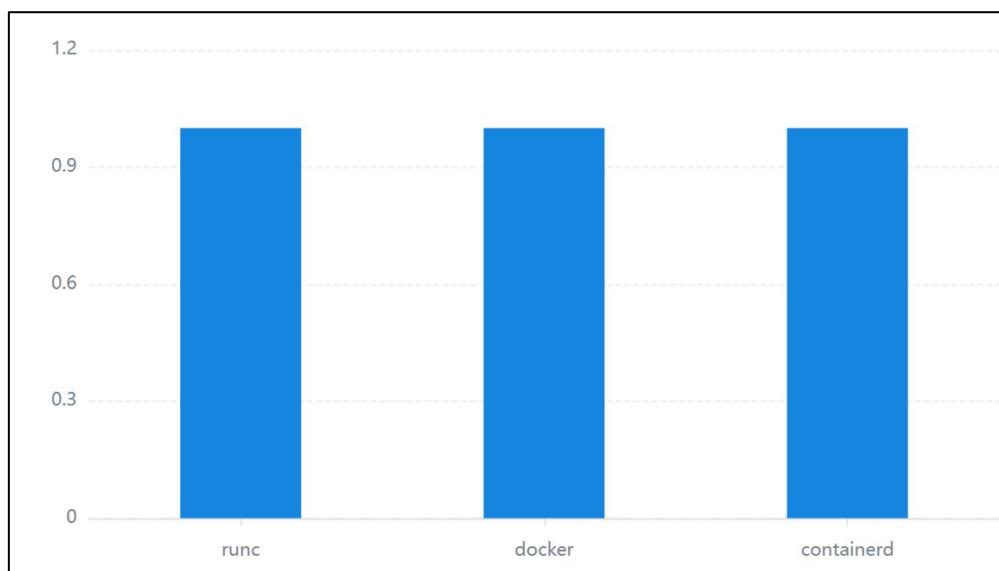
- **Metric Card:** Displays a single core metric, optionally with auxiliary values.



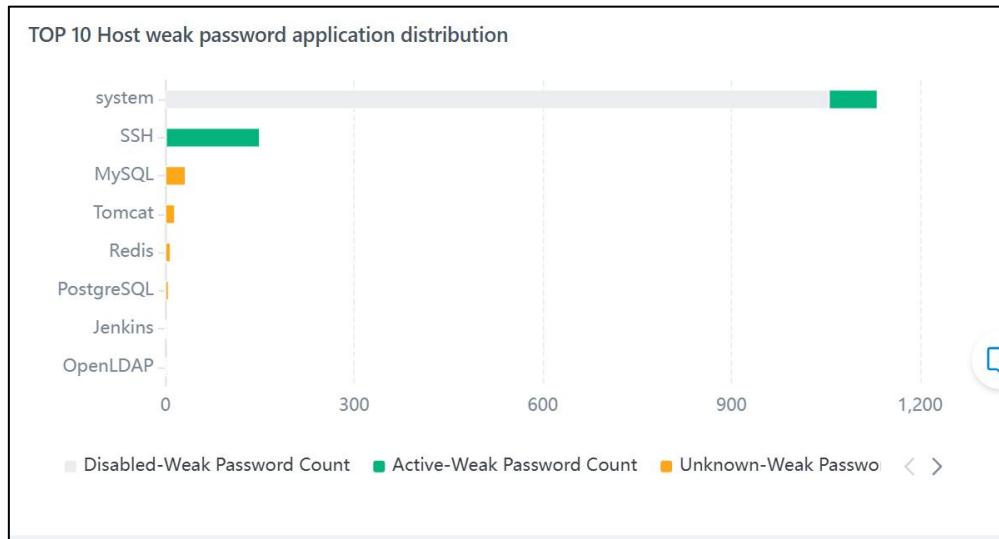
- **Line Chart:** Commonly used for trend analysis, with time on the x-axis and metrics on the y-axis.



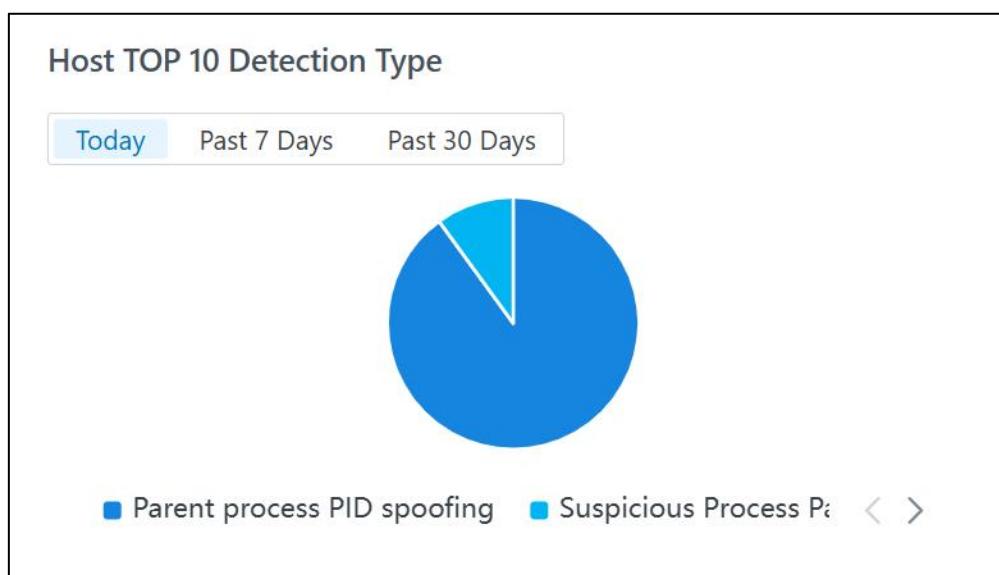
- **Column chart:** The height of the column reflects the number of indicators, commonly used for comparative analysis under different dimensions.



- **Bar Chart:** Uses bar height to represent metric values, often used for comparison across different dimensions.



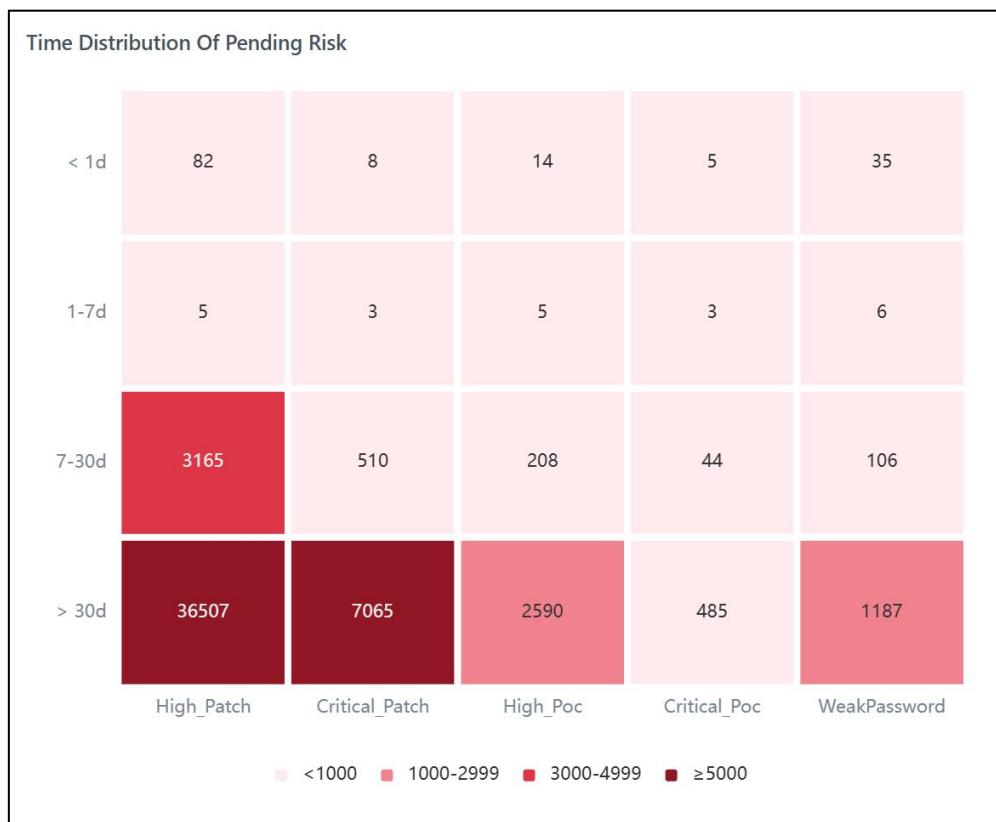
- **Pie Chart/Doughnut Chart:** Uses sectors to represent the proportion of different dimension items.



- **Word Cloud:** Uses font size to represent the frequency or quantity of text, often used to highlight specific text content.

docker
containerd
runc

- **Heatmap:** Uses color intensity to represent data quantity, often used to show data distribution across two dimensions.



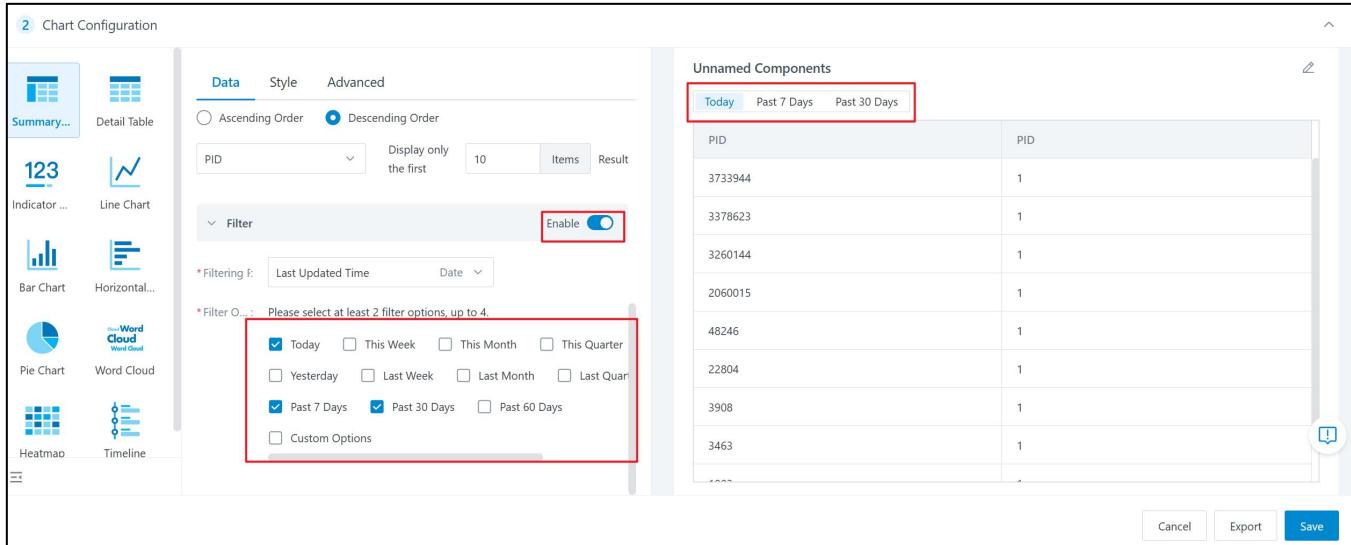
- **Timeline:** Displays data in chronological order, useful for visualizing event processes.

Latest vulnerability information [View more](#)

- 2025-01-21
 - ◆ Oracle WebLogic Server 命令执行漏洞(CVE-2025-21535)
Affected objects:0
- 2025-01-21
 - ◆ Oracle WebLogic Server 拒绝服务漏洞(CVE-2025-21549)
Affected objects:0
- 2024-12-25
 - ◆ Apache MINA 注入漏洞(CVE-2024-52046)
Affected objects:0
- 2024-12-23
 - ◆ Adobe ColdFusion 路径遍历漏洞(CVE-2024-53961)
Affected objects:0
- 2024-12-19
 - ◆ Spring Framework 路径遍历漏洞(CVE-2024-38819)
Affected objects:2 [View details](#)
- 2024-12-17

(2) Data Configuration

- Sorting: Supports sorting based on a dimension field or metric, and can limit the display to the top N items.
 - step: Click to expand sorting, select "forward order" or "reverse order", set the sorting criteria options, and fill in to display only N items
- Filters: Interactive filter conditions on the component, currently only supporting date-type filters.
 - step: Click on the switch on the filter, set it to "on", select the field type of date in the filtering field, configure the filtering items, and the configured date filter will appear in the upper left corner of the right component



- Different types of statistical charts have different parameters for data and style configuration.

Please refer to the table below for details:

N o	Statistical chart types	Data parameter descriptions	Style configuration instructions
1	Summary Table	<ul style="list-style-type: none"> At least one dimension must be set, and the display name of the dimension can be modified. If the selected field for the dimension is of date type, the granularity of the date can be set. For example, if the original date data is 2024-10-01 	<ul style="list-style-type: none"> Header Display: Supports enabling or disabling the display of the table header. Gridline Display: Supports enabling or disabling the display of gridlines. Serial Number Display: Supports enabling or disabling the display of serial numbers. Color: Supports setting the theme color effect for the table.

		<p>12:08:08 and the date granularity is set to Year-Month-Day, the data will be aggregated by day, and the date will be displayed as 2024-10-01.</p>	
2	Detail Table	<ul style="list-style-type: none">At least one column must be set.Supports adding multiple columns.Supports setting the display name for each column.	
3	Metric Card	<ul style="list-style-type: none">Statistical Indicator:<ul style="list-style-type: none">Required: Must be filled.Display Format: Supports setting the display style of statistical indicator data, such as retaining two	<ul style="list-style-type: none">Basic<ul style="list-style-type: none">Alignment: Supports setting the alignment of the content within the indicator card.Size Selection: Supports setting the size of the content within the indicator card.Color:<ul style="list-style-type: none">Statistical Indicator: Supports

		<p>decimal places or rounding to the nearest integer.</p> <ul style="list-style-type: none">• Auxiliary Value:◦ Optional: Not required.◦ Add Filter Conditions: Supports setting filter conditions for auxiliary values.◦ Display Format: Supports setting the display style of auxiliary value data, such as retaining two decimal places or rounding to the nearest integer.◦ Auxiliary Value Percentage:	<p>setting the color of the statistical indicator data.</p> <ul style="list-style-type: none">◦ Auxiliary Value: Supports setting the color of the auxiliary value data.◦ Auxiliary Value Title: Supports setting the font color of the auxiliary value title.◦ Auxiliary Value Percentage: Supports setting the color of the auxiliary value percentage data.• Icons:◦ Icon Color: Supports setting the color of the icon.◦ Icon: Supports setting the icon within the indicator card.
--	--	---	--

		<p>Calculation formula</p> $= (\text{Auxiliary Value} / \text{Statistical Indicator}) * 100\%.$	
4	Line Chart	<ul style="list-style-type: none"> • Must set one dimension, which serves as the X-axis dimension. • Metric Settings: At least one Y-axis metric must be set. • Supports setting a dual-axis chart: You can add metrics to the Y-axis (right axis). • Supports grouping: After selecting a grouping dimension, all added metrics will be split into multiple metrics based on the grouping dimension. • Example: If the metric is "Number of Hosts" and the grouping dimension is set 	<ul style="list-style-type: none"> • Basic Settings <ul style="list-style-type: none"> ○ Data Labels: Supports enabling or disabling data labels on the line chart points. ○ Legend: Supports enabling or disabling the legend. If enabled, the legend's display position can also be set. • Color <ul style="list-style-type: none"> ○ Color Template: Supports selecting a color template to set the line colors. ○ Custom Colors: You can click the "Custom Colors" button to configure the line colors.

		<p>to "Operating System Type," the line chart will display two metrics: "Linux - Number of Hosts" and "Windows - Number of Hosts."</p>	
5	Column Chart	<ul style="list-style-type: none"> • Must set one dimension: 	<ul style="list-style-type: none"> • Basic Settings
6	Bar Chart	<ul style="list-style-type: none"> ○ For Column Charts: This serves as the X-axis dimension. ○ For Bar Charts: This serves as the Y-axis dimension. 	<ul style="list-style-type: none"> ○ Chart Type: <ul style="list-style-type: none"> ▪ Clustered Column Chart: After adding a grouping, different grouping items are displayed on separate columns, distinguished by different colors. ▪ Stacked Column Chart: After adding a grouping, data from different grouping items is displayed on a single column, distinguished by different colors. ○ Data Labels:

		<ul style="list-style-type: none">▪ Supports enabling or disabling the display of metric data on the columns. <ul style="list-style-type: none">○ Legend:<ul style="list-style-type: none">▪ Supports enabling or disabling the legend. If enabled, the legend's display position can also be set.○ Color:<ul style="list-style-type: none">▪ Color Template: Supports selecting a color template to set the column colors.▪ Custom Colors: You can click the "Custom Colors" button to configure the column colors.
7	Pie Chart/Doughnut Chart	<ul style="list-style-type: none">• Must set one sector dimension.• Basic Settings <ul style="list-style-type: none">○ Chart Type:<ul style="list-style-type: none">▪ Pie Chart: Displays data as

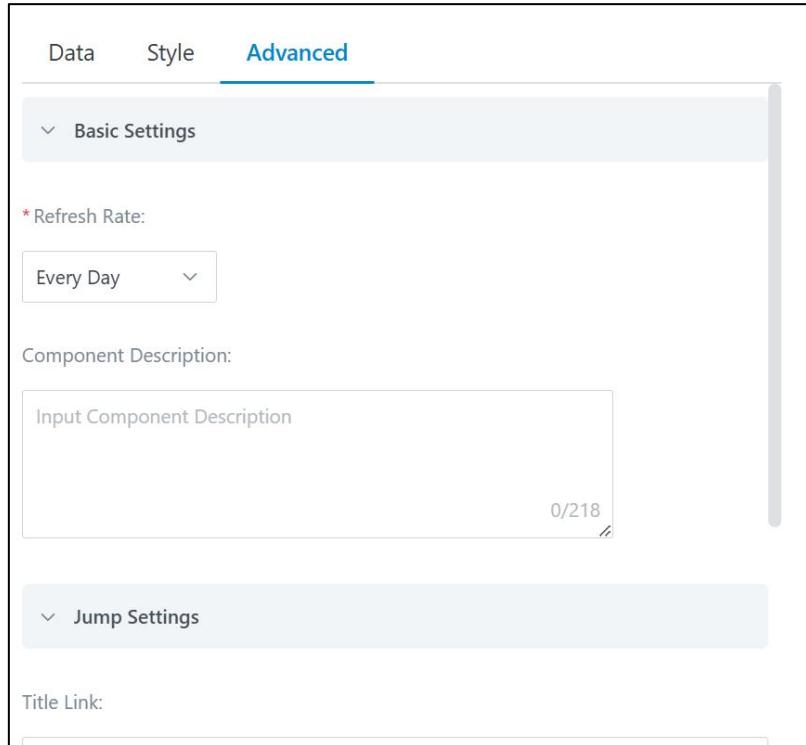
	<ul style="list-style-type: none">• Grouping is not supported.	<ul style="list-style-type: none">a pie chart.
		<ul style="list-style-type: none">▪ Donut Chart: Displays data as a ring-shaped chart.○ Data Labels:<ul style="list-style-type: none">▪ Supports enabling or disabling the display of data labels on the pie/donut chart.○ Legend:<ul style="list-style-type: none">▪ Supports enabling or disabling the legend. If enabled, the legend's display position can also be set.○ Color:<ul style="list-style-type: none">▪ Color Template: Supports selecting a color template to set the colors of the sectors.▪ Custom Colors: You can click the "Custom Colors"

			button to configure the color of each sector individually.
8	Word Cloud	<ul style="list-style-type: none"> Must set one dimension, which serves as the field for the text dimension. Must set at least one metric. <p>Supports setting the word cloud to display only the top N results.</p>	<ul style="list-style-type: none"> Color: Supports setting the color of the text font.
9	Heatmap	<ul style="list-style-type: none"> Dimension Settings: Must set one X-axis dimension and one Y-axis dimension. Metric Settings: Must set at least one metric. Display Names: Supports setting separate display names for dimensions and metrics. 	<p>Basic Settings</p> <ul style="list-style-type: none"> Data Labels: <ul style="list-style-type: none"> Supports enabling or disabling the display of metric data on the heatmap's color blocks. Legend: <ul style="list-style-type: none"> Supports enabling or disabling the legend. If enabled, the legend's display position can also be set. Color: <ul style="list-style-type: none"> Color Template: Supports

		<p>selecting a color template to set the color of the heatmap's blocks. The color of the metric data can be set in segments.</p>
10 Timeline	<ul style="list-style-type: none">• Dimension Settings: Must set one date dimension field.• Data Types for Timeline: Supports two types of data display: Field Display and Grouped Statistics.<ul style="list-style-type: none">◦ Field Display: Similar to a detailed table, displaying detailed data at each point on the timeline.◦ Grouped Statistics: Similar to a summary table, displaying grouped	<ul style="list-style-type: none">• Colors: Supports setting the color of the timeline point icons.

and aggregated
data at each point
on the timeline.

(3) Advanced Configuration



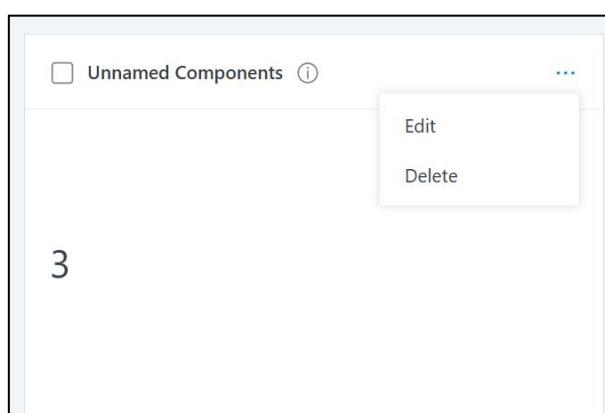
- Refresh Frequency: Options include daily, hourly, and every 15 minutes.
 - Daily: Starting from 00:00:00 every day, refresh component data
 - Hourly: Refresh component data by the entire hour, for example, once at 10:00:00, the next refresh will be at 11:00:00
 - Every 15 minutes: Refresh component data every 15 minutes, for example, once at 10:00:00, and the next refresh will be at 10:15:00
- Component Description: Descriptive information about the component.
- Link Settings: Supports clicking on the component to jump to a corresponding page.

TOP 10 Host High Frequency Patch ⓘ			
①	QT012024000700	CentOS 7 : kernel (CESA-2024: 0346)	507
②	QT012024001234	CentOS 7 : linux-firmware (CESA-2024:0753)	505
③	QT012023007972	CentOS 7 : kernel (CESA-2023: 5622)	501
4	QT012023000487	CentOS 7 : kernel (CESA-2023: 0399)	500
5	QT012023001623	CentOS 7 : kernel (CESA-2023: 1091)	500

12.3.1.5. Edit Widget

Steps:

- Only custom components support editing and deletion.
- Only components with chart types of summary table or detail table support exporting data to CSV.
- In the component management page, click the "..." button and select "Edit" to modify the component configuration.



12.3.2. Dashboard Management

Dashboards are pages that integrate data components, providing visual charts to help users quickly understand the overall security status of protected objects, such as the number of online/offline

agents, risk counts, and new alert details. Through Dashboard, you can :

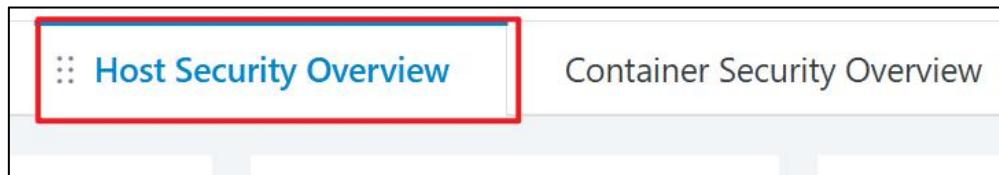
- Conveniently view the security overview of the system
- Quickly build a dashboard that gathers the statistical data you are most concerned about
- Make custom dashboards public and collaborate with other departments

12.3.2.1. Home

The home page displays the system's dashboards.

Steps:

- Hover over the tab to reveal the sort button. You can drag  button to reorder dashboards.



12.3.2.2. Show/Hide Dashboard

For less frequently used dashboards, the system supports hiding them. Hidden dashboards will not be displayed on the home page but can be adjusted in the dashboard management page.

Steps:

- Enter the "Dashboard Management" page and toggle the status switch in the list.

Board Management					
Preset Dashboard		Public Dashboard	Custom Dashboard		
9 items	Please select filter content	<input type="text"/>		<input type="button" value="Import"/>	
Status	Dashboard Name	Version	Update Time	Operation	⋮
<input checked="" type="checkbox"/> Display	Container Security Overview		2025-02-07 15:38:09	Copy	
<input checked="" type="checkbox"/> Display	DevSecOps Overview		2025-02-07 15:38:09	Copy	
<input type="checkbox"/> Hide	Asset Overview		2025-02-07 15:38:09	Copy	
<input type="checkbox"/> Hide	Host Risk Overview		2025-02-07 15:38:09	Copy	

12.3.2.3. View Dashboard

The system supports viewing dashboard content on the home page. Additionally, hidden dashboards can be viewed in the dashboard management page.

Steps:

- Enter the "Dashboard Management" page and click on the dashboard name to preview it.

Board Management						
		Preset Dashboard	Public Dashboard	Custom Dashboard		
9 items		Please select filter content			Import	
Status	Dashboard Name				Version	Update Time
<input checked="" type="checkbox"/> Display	Container Security Overview				2025-02-07 15:38:09	Copy
<input checked="" type="checkbox"/> Display	DevSecOps Overview				2025-02-07 15:38:09	Copy
<input type="checkbox"/> Hide	Asset Overview				2025-02-07 15:38:09	Copy

12.3.2.4. Create New Dashboard

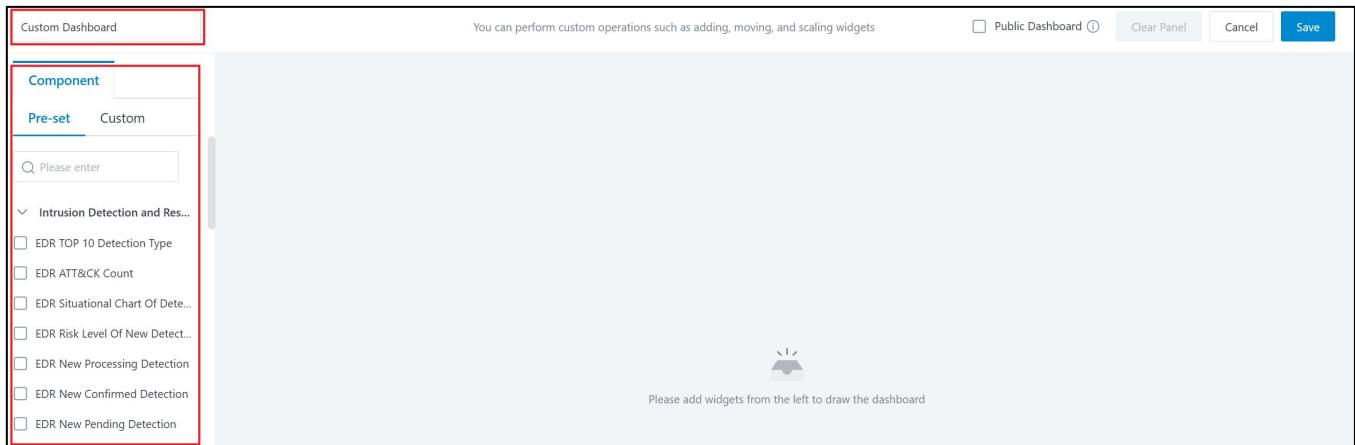
You can create a custom dashboard based on your needs and display it on the home page.

Steps:

- In the custom dashboard page, click the "Create New Dashboard" button in the upper right corner.

Board Management						
		Preset Dashboard	Public Dashboard	Custom Dashboard		
1 items		Please select filter content			New Dashboard	
<input type="checkbox"/>	Status	Dashboard Name	Creator	Creation Time	Last Modified Time	Operation
<input type="checkbox"/>	<input checked="" type="checkbox"/> Hide		admin	2024-12-11 11:35:10	2024-12-11 11:35:10	Copy Edit Delete Export Resources

- Modify the dashboard name in the upper left corner of the page.



- Add data components to the dashboard by selecting from the left component list.
- Custom components you created can also be added to the dashboard.
- Components in the dashboard can be deleted, dragged to adjust order, and resized.

12.3.2.5. Copy Dashboard

When you want to create a dashboard similar to an existing one, you can use the copy dashboard function.

Steps:

- Pre-configured, public, and custom dashboards all support the copy function.
- Click the "Copy Dashboard" button in the dashboard list. The system will create a copy of the dashboard and navigate to the edit page.
- On the edit page, you can modify the dashboard name, adjust components, component order, and component size as needed.

12.3.2.6. Publish Dashboard

Custom dashboards created by users are not visible to others. The system supports sharing your dashboards with other members to enable key metric data sharing and collaborative work.

Steps:

- In the custom dashboard page, click the "Edit" button to enter the edit page.

- Check the "Publish Dashboard" option in the upper right corner to share your dashboard with other accounts under the same tenant.



12.3.3. Report Management

Report Management helps users create and export various types of reports, providing unified management of report templates and report files.

12.3.3.1. Report Templates

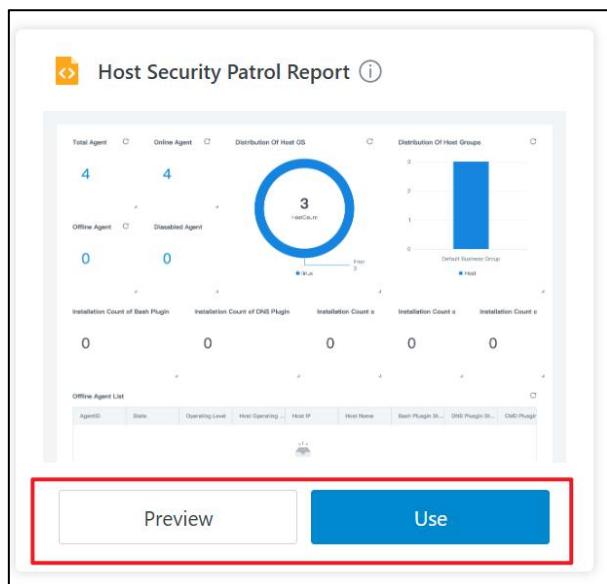
The system supports the management of report templates, including:

- Create Report Template
- Edit Report Template
- Delete Report Template
- Preview Report Template
- Use Report Template



Note:

- Report templates that are already in use by reports cannot be deleted.
- When hovering over a report template card, "Preview" and "Use" buttons will appear. Click "Preview" to open a drawer at the bottom of the page to preview the template content. Click "Use" to open a drawer for creating a new report using the selected template.



12.3.3.1.1. Create Report Template

Steps:

- Click the "New Template" button.

New Report Template

① Basic Information ————— ② Template Settings ————— ③ Completed

Basic Information

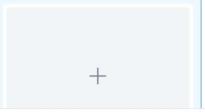
* Template Name : Please enter the template name

Template Description : Please enter template description

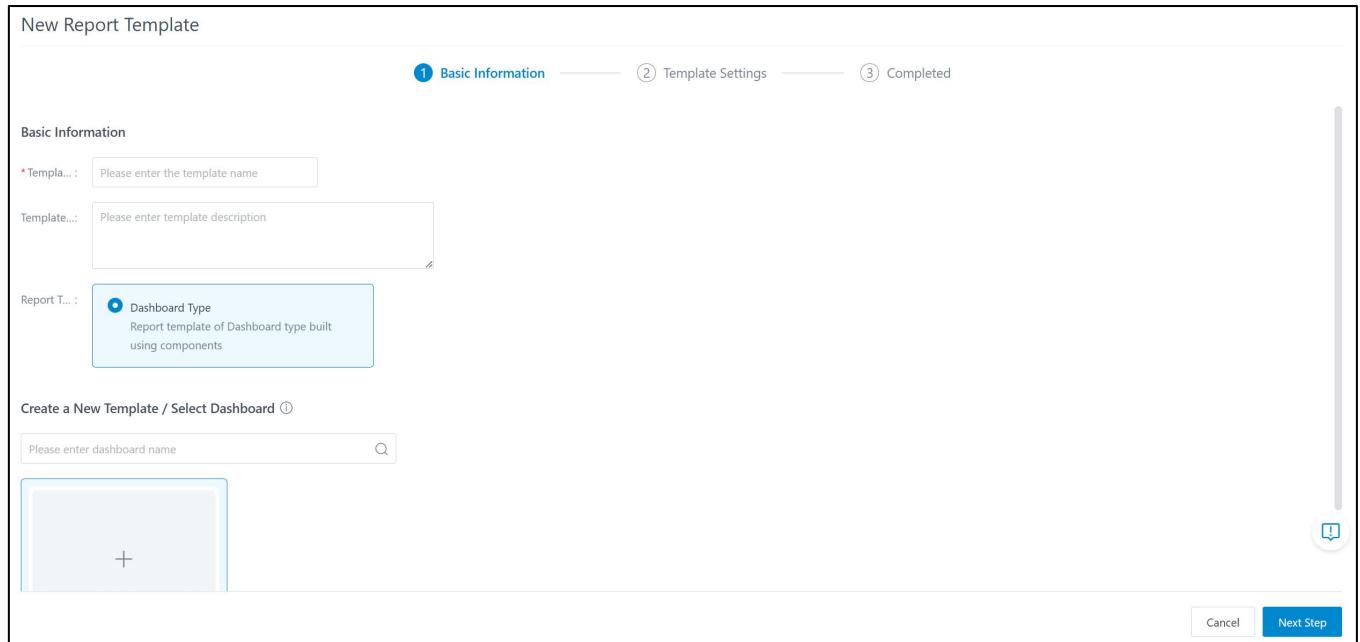
Report Type : Dashboard Type
Report template of Dashboard type built using components

Create a New Template / Select Dashboard ⓘ

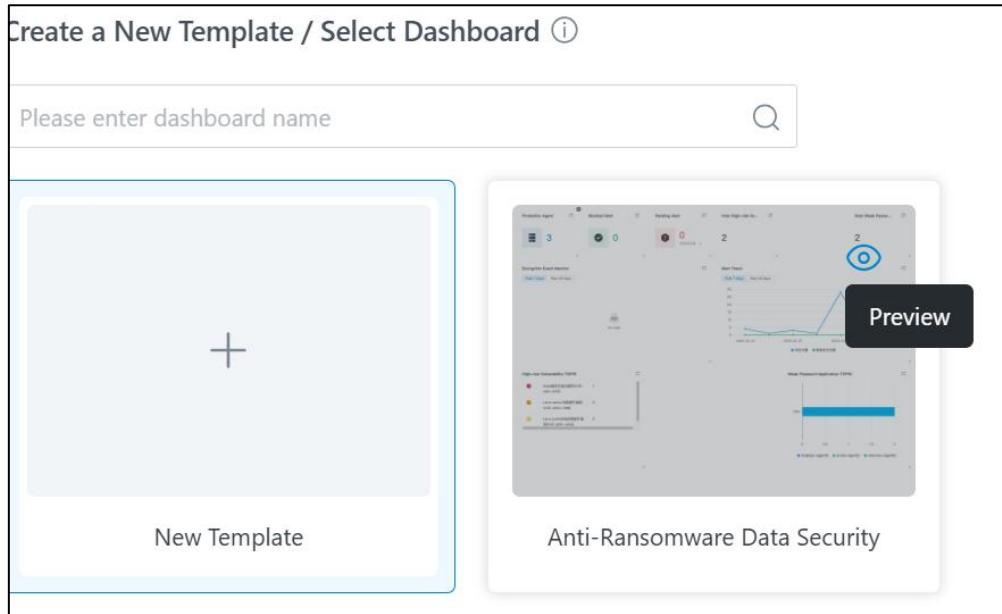
Please enter dashboard name Q

+ 

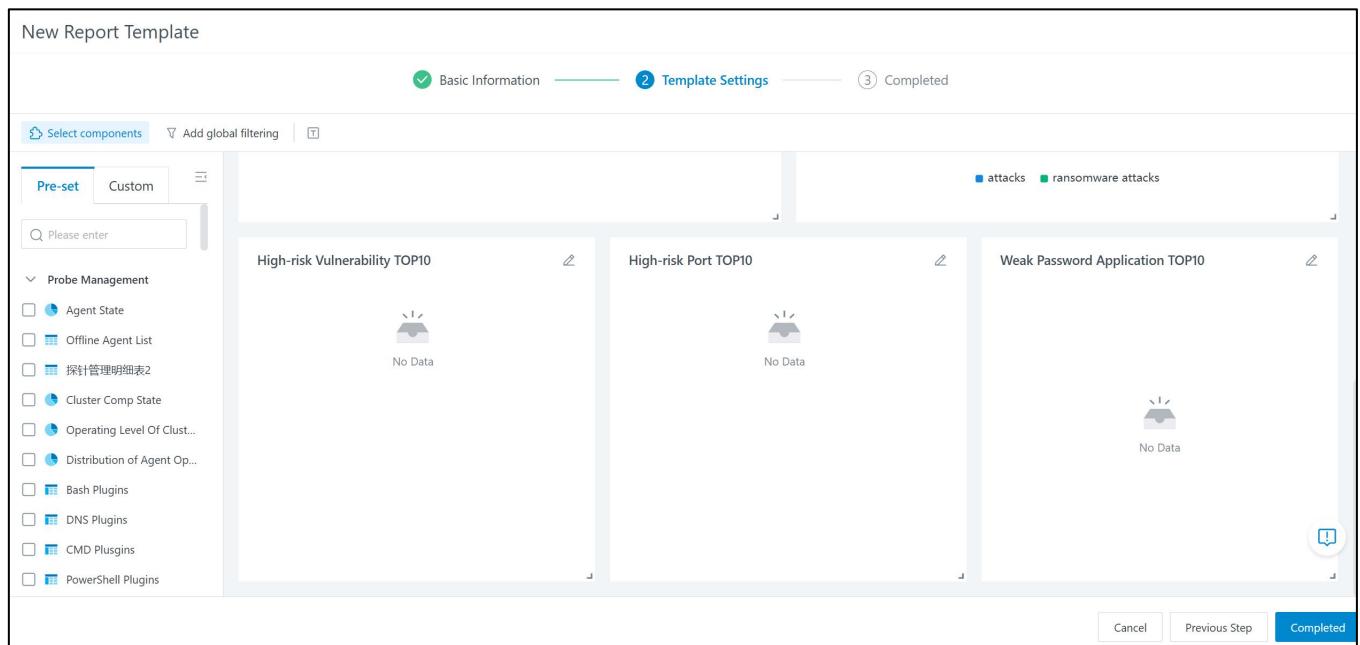
Cancel Next Step



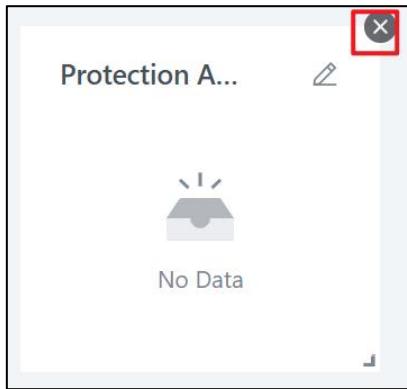
- Creating a report template involves three steps: configuring basic information, configuring the template, and completing the setup.
 - **Basic Information Configuration:** Includes template name, template description, and report type. Currently, only dashboard-type reports (i.e., HTML-type reports) are supported.
 - The system supports selecting an existing dashboard and reusing its components to quickly build a report template.
 - Dashboards can be previewed by hovering over the dashboard card and clicking the "Preview" button, which will redirect to the dashboard preview interface.



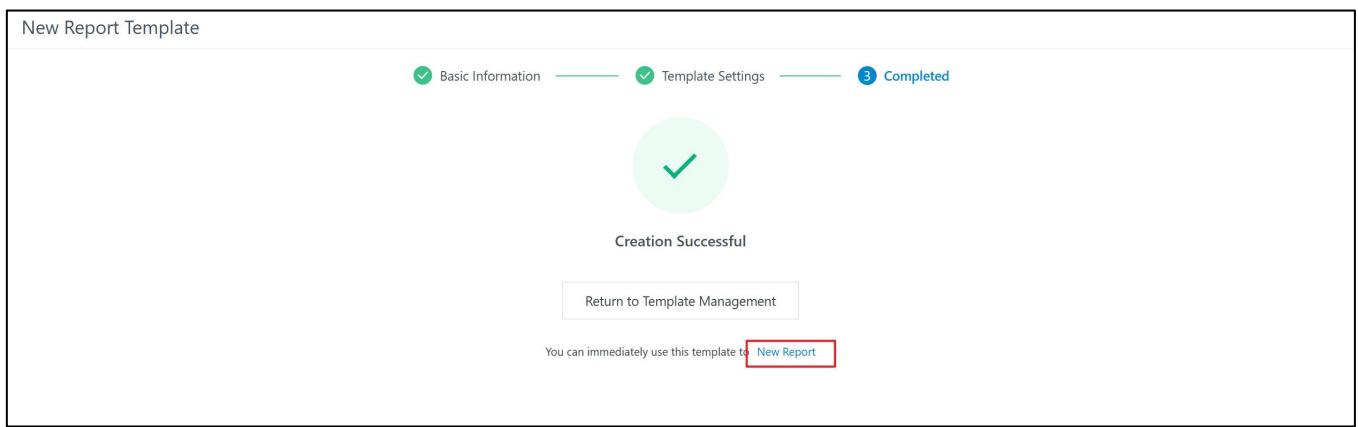
- After completing the basic information configuration, click the "Next" button.



- **Template Configuration:** You can select predefined or custom components from the left-side component list to build the report template.
 - Components in the report template can be added, deleted, moved, and resized.
 - Hover over a component to reveal a delete icon in the top-right corner. Click the icon to remove the component from the template.



- Click the "Complete" button to end configure.



- Once the report template is successfully saved, you can click "Create Report" to use the newly created template to generate a new report.

12.3.3.2. Report List

The Report List is used to manage all created report tasks. Report task management includes:

- Create Report
- Edit Report
- Execute Report
- Delete Report
- Download Latest Report
- View Execution Records

The screenshot shows a 'Report List' interface. At the top, there's a search bar with placeholder text 'Please enter a search term' and a magnifying glass icon. To the right of the search bar are three buttons: 'Delete', 'Execute', and a blue 'New Report' button. Below the search bar is a table header row with columns: 'Report Name', 'Report file format', 'Report Template', 'Creation Time', 'Recent Execution Time', 'Recent Executio...', 'Execution Reco...', and 'Operation'. Underneath the table header, it says '0 items' and 'No Data' with a small icon of a document with a gear.

12.3.3.2.1. Create Report

Steps:

- Click the "New Report" button in the upper right corner of the Report List page.

The screenshot shows the 'Add Report' dialog. On the left, under 'Select Template', there are two sections: 'Preset Template (3)' which lists three templates with icons and names ('Host Security Patrol Report', 'Container Security Patrol...', 'Host Security Patrol Rep...'); and 'Custom Template (0)' which shows 'No Data'. On the right, under 'Report Settings', there are fields for 'Report ...:' (with placeholder 'Please enter the report name'), 'Report D...:', 'Statistica...' (radio buttons for Once, Daily, Weekly, Expression, Daily is selected), 'Start Time' (set to 00:00), and a 'Report push' section with a 'Schedule...' toggle. At the bottom right are 'Cancel' and 'Save' buttons.

- Select Report Template:** Supports selecting predefined or custom templates.
- Statistical Period:** The period for report generation, which can be set to one-time, daily, weekly, or a custom expression. The system will generate report files periodically based on the set period.

12.3.3.2.2. Execute Report

Reports are executed immediately after creation. During execution, editing, deleting, executing, or

downloading the report file is not allowed.

Steps:

- If you need to generate the latest report file immediately, click "Execute".

Report List								
<input type="text" value="Please enter a search term"/> <input type="button" value="Search"/> Delete Execute New Report								
<input type="checkbox"/> Report Name <input type="checkbox"/> Report file format <input type="checkbox"/> Report Template <input type="checkbox"/> Creation Time <input type="checkbox"/> Recent Execution Time <input type="checkbox"/> Recent Executio... <input type="checkbox"/> Execution Reco... <input type="checkbox"/> Operation								
<input type="checkbox"/>	2	Html	Host Security Patrol Re...	2025-02-25 09:40:54	2025-02-25 09:40:54	In Progress	<input type="button" value="Download th..."/> <input type="button" value="Execute"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	
<input type="checkbox"/>	1	Html	Host Security Patrol Re...	2025-02-25 09:40:14	2025-02-25 09:40:33	Successful	<input type="button" value="Download th..."/> <input type="button" value="Execute"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	

- The latest execution status will change to "In progress" and all operations for the report will be disabled.
- Once the report execution is complete, the latest status will change to "Success" or "Failure." Reports with a "Successful" status can be downloaded by clicking "Download the Latest Report."

12.3.3.2.3. View Execution Records

Execution records help customers view and download historically generated reports.

Steps:

- On the Report List page, click "Execution Records."

Report List								
<input type="text" value="Please enter a search term"/> <input type="button" value="Search"/> Delete Execute New Report								
<input type="checkbox"/> Report Name <input type="checkbox"/> Report file format <input type="checkbox"/> Report Template <input type="checkbox"/> Creation Time <input type="checkbox"/> Recent Execution Time <input type="checkbox"/> Recent Executio... <input type="checkbox"/> Execution Reco... <input type="checkbox"/> Operation								
<input type="checkbox"/>	2	Html	Host Security Patrol Re...	2025-02-25 09:40:54	2025-02-25 09:40:54	Successful	<input type="button" value="Download th..."/> <input type="button" value="Execute"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	
<input type="checkbox"/>	1	Html	Host Security Patrol Re...	2025-02-25 09:40:14	2025-02-25 09:40:33	Successful	<input type="button" value="Download th..."/> <input type="button" value="Execute"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	

- Execution records retain only the last 10 entries. Please download reports promptly.

- You can click the "Download Report" button in the execution record to download the report file with a "Success" status to your local device.

Execution Records					
Basic Information					
Report Name:	1	Report Description:	-		
Report file format:	Html	Report Template:	 Host Security Patrol Report		
Statistical Cycle:	Once	Creation Time:	2025-02-25 09:40:14		
Statistical Time:	2025-02-25 09:40:33				
Execution Records					
3 items					
Execution Time	Report File Name	File Size	Execution Time	Execution Status	Operation
2025-02-25 09:40:33	1_20250225094033.html	5.93MB	0秒	Successful	Download Report
2025-02-25 09:40:28	1_20250225094028.html	5.93MB	0秒	Successful	Download Report
2025-02-25 09:40:14	1_20250225094014.html	5.93MB	0秒	Successful	Download Report

- After downloading the report file, click to view it.



The screenshot shows the "Host Security Patrol Report" dashboard. At the top, there's a header with the title and a small blue square icon. Below the header, the "Report Information" section displays the report name (1), creation time (2025-02-25 09:40:14), and creator (admin). At the bottom, there are four tabs: "Total Agent", "Online Agent", "Agent State", and "Distribution of Agent Operating States".

12.3.4. Screen Management

Large screen management assists customers in comprehending the security situation.

12.3.4.1. Pre-installed large screen

The system currently offers two security status dashboards with different styles. You can hover the mouse over a preset dashboard and click the "Full Screen" button to view it in full screen mode. To exit full screen preview, simply press the "Esc" key.

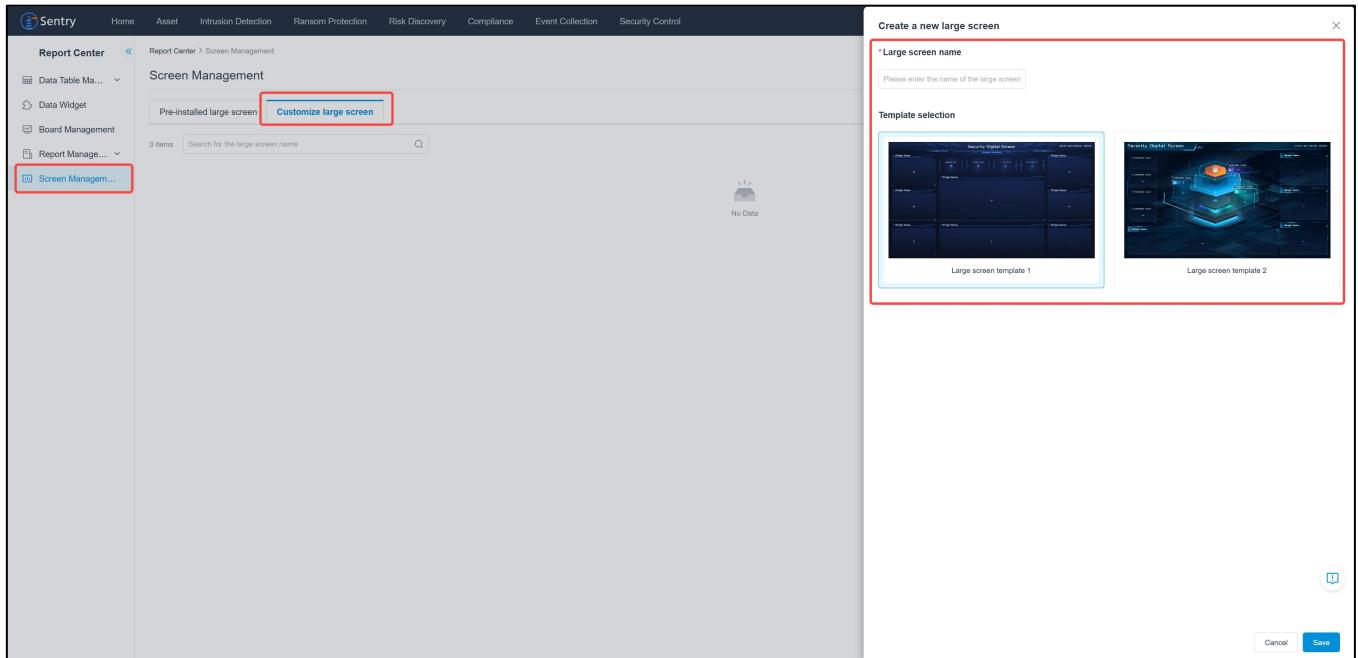


12.3.4.2. Customize large screen

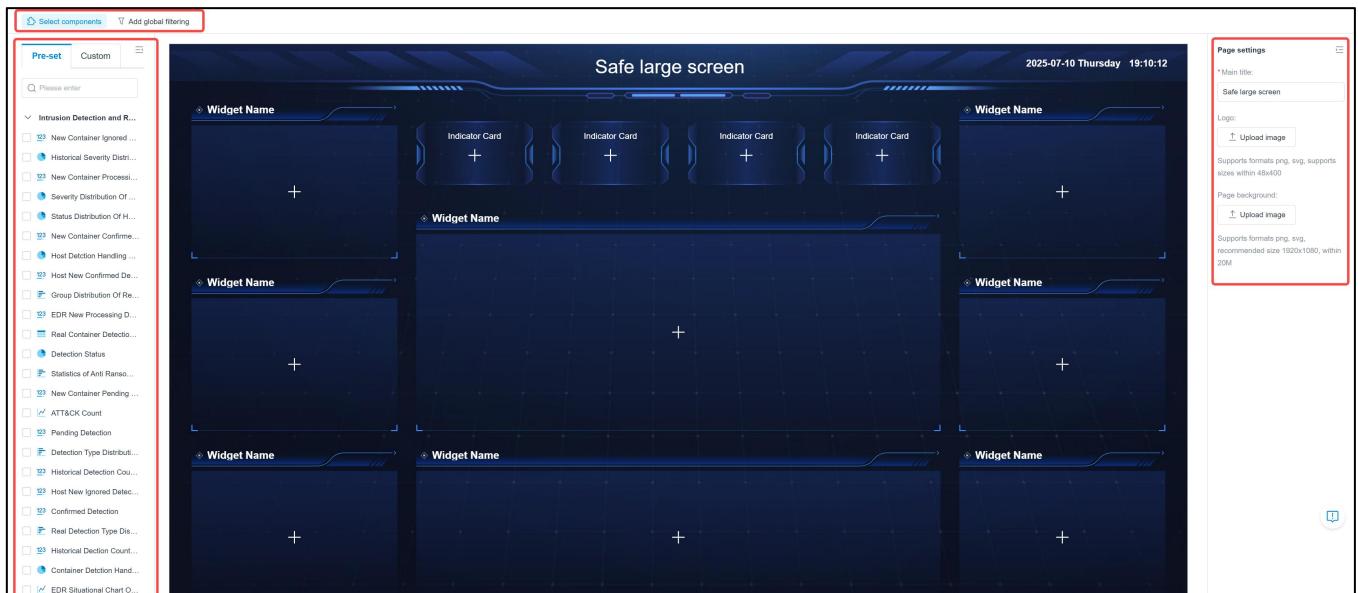
You have the option to customize the dashboard according to your specific business analytics and visualization requirements.

Operation Steps:

- Click the "Custom Dashboard" tab, then click the "New Dashboard" button in the upper-right corner of the page. Enter a dashboard name and select a template provided by the system.



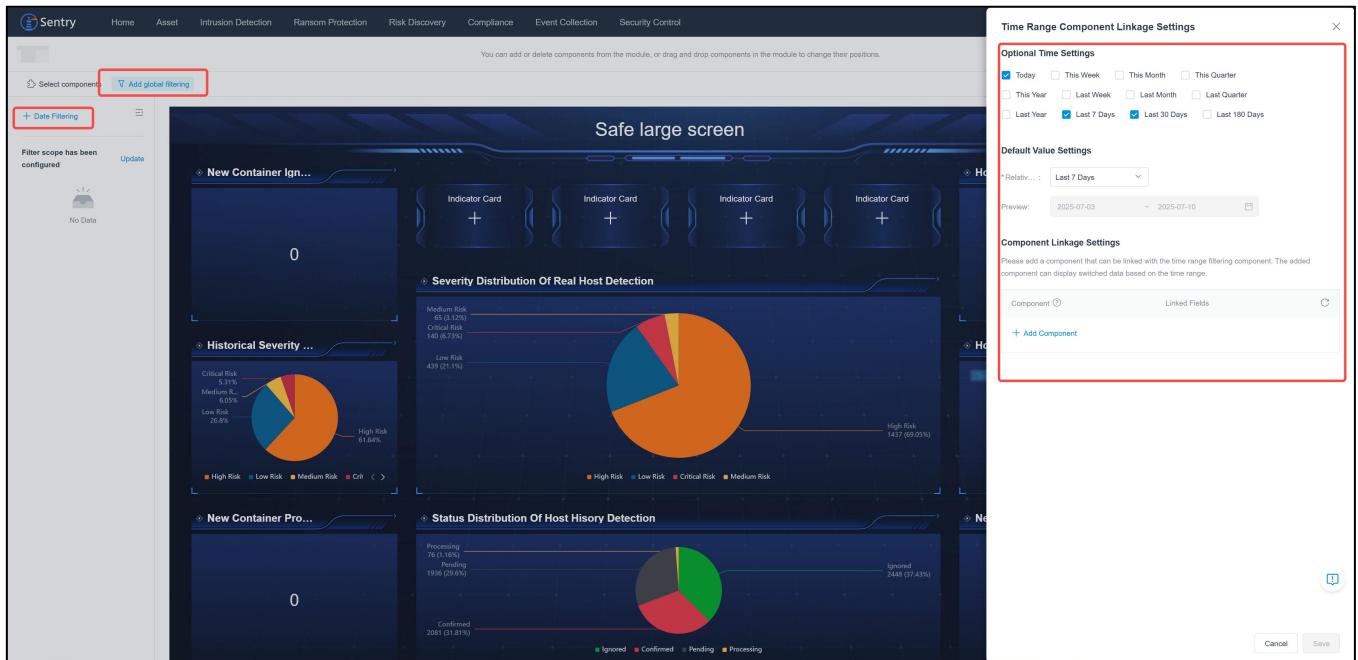
- Upon saving, the system loads the dashboard config page for:
 - Adding data components
 - Setting titles/filters
 - Configuring branding (logo/background)



- Component Selection: Click on any dashboard module to select it, then choose a data component from the left panel to add statistical charts to the module.
- Page Settings: Modify the main title, upload a logo, or set a background image for the

dashboard.

- Add Global Filters: Configure dashboard-wide filter conditions by clicking the "Add Global Filter" button in the top-left corner. This establishes filter relationships across all data components in the dashboard.



- After completing the configuration, click the "Save" button to finish creating the new dashboard.

12.4. Permission Management

A series of management functions performed by accounts with the ability to create, modify, delete, and assign account permissions, which ensure the compliance, security, and validity of accounts in the system. Through account management, system administrators can fully control the lifecycle of user accounts, ensuring legitimate access and efficient utilization of system resources.

12.4.1. Account

An account is a unique identifier used in the system to identify and verify a user's identity, allowing them to access and control system resources and enjoy the services provided by the platform.

steps:

- To add a new account, you can click the "Create New Account" and fill in the relevant information.
- In addition to manually adding accounts, the system also supports importing accounts directly from external sources. You can first review the instructions and then select the file to complete the import.
- Click  to disable an account.
- The system supports batch Enable/Disable and account deletion.

Account								
<input type="text" value="Please enter filter content"/> <input type="button" value=""/>								
133 items								
Enable status	Account name	Role	Access control	Account validity period	Creation Time	Last Login Time	Operation	
<input checked="" type="checkbox"/>	admin	DeployAdmin Administrator	No Limit	permanent	2023-05-12 11:10:05	2024-07-01 14:51:24	Details Account configuration Delete	
<input checked="" type="checkbox"/>	dev_admin	Administrator DeployAdmin	No Limit	permanent	2023-05-16 20:10:27	2024-06-07 11:26:41	Details Account configuration Delete	
<input checked="" type="checkbox"/>	rule_admin	Viewer	No Limit	permanent	2023-08-30 18:37:40	2024-02-02 10:40:53	Details Account configuration Delete	
<input checked="" type="checkbox"/>	guest	Viewer	No Limit	permanent	2023-09-12 14:45:42	2024-06-07 10:04:50	Details Account configuration Delete	

- For the newly added account, you can view details, which include account information and associated data.
 - On the details page, the system supports password reset and editing of basic account information.
 - To better define functions and data permissions, you can assign roles, link user groups, and select data templates to the account.
- You can also click the "Account Configuration" button to quickly complete tasks such as

assigning roles, linking user groups, and selecting data templates.

The screenshot shows the 'admin (account name)' page in the Sentry CWPP interface. It includes sections for 'Account details' (status: Enabled, validity: permanent, creation date: 2023-05-12 11:10:05), 'User info' (User name: [REDACTED], Mobile number: [REDACTED]), and 'Associate Information' (Role tab selected, showing a list of roles including 'Administrator' with a description 'Default Admin Role').

12.4.1.1. General Login Settings

General login settings primarily involve a series of restrictions and regulations on login activities, including login security policies, authentication service configurations, and two-factor authentication. These settings aim to enhance system security, preventing unauthorized access and misuse.

Steps:

- The system supports restrictions on login attempts, account lockout durations, and other related settings. You can click "Login Security Policy" to configure these settings.
- Authentication services include password-based login, generic LDAP servers, Microsoft AD domain servers, Qingteng Single Sign-On, and OpenID servers. You can choose an authentication service as needed. Specifically:
 - Generic LDAP Server: Uses the OpenLDAP framework to verify account legitimacy.
 - Microsoft AD Domain Server: A special LDAP protocol for Windows operating systems, where the service address must be a domain name and anonymous access is not allowed.
 - OpenID Server: Authenticates accounts based on the OpenID Connect protocol.

- For two-factor authentication, you can choose the verification method, such as not using two-factor authentication or using OTP verification.

Login Common Settings

Login Security Policy Authentication Service Configuration Two-Factor Authentication

Login Restrictions

Allowed Attempts: Attempts
Number of allowed attempts to enter the password, configurable from 0-16 times, 0 means no limit, applies immediately

Attempt Reset Du...: Minutes
Duration of account lock due to multiple incorrect password inputs, configurable from 0-6000 minutes, 0 means no lock, applies immediately

Account Lock Dur...: Minutes
Duration of account lock due to multiple incorrect password inputs, configurable from 0-6000 minutes, 0 means no lock, applies immediately

Single Session Lo... : Open Close

Session Duration: Minutes
Single session time limit when idle, configurable from 1-60 minutes

Apply Modification

12.4.2. User Groups

User groups aggregate users, and by assigning roles and data permissions to these groups, functional and data permissions can be allocated to users within the group.

Steps:

- The system supports the creation of new user groups.
- For any user group, you can view detailed information. Specifically:
 - The system supports editing basic information.
 - You can also assign members, roles, and data permissions to the user group.
- The system supports batch deletion of user groups.

User Groups			
2 items		Please enter filter content	
		User Group Name	User Group Description
<input type="checkbox"/>	Administrator	-	Member Account 1
<input type="checkbox"/>	Asset Analyst	-	Member Account 1

2 items < 1 > 50 Item/Page

12.4.3. Roles

Role settings simplify permission management, enhancing system security and maintainability.

System roles include predefined roles and custom roles.

Steps:

- The system provides four predefined roles: Admin, Audit, DeployAdmin, and Viewer.
- The system does not support editing the basic information of predefined roles, deactivating predefined roles, or editing permission policies.
- To view the details of a role, click the "Details" button. On the details page, you can assign members and user groups to the role.
- In addition to predefined roles, you can also create custom roles. Specifically:
 - Custom roles can be activated or deactivated.
 - On the details page, you can edit basic information, assign policies, members, and user groups.
 - The system supports the deletion of custom roles.

Roles										
20 items		Please enter filter content								
Status	Role Name	Description	Associate Permis...	Assign User Count	Assign User Grou...	Creator	Last Update Ti...	Operation		
<input checked="" type="checkbox"/>	Administrator	Default Admin Role	36	2	0	[system]	2021-07-01 08:00:00	Details		
<input checked="" type="checkbox"/>	Asset Analyst	The related functions of asset inquiry and analysis,...	1	0	0	[system]	2021-07-01 08:00:00	Details		
<input checked="" type="checkbox"/>	Asset Manager	Full Permissions of the Asset APP	1	0	0	[system]	2021-07-01 08:00:00	Details		
<input checked="" type="checkbox"/>	Audit	For console auditing, it includes auditing of variou...	2	0	0	[system]	2021-07-01 08:00:00	Details		

12.4.4. Permission Policies

Permission policies describe a collection of permissions for a specific business operation, such as creating a resource or adjusting an attribute, and can be directly assigned to roles.

Steps:

- For user convenience, the system includes predefined commonly used permission policies, eliminating the need for users to configure them again.
- You can view the details of system policies but cannot edit them.
 - The content of predefined policies cannot be modified.
 - You can associate roles with predefined system policies.
- In addition to predefined policies, you can create custom permission policies based on your needs.

Steps:

- Click the "Create Permission Policy" button.
- Fill in the basic information and select interface elements and API.

Create Policy

Basic Information

* Policy N...: Please enter a policy name

* Descript...: Please enter a description

Policy Content

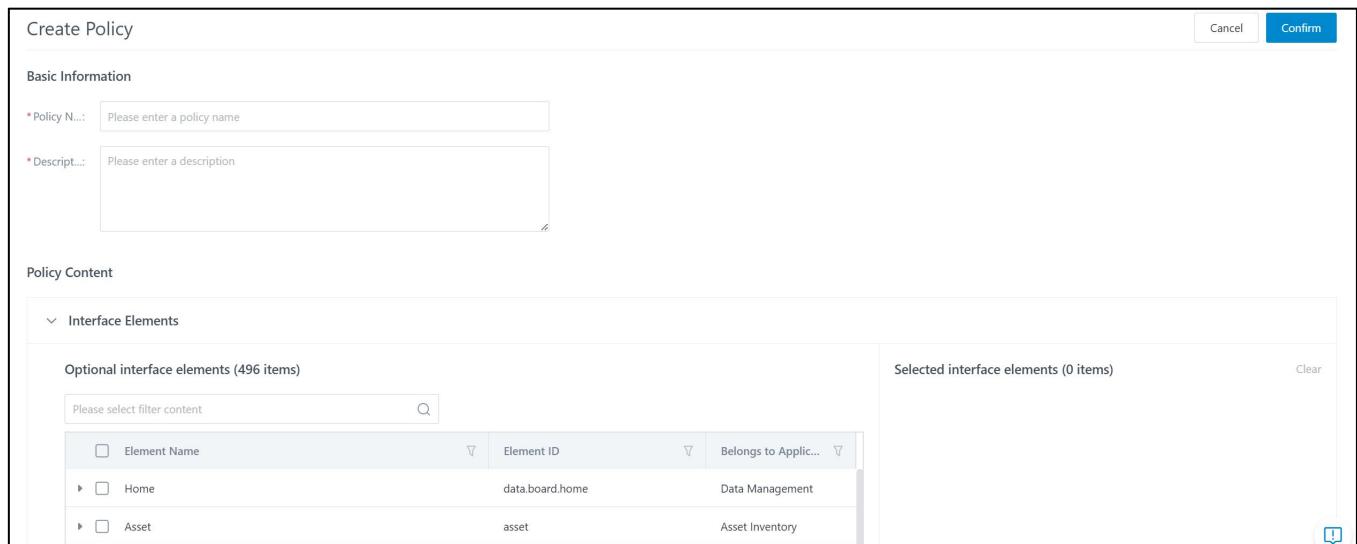
Interface Elements

Optional interface elements (496 items)

Please select filter content	Q				
<input type="checkbox"/> Element Name	V	Element ID	V	Belongs to Appli...	V
▶ <input type="checkbox"/> Home		data.board.home		Data Management	
▶ <input type="checkbox"/> Asset		asset		Asset Inventory	

Selected interface elements (0 items) Clear

Cancel Confirm



12.4.5. Data Templates

Data templates serve as an intermediate layer for data permissions, carrying the corresponding data scope. When assigning data permissions to users or user groups, data templates can be used to delineate data permissions.

Steps:

- The system supports the creation of new data templates. Fill in the basic information and select the data scope.
- For created data templates, you can perform editing and deletion operations.
- The system supports batch deletion.

Data Templates					
<input type="checkbox"/> Please select filter content <input type="button" value="Create Data Template"/>					
Template name	Template description	Last Update Time	Related Objects	Operation	
<input type="checkbox"/> [Redacted]	-	2025-01-04 15:53:57	Business Group (2)	Edit	Delete
1 items				< 1 >	50 Item/Page

12.5. SystemManagement

12.5.1. Deployment Management

The SaaS platform provides users with multiple CWPP product modules. Users can manage the functionality and versions of each module on the platform, including:

- Application installation management
- Application rule updates
- Product authorization management
- Platform system configuration

12.5.1.1. Application Management

Application management allows users to view and manage currently deployed applications, including:

- Application version management
- Application data export

The top of the page displays the currently deployed products, the most recently updated products, and the update time.

The application list shows the summary information of currently deployed applications, including: application name, application type, APP ID, version, and last update time.

12.5.1.1.1. View Application Version Details

Click on the application name to display the application information summary and dependencies.

Application Management					Install Application
Currently deployed product	Recently Updated Applications	Recent Update Time	Number of System Applications	Number of Business Applications	
cloud-native security management platform ...	Association Engine	2025-02-07 14:23:11	2	13	
16 items	Please select filter content	<input type="text"/>			<button>Export All</button>
Application	Type	Version	Recent Update Time		
 Association Engine	Business Application	v2.4.0-20250114.1752	2025-02-07 14:23:11		
 Intrusion Detection and Response	Business Application	v2.6.1-20250123.1813	2025-02-07 14:22:33		

Association Engine

Summary Dependencies

 Association Engine
v2.4.0-20250114.1752

Association Engine

Property Information

First Release Date:	2024-09-04	Application Type:	Business Application
Current Version	2025-01-14	Supported Extension	Extension Types:
Release Date:			

Associated Information

Rules: No Rules Needed

Description:

- The attribute information in the summary includes the application type, APP ID, release date, etc. The APP ID is used to uniquely identify the application.
- Associated information refers to other data information required for the application to run. For details about rules, refer to the rule management section.
- Dependencies refer to the system kernel version required for the application to run.

12.5.1.1.2. Query Applications

Click on the search box to display the search tag "Last Update Time," and select a time range to search for applications updated within the specified time range.

Application Management

Install Application

Currently deployed product	Recently Updated Applications	Recent Update Time	Number of System Applications	Number of Business Applications
cloud-native security management platform ...	Association Engine	2025-02-07 14:23:11	2	13

16 items

App	Recent Update Time	Type	Version	Recent Update Time	Recent Update Time	Recent Update Time

Export All

12.5.1.1.3. Install Applications

Click "Install Application."

The screenshot shows the 'Application Management' section of the Sentry CWPP interface. At the top right, there is a blue button labeled 'Install Application' with a red rectangular border around it. Below this, there are several statistics: 'Currently deployed product' (cloud-native security management platform ...), 'Recently Updated Applications' (Association Engine), 'Recent Update Time' (2025-02-07 14:23:11), 'Number of System Applications' (2), and 'Number of Business Applications' (13). Below these stats is a search bar with placeholder text '16 items' and a search icon. Underneath is a table with columns: Application, Type, Version, and Recent Update Time. The table has a header row and several data rows. At the bottom right of the table area are export options: 'Export All' and icons for CSV, PDF, and XLSX.

12.5.1.1.3.1. Local upload

Download the installer package locally and perform installation through local file upload.

The screenshot shows the 'Installation and Upgrade' wizard. The title bar says 'Installation and Upgrade'. Below it, a sub-header says 'This wizard will assist you in updating each module of your deployment. Please follow the instructions.' The main flow consists of five steps: ① Upload File, ② Check Environment, ③ Confirm Update, ④ Update Application, and ⑤ Completed. Step ① is currently active, indicated by a blue background. Step ⑤ is shown as a preview. The 'Upload File' section contains a sub-header 'Upload File' and a note 'Please upload the upgrade file. The wizard will assist you in the subsequent steps.' It includes a 'System Information' table with four rows: QTcore Version (v3.10.0), Kernel Application (v3.10.0-20250627.1249), System Applications (Quantity: 3), and Business Applications (Quantity: 12). The 'Upgrade files' section has a radio button for 'Local upload' (selected) and an input field for 'Enter file address to upload'. A large blue watermark of a person holding a shield is visible on the right side of the page.

Description:

- Step 1: After the user uploads the file, the system information will automatically update to the corresponding information of the uploaded file.
- Step 2: Environment check refers to detecting whether the system and other application versions can support the normal operation of the currently installed application. If supported, proceed to the next step; if not, the upload cannot be completed.
- The application upgrade package must be in zip or tar format.

12.5.1.1.3.2. Enter file address to upload

Pre-upload the app container image to the registry, then update the application by fetching the updated image from the registry.

The screenshot shows the 'Installation and Upgrade' wizard with the following steps:

- ① Upload File**: Upload and verify the upgrade file.
- ② Check Environment**: Check if the upgrade environment is ready.
- ③ Confirm Update**: Confirm the update items for final preparation.
- ④ Update Application**: Execute updates for each module.
- ⑤ Completed**: Check the update results and complete the wizard.

Upload File

Please upload the upgrade file. The wizard will assist you in the subsequent steps.

System Information

QtCore Version	Version: v3.10.0	Update Time: 2025-06-29 09:15:38
Kernel Application	Version: v3.10.0-20250627.1249	Update Time: 2025-06-29 07:15:19
System Applications	Quantity: 3	Update Time: 2025-06-29 07:26:05
Business Applications	Quantity: 12	Update Time: 2025-06-29 09:15:28

Upgrade files

Local upload Enter file address to upload

Support the installation and update of configured registry or unauthenticated registry

Please enter the link address of the image file in the image repository

Example of image file link: registry.demo.cn/ms-app/com.qt.os.kernel:v3.7.0-20250214.1700

12.5.1.1.4. Agent Package Management

This feature is designed for uploading standalone probe upgrade packages.

Click 'Upload Probe Upgrade Package', select the file, and the upload will complete automatically.

Successfully uploaded Agent versions will be displayed in the list.

The screenshot shows the 'Agent Packages' management interface with the following details:

Agent Packages

Please Select Filtering Content

Upload Probe Upgrade Package

68 items

Probe Type	Probe main program version	System Type	Upgrade ...	Upgrade Package Name	Upgrade Pa...	Download Address
Agent	3.11.0.0-250627.92.x86_64	Windows x86_64	App Upgrade	-	-	https://cloud.qingteng.cn:443/static/agent/os/3.11.0.0-2506...
Agent	3.11.0.0-250627.92.x86_64	Linux x86_64	App Upgrade	-	-	https://cloud.qingteng.cn:443/static/agent/os/3.11.0.0-2506...
Agent	3.11.0.0-250627.92.aarch64	Linux aarch64	App Upgrade	-	-	https://cloud.qingteng.cn:443/static/agent/os/3.11.0.0-2506...
Cluster Agent	3.11.0.0-250627.92.x86_64	Linux x86_64	App Upgrade	-	-	https://cloud.qingteng.cn:443/static/agent/os/3.11.0.0-2506...
Cluster Agent	3.11.0.0-250627.92.aarch64	Linux aarch64	App Upgrade	-	-	https://cloud.qingteng.cn:443/static/agent/os/3.11.0.0-2506...
Agent	3.10.0.1-250619.86.x86_64	Windows x86_64	Package Upload	titan-agent-Release-windows-x86_64-v3.10.0.1-2025-06-1...	38.81MB	https://cloud.qingteng.cn:443/static/agent/os/3.10.0.1-2506...
Agent	3.10.0.0-250522.84.x86_64	Windows x86_64	App Upgrade	-	-	https://cloud.qingteng.cn:443/static/agent/os/3.10.0.0-2505...
Agent	3.10.0.0-250522.84.x86_64	Linux x86_64	App Upgrade	-	-	https://cloud.qingteng.cn:443/static/agent/os/3.10.0.0-2505...
Agent	3.10.0.0-250522.84.aarch64	Linux aarch64	App Upgrade	-	-	https://cloud.qingteng.cn:443/static/agent/os/3.10.0.0-2505...

Note:

Package sources include Package Upload and APP Upgrade modes.

- **Package Upload:** Refers to users manually uploading probe upgrade packages
- **APP Upgrade:** Indicates system-maintained updates

Probe upgrade packages only accept files in .tar, .gz, or .gar.gz formats.

12.5.1.1.4.1. Agent version Distribution

Clicking "Agent Version Distribution" displays the distribution of installed Agent versions across tenants, with statistics including:

- Total Agents
- Online Agents
- Deactivated Agents
- Degraded Agents

Supports filtering and sorting of all list data

Agent Version Distribution								
This function supports viewing the distribution of installed Agents by version for the tenant, and updates the data every 5 minutes.								
Please Select Filtering Content								
Tenant Name	System Type	Running Mode	Agent Version	Total Agent Count	Agent Online Count	Number of Agent Deacti...	Number of Agent Downt...	
███████████	linux-x86_64	Host	3.10.0.0-250522.84.x86_64-06-d8f78d29 ⓘ	1671	1660	0	0	
███████████	windows-x86_64	Host	3.10.0.0-250522.84.x86_64-06-ce1bc9f2 ⓘ	986	703	0	4	
default	linux-x86_64	Host	3.11.0.0-250627.92... ⓘ Default Installation	585	573	0	0	

12.5.1.1.4.2. Default Installation Version Configuration

Default Installation Version refers to the version automatically deployed during Agent installation.

Users may configure global default versions and create tenant-specific custom configurations.

- **Default Configuration:** Applies to all tenants. Click *Edit* to set installation versions for Agents, cluster components
- **Custom Configuration:** Tenant-specific override (takes precedence over default)

- Workflow:
 - Click *New*
 - Select tenant
 - Configure versions
 - Complete setup
- Governance Rules:
 - Only one custom configuration permitted per tenant
 - Deleting a custom configuration reverts the tenant to default settings

Default Installation Version Configuration
This function is used to configure the default installation version of the tenant's Agent.

Default Configuration

Effective Tenants	Default Installation Version	Last Modified Time	Modified By
All Tenants	linux-x86_64 3.11.0.0-250627.92.x86_64-05-b8ea3fe2 linux-arch64 3.11.0.0-250627.92.aarch64-05-e32e8685 windows-x86_64 3.11.0.0-250627.92.x86_64-05-71b85215	2025-06-29 15:15:07	tao.su

Custom Configuration

You can customize the default installation version for an individual tenant, and its priority is higher than the system default configuration.

Please Select Filtering Content		Operation
Effective Tenants	System Type Agent Version	Last Modified Ti... Modified By Operation
███████████	linux-x86_64 3.11.0.0-250627.92.x86_64-05-b8ea3fe2 linux-arch64 3.11.0.0-250627.92.aarch64-05-e32e8685	2025-06-30 01:09:45 test_admin Edit Delete
vulautotest	linux-x86_64 3.11.0.0-250627.92.x86_64-05-b8ea3fe2 linux-arch64 3.11.0.0-250627.92.aarch64-05-e32e8685	2025-07-01 09:26:03 vulautotest Edit Delete

12.5.1.1.4.3. Agent version Management

This functionality manages all Agent versions within the system. Agent version data originates from two sources:

System-Generated Agent Versions: Automatically created when:

- a) Server-side full-package updates occur, OR
- b) Users manually upload packages in *Deployment > Application Management*

Generates a new composite Agent version set (one per system type)

Operational Rules:

1. Multi-tenant Environments:

- Global default installation version remains unchanged (requires manual update)

2. Single-tenant Environments:

- Global default version auto-updates with new Agent releases

3. Version Update Logic:

- Unused versions → Auto-updated to latest
- Previously used versions → New version created

User-Defined Agent Versions: Created/managed in *Deployment > Application Management > Agent Version Management*.

Version Management:

- Create Version Select probe type + system type → Specify main Agent + APP versions
- Edit/Delete Supported for custom versions never deployed
- Clone Version Duplicate existing version for rapid modification
- Version Compare Side-by-side comparison of 2 versions with identical probe/system types

Agent Version Management								
Please Select Filtering Content						<input type="button" value="Delete"/> <input type="button" value="View Comparison"/> <input type="button" value="New Version"/>		
Probe Type	System Type	Probe Version		Version creation ...	Update Time	Operation		
Cluster Agent	Linux x86_64	3.11.0.0-250627.92.x86_64-02-9886b72b	<input type="button" value="up-to-date"/>	Default Installation	2025-06-29 07:25:56	2025-06-29 09:15:35	<input type="button" value="copy"/>	
Cluster Agent	Linux aarch64	3.11.0.0-250627.92.aarch64-02-43c05874	<input type="button" value="up-to-date"/>	Default Installation	2025-06-29 07:25:54	2025-06-29 09:15:35	<input type="button" value="copy"/>	
Agent	Linux aarch64	3.11.0.0-250627.92.aarch64-05-e32e8688	<input type="button" value="up-to-date"/>	Default Installation	2025-06-29 07:25:53	2025-06-29 09:15:35	<input type="button" value="copy"/>	
Agent	Windows x86_64	3.11.0.0-250627.92.x86_64-05-71b85215	<input type="button" value="up-to-date"/>	Default Installation	2025-06-29 07:25:53	2025-06-29 09:15:35	<input type="button" value="copy"/>	
Agent	Linux x86_64	3.11.0.0-250627.92.x86_64-05-b8ea3fe2	<input type="button" value="up-to-date"/>	Default Installation	2025-06-29 07:25:53	2025-06-29 09:15:35	<input type="button" value="copy"/>	
Agent	Windows x86_64	3.10.0.1-250619.86.x86_64-01-fa26020			2025-06-19 13:07:07	2025-06-19 13:07:07	<input type="button" value="copy"/>	
Agent	Linux aarch64	3.10.0.0-250522.84.aarch64-06-2aa694ef			2025-05-26 20:03:21	2025-05-26 20:03:21	<input type="button" value="copy"/>	
Agent	Windows x86_64	3.10.0.0-250522.84.x86_64-06-ce1bc9f2			2025-05-26 20:03:21	2025-05-26 20:03:21	<input type="button" value="copy"/>	

12.5.1.1.5. Installation History

Click "Installation History" to view the records of previously installed application versions.

System Management > Deployment > Application Management

Agent Package Management Installation History

Install Application

Application Management

Currently deployed product: Sentry (v5.1.5.0)

Recently Updated Applications: Compliance Baseline

Recent Update Time: 2025-12-16 17:23:42

Number of System Applications: 6

Number of Business Applications: 14

Please select filter content

21 items

Application	Type	Version	Recent Update Time
Compliance Baseline	Business Application	v1.20.0-20251216.1710	2025-12-16 17:23:42
Vulnerable	Business Application	v1.21.0-20251216.1548	2025-12-16 16:30:30
Intrusion Detection and Response	Business Application	v2.15.0-20251212.1821	2025-12-13 09:27:20
Probe Management	System Application	v3.16.0-20251212.1010	2025-12-12 10:46:18
Asset Inventory	Business Application	v2.22.0-20251209.1459	2025-12-09 15:30:07

Application name, application version, update time, update result, and operator can be viewed in each update record.

Installation History

Please select filter content

80 items

Application Name	Version	Result	Start Time	End Time	Duration	Operator
Compliance Baseline	v1.20.0-20251216.1710	Successful	2025-12-16 17:23:17	2025-12-16 17:23:42	25 seconds	admin
Compliance Baseline	v1.20.0-20251216.1627	Successful	2025-12-16 16:35:42	2025-12-16 16:35:59	17 seconds	admin
Vulnerable	v1.21.0-20251216.1548	Successful	2025-12-16 16:30:05	2025-12-16 16:30:30	25 seconds	admin
Compliance Baseline	v1.20.0-20251216.1525	Successful	2025-12-16 15:42:43	2025-12-16 15:43:05	22 seconds	admin
Compliance Baseline	v1.20.0-20251216.1450	Successful	2025-12-16 15:12:39	2025-12-16 15:13:03	24 seconds	admin
Compliance Baseline	v1.20.0-20251216.1406	Successful	2025-12-16 14:14:50	2025-12-16 14:15:07	17 seconds	admin
Compliance Baseline	v1.20.0-20251216.1149	Successful	2025-12-16 12:33:44	2025-12-16 12:34:07	23 seconds	admin
Vulnerable	v1.21.0-20251213.1108	Successful	2025-12-15 09:49:10	2025-12-15 09:49:38	28 seconds	admin

Select the checkboxes of the items to be exported, then click export to download the installation records in CSV format to the local machine. Each download record can be viewed in the download center.

Installation History

Please select filter content

2/146 selected

Update Items	Result	Start Time	End Time	Duration	Operator
Asset Inventory	Successful	2025-06-29 08:52:50	2025-06-29 09:15:28	22 minutes 38 seconds	[system]
Vulnerable	Successful	2025-06-29 08:19:13	2025-06-29 08:47:04	27 minutes 51 seconds	[system]
Intrusion Detection and Response	Successful	2025-06-29 07:28:51	2025-06-29 08:19:08	50 minutes 17 seconds	[system]
Compliance Baseline	Successful	2025-06-29 07:26:09	2025-06-29 07:28:48	2 minutes 39 seconds	[system]

12.5.1.2. Rule Management

Rules generally refer to the detection criteria corresponding to product functionalities. For example, the rules in antivirus engine management are datasets of virus behavior characteristics detected and extracted by the system, serving as criteria for virus detection.

In rule management, users can comprehensively manage the rules used by each module, including:

- Overview of application rule details
- Application rule update management

The top of the page displays the latest rule import time, the time of rules currently being updated, and the number of existing rule types.

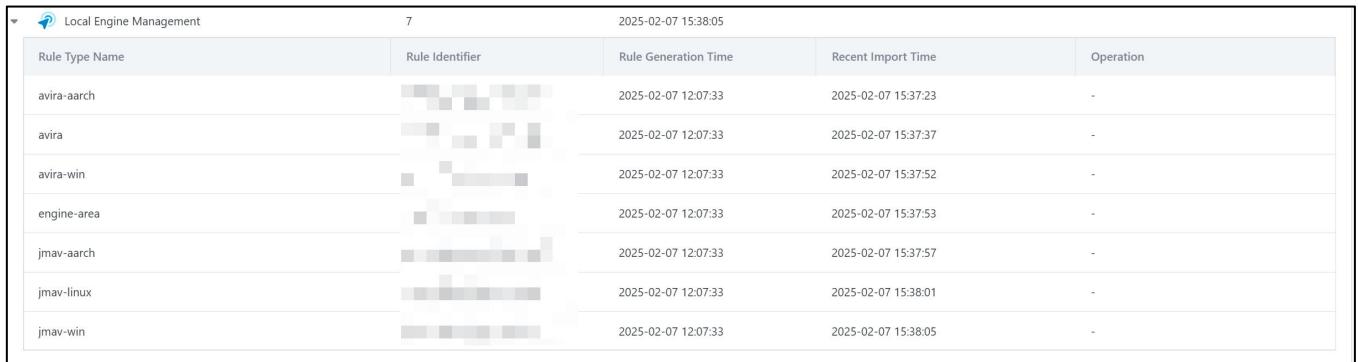
The rule list displays rule information by application module, including the number of rule types and the last import time.

12.5.1.2.1. View Rule Details

The list is displayed by application name (first level) and rule type name (second level). Click the triangle on the left of the item to be viewed to expand the second-level list.

Rule Updates				
Recent Import Time	Recent Online Update Time	Rule Type Count		
2025-02-07 15:55:58	-	121		
10 items	Please select filter content	<input type="text"/>		
Application/Rule Type Name	Rule Type Count	Recent Import Time		
Asset Inventory	1	2025-02-07 15:41:48		
Rule Type Name	Rule Identifier	Rule Generation Time	Recent Import Time	Operation
Asset	qasset	2025-02-07 12:07:33	2025-02-07 15:41:48	-
Local Engine Management	7	2025-02-07 15:38:05		

The second-level list includes the rule type name, rule identifier, rule generation time, and last import time.



A screenshot of a web-based management interface titled "Local Engine Management". At the top, there is a small icon of a globe with a checkmark, followed by the text "Local Engine Management", a number "7", and a timestamp "2025-02-07 15:38:05". Below this is a table with columns: "Rule Type Name", "Rule Identifier", "Rule Generation Time", "Recent Import Time", and "Operation". The table contains seven rows, each representing a different rule type: "avira-aarch", "avira", "avira-win", "engine-area", "jmav-aarch", "jmav-linux", and "jmav-win". Each row includes a small grayscale thumbnail under the "Rule Identifier" column.

Rule Type Name	Rule Identifier	Rule Generation Time	Recent Import Time	Operation
avira-aarch	[REDACTED]	2025-02-07 12:07:33	2025-02-07 15:37:23	-
avira	[REDACTED]	2025-02-07 12:07:33	2025-02-07 15:37:37	-
avira-win	[REDACTED]	2025-02-07 12:07:33	2025-02-07 15:37:52	-
engine-area	[REDACTED]	2025-02-07 12:07:33	2025-02-07 15:37:53	-
jmav-aarch	[REDACTED]	2025-02-07 12:07:33	2025-02-07 15:37:57	-
jmav-linux	[REDACTED]	2025-02-07 12:07:33	2025-02-07 15:38:01	-
jmav-win	[REDACTED]	2025-02-07 12:07:33	2025-02-07 15:38:05	-

12.5.1.2.2. Query Application Rules

Click on the search box to display search tags, and search based on the tags, including:

- Search application rules by application/rule type name **keywords**
- Search application rules imported within a specified time range by last import time



A screenshot of a web-based management interface titled "Rule Updates". At the top, there are buttons for "Online Update" and "Import rule package". Below this is a summary section with three metrics: "Recent Import Time" (2025-02-07 15:55:58), "Recent Online Update Time" (-), and "Rule Type Count" (121). A red box highlights the search bar and the table below it. The table has a header row with columns: "Application/Rule Type Name", "Recent Import Time", and "Recent Online Update Time". Below the header, there is a single data row for "ASSET inventory". The entire table area is also highlighted with a red box.

Rule Updates		
Recent Import Time	Recent Online Update Time	Rule Type Count
2025-02-07 15:55:58	-	121
10 items		
Application/Rule Type Name	Recent Import Time	Recent Online Update Time
ASSET inventory	2025-02-07 15:41:48	

12.5.1.2.3. Update Rules

The detection rules of applications need to be continuously updated to enhance security. Users can set rule updates by manually importing rule packages and setting automatic updates.

12.5.1.2.3.1. Import Rule Packages

Users can manually import local rule packages to update the detection rules of applications.

Click the "Import Rule Package" and complete the import to update the existing rules.

The screenshot shows a user interface for managing rule updates. At the top right, there are two buttons: "Online Update" and "Import rule package". The "Import rule package" button is highlighted with a red rectangle. Below these buttons, there are three status indicators: "Recent Import Time" (2025-02-07 15:55:58), "Recent Online Update Time" (blank), and "Rule Type Count" (121). At the bottom left, there are buttons for "10 items", "Please select filter content", and a search icon. On the far right, there is an "Export All" button.

Description:

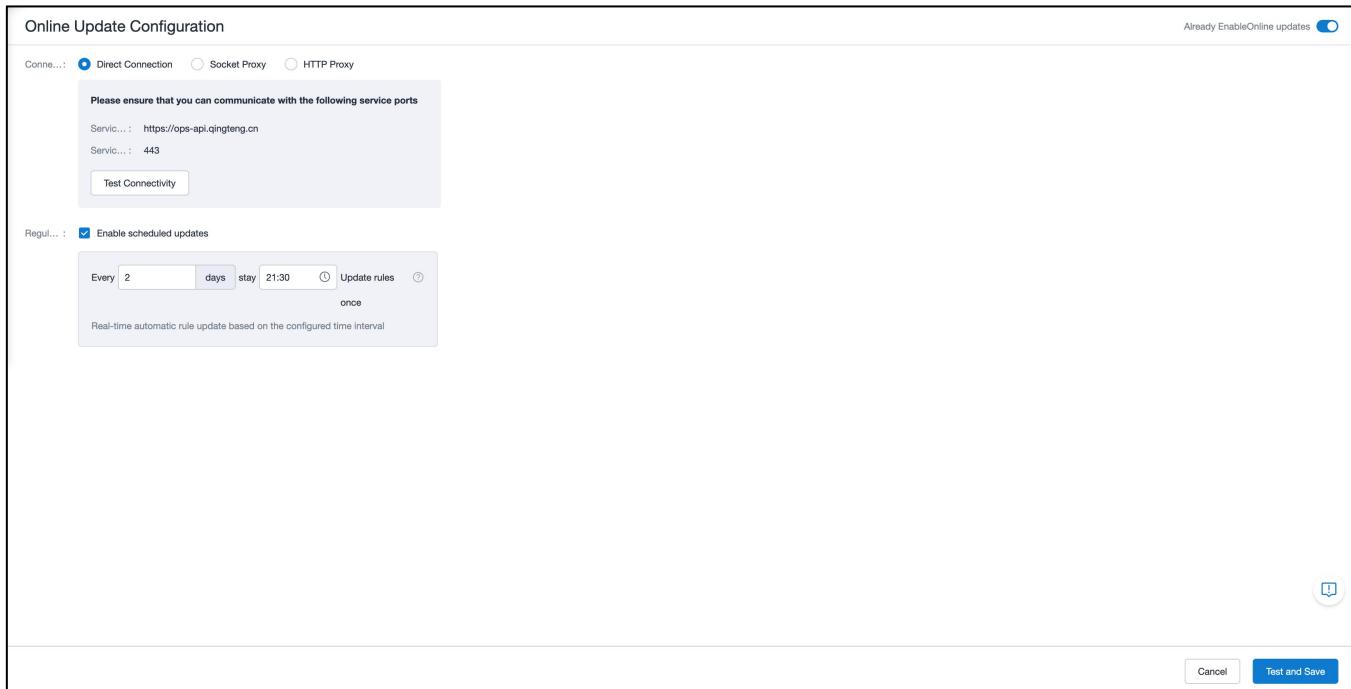
- This method is suitable for situations where the local environment cannot connect to the internet.
- The rule package must be in zip format.
- To update rules using this method, users must first download the rule package to the local environment and then manually upload it.

12.5.1.2.3.2. Online Update

Users can set automatic updates for application rules, after which the system will periodically obtain the latest rules from the online rule server and update them to the local environment without further user intervention.

Click the "Online Configuration Update," configure the automatic update cycle and connection method, click test and apply, and the application rules will begin to update.

The screenshot shows the same user interface as the previous one, but with a different highlighted button. The "Online configuration update" button at the top right is highlighted with a red rectangle. The rest of the interface is identical to the first screenshot, including the status indicators and bottom buttons.



Description:

- This method is suitable for situations where the local environment can connect to the internet.
- Online rule update refers to whether the rules are applied to the host immediately after updating. If online rule update is turned off, the rules will need to be manually enabled after all hosts have been updated.
- Update time configuration refers to the scheduled start time for rule updates. Only "day" units are supported.
- Connection method refers to the way the system establishes connections with each host to update its applications. Currently, direct connection, socket proxy, and HTTP proxy are supported.
- Proxy refers to a service that acts as an intermediary for network information. Users need to configure it themselves.

Socket Proxy Description:

- Socket proxy (SOCKS proxy) refers to a proxy method using a SOCKS server.
- If socket proxy is selected, the proxy address must be filled in, which is the domain name and

port or IP and port of the proxy server used by the user. The port is usually 1080.

HTTP Proxy Description:

- HTTP proxy is specifically used for proxy hosts to access web pages in a browser.
- If HTTP proxy is selected, the proxy address must be filled in, such as <http://dev.api.com/testproxy>.
- HTTP certificate refers to the SSL certificate of the proxy server used by the user, ensuring the security of the server and connection. Users can choose whether to perform certificate verification.

12.5.1.3. Liscense Management

After purchasing CWPP products, users gain usage permissions for different modules, such as points, usable time, etc., i.e., they obtain licenses.

License management allows users to manage their current product permissions, including:

- View authorized products
- Manage product permissions

The page displays the current License status, including: license code, details of existing authorized products.

12.5.1.3.1. Download Certificates

Click "Download certificate"to download the certificate to the local machine.

License Management (Activated)

Licensed product (1)

TestCertificate Valid Download certificate

Customer ...: 在线POC环境 **Sales type:** Subscription

Product ... : 标准版 **Deployme...:** b3e03024-8db7-44f0-9a13-0aa32c0d19aa

FormalCertificate Valid Download certificate

Customer ...: 线上POC **Sales type:** Subscription

Product ... : 标准版 **Deployme...:** b3e03024-8db7-44f0-9a13-0aa32c0d19aa

12.5.1.3.2. Activate Products

Click import certificate, complete the upload to activate or renew the product.

License Management (Activated)

Import certificate

Licensed product (1)

Description:

- The certificate must be in zip format.

12.5.1.3.3. View Activation History

Click "Import History," select "License Details" under the operation bar to view the detailed information of the certificate. Click "Change Content" to see the differences between this certificate and the latest certificate.

Import History

11 items

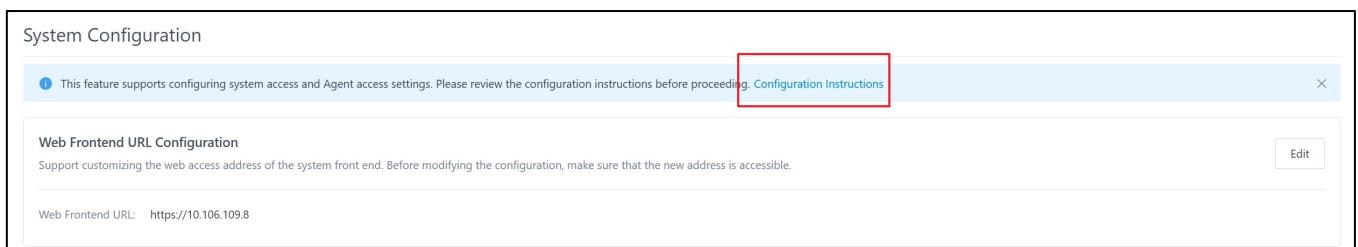
Change Time	Associated Product	License Type	Operator	Operation
2025-02-07 14:48:48		Formal	admin	License Details Change Content

12.5.1.4. System Access Configuration

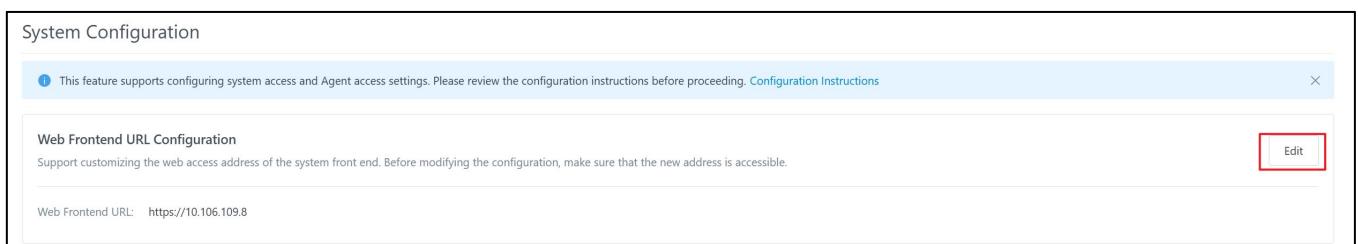
System: Users access the SaaS platform using CWPP products through addresses, domain names, or ports. The SaaS platform used is referred to as the system.

In system configuration, users can configure system access, connection, and other information.

Click "Configuration Instructions" in the top prompt to view detailed system instructions.



Click the "Edit" button of the item to be changed, fill in the content, and click confirm to complete the configuration change.



Web Access Configuration Description:

- Web Access refers to the browser address users enter to access the SaaS platform.
- To set up custom web access, configure the self-accessible URL established by the user.

Web Access IP Allowlist:

- It is mainly used to restrict the access IP of the system console, supporting IP and CIDR formats.
 - Multiple IPs can be separated by line breaks or English commas.
- When the depth of X-Forwarded-For is 0, it means that the direct connection IP address of the request is used to match the whitelist.
- Only the filled IPs are allowed to access the system console.

Agent Connection Service Configuration:

- Agent is a probe installed on the host to collect host security information. It needs to connect to the server to exchange data and execute tasks issued by the server. Agent connection enables communication and coordination between the server and client.
- Custom Agent connection address requires users to fill in the address they use to connect.

TLS Protocol Version Configuration:

- TLS protocol (Transport Layer Security) is used to create secure connections between two applications over the network, preventing eavesdropping and tampering during data exchange.
- The minimum supported TLS protocol version is 1.2, released in 2008.

HTTPS Certificate Configuration:

- HTTPS certificate refers to the SSL certificate of the proxy server used by the user, ensuring the security of the server and connection. Users can choose whether to perform certificate verification.
- The client and system frontend use the same certificate. If an HTTPS certificate is used, the system access domain name must match the domain name of the uploaded certificate; otherwise, verification errors will occur.
- The HTTPS communication protocol uses a key, requiring the sender to encrypt data with the key and the receiver to decrypt data with the key to enhance data transmission security. Users can obtain the key along with the HTTPS certificate.
- The certificate and key must be in pem format.

Custom Navigation Configuration:

- Allows customization of the console's default homepage, which users are directed to upon

login.

Client file upload rate limiting configuration:

- Mainly used to limit the client upload speed, including log upload, file upload, etc. Currently, only local rate limiting is supported, so the maximum upload rate for multiple nodes is the sum of the rates of each node.

Client file download rate limiting configuration:

- Mainly used to limit the client download speed, including installation package download, rule file download, etc. Currently, only local rate limiting is supported, so the maximum download rate for multiple nodes is the sum of the rates of each node.

Console file upload rate limiting configuration:

- Mainly used to limit the file upload speed of console users, including installation packages, rule packages, etc. Currently, only local rate limiting is supported, so the maximum upload rate for multiple nodes is the sum of the rates of each node.

Console file download rate limiting configuration:

- Mainly used to limit the file download speed of console users, mainly for limiting the download speed of files in the download center. Currently, only local rate limiting is supported, so the maximum download rate for multiple nodes is the sum of the rates of each node.

Outbound request access whitelist:

- It is used to restrict the system's access to external resources, supporting domain name and IP address formats. Multiple entries are separated by line breaks or English commas.

Agent Performance Monitor:

- This option configures whether performance monitoring is enabled by default for newly

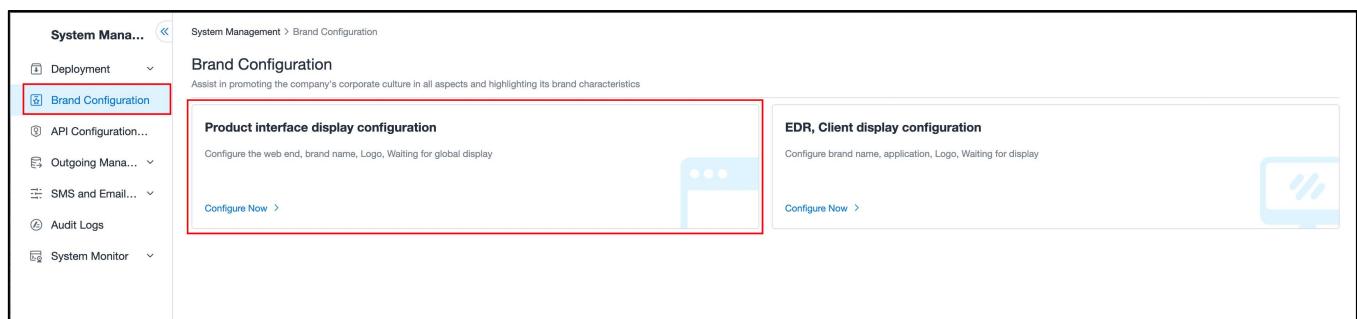
installed Agents. You can modify this setting later in the Agent Management module.

12.5.2. Brand Configuration

Helps users customize the theme color of the console, the product name, and the logo image, as well as the product name and logo image of the EDR client.

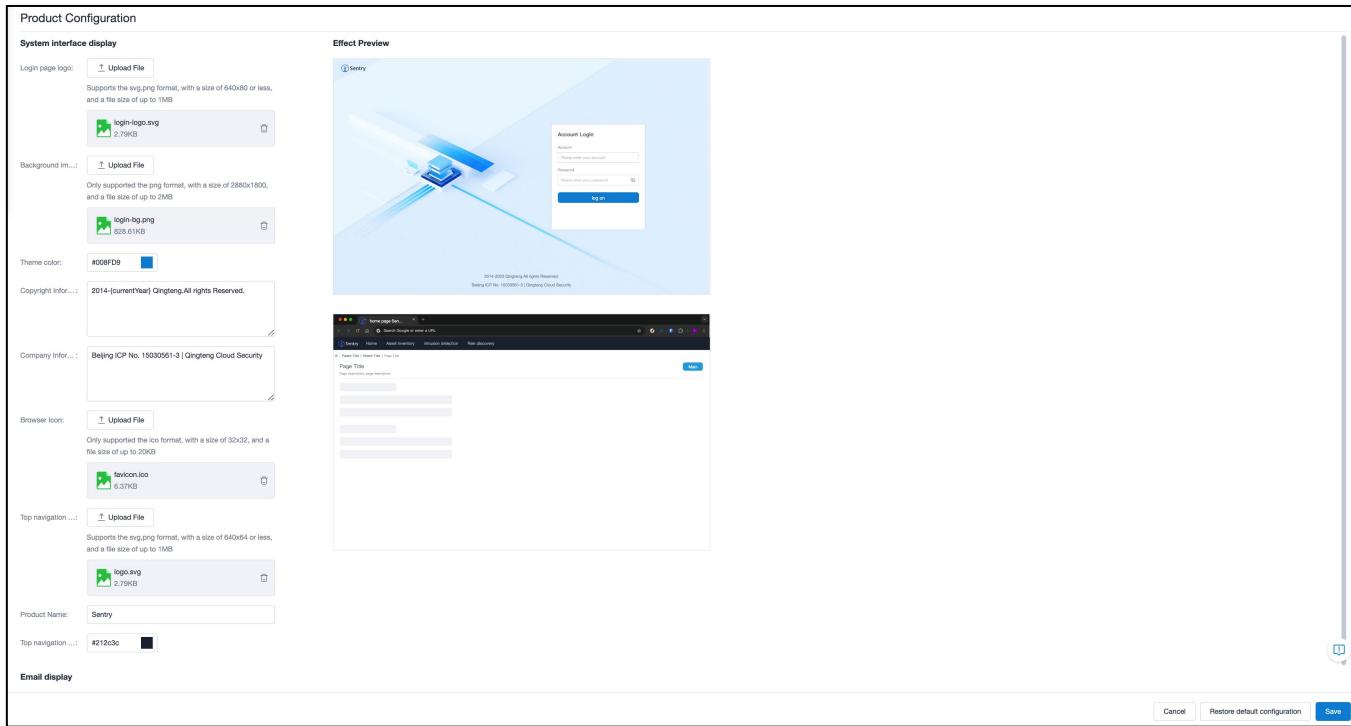
12.5.2.1. Console Display Configuration

When needing to change the console style, go to the [System Management] - [Brand Configuration] page, and select [Product Interface Display Configuration], as shown in the following figure:



Click the "Configure Now" button to enter the configuration page.

- When moving the mouse over the style fields on the left, the modified areas can be viewed on the right.
- After modifying the configurations on the left, the effect can be previewed on the right.
- After making changes, you can click the "Restore Default Configuration" button at the lower right corner of the page to quickly revert to the default brand style of Qingteng Shenrui with one click.



12.5.2.2. EDR Client Display Configuration

You can configure the same logo image and product name for the local client as those of the console.

Go to the [System Management] - [Brand Configuration] page, select [EDR Client Display Configuration], and click the "Configure Now" button to enter the configuration page, as shown in the following figure:

The screenshot shows the 'EDR Client Configuration' page. On the left, there are two main sections: 'Interface configuration' and 'Menu Configuration'. In 'Interface configuration', users can upload files for 'apply name' (Sentry), 'Window, Logo' (logo.svg, 1.26KB), and 'application icon' (favicon.png, 17.28KB). An 'Effect Preview' window on the right shows a 3D shield icon with the text 'Sentry have protected you for 100 days' and 'No risk items found | Last scan time: 2025-03-20 08:47'. In 'Menu Configuration', there is a toggle switch for 'About Us' which is currently off. At the bottom right are buttons for 'Cancel', 'Restore default configuration', and 'Save'.

- When moving the mouse over the style fields on the left, the modified areas can be viewed on the right.
- After modifying the configurations on the left, the effect can be previewed on the right.
- After making changes, you can click the "Restore Default Configuration" button at the lower right corner of the page to quickly revert to the default brand style of Qingteng Shenrui with one click.

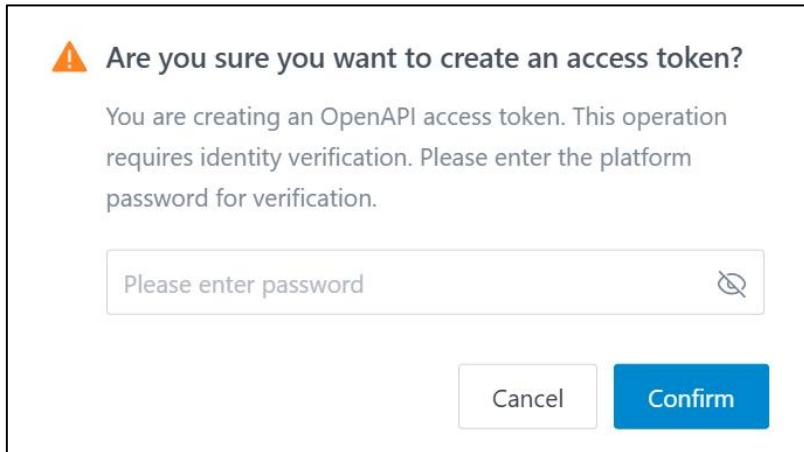
12.5.3. API Configuration Management

You can create personal access tokens for each application that needs to use the OpenAPI. These tokens are used for OpenAPI authentication, and you can create up to 10 access tokens.

The screenshot shows the 'API Configuration Management' page. It displays two access token entries in a table format. Each entry includes a hexagonal icon, the token name ('bxml'), 'Permission...': 'All', 'Creation Ti...': '2024-09-12 17:51:05', 'Last Usag...': '1 minutes ago', and 'Expiration ...': '-'. A blue 'Create Access Token' button is located at the top right of the table area.

Steps:

- Click "Create Access Token". You will first need to verify your identity by entering your platform password (current account password).



- After identity verification is successful, you will be directed to the Create Access Token page.

Create Access Token

Token ...:

Expira...: permanent 3 months 6 months 12 months custom

Permi...: all
Allow the use of all externally developed APIs in the system
 custom
Please customize the selection of allowed functional APIs

Asset Inventory
Allowed to use APIs of Asset Inventory

Local Engine Management
Allowed to use APIs of Local Engine Management

Compliance Baseline
Allowed to use APIs of Compliance Baseline

Event Collect
Allowed to use APIs of Event Collect

Intrusion Detection and Response
Allowed to use APIs of Intrusion Detection and Response

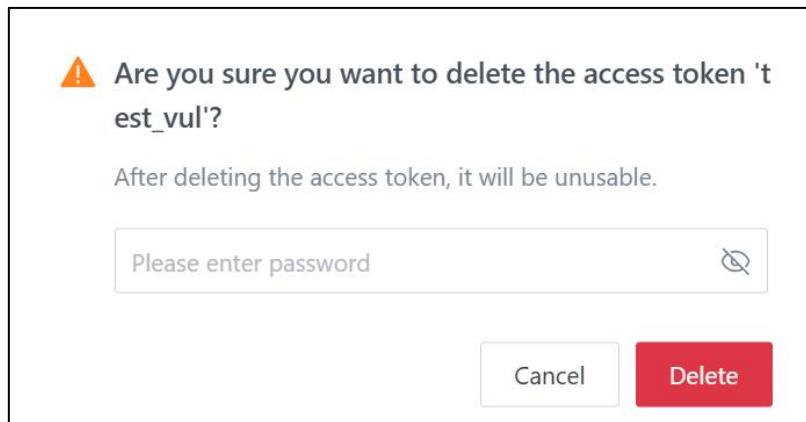
Outgoing
Allowed to use APIs of Outgoing

Vulnerable

!

- **Token Name:** Enter a memorable name.
- **Expiration Time:** Token validity period, options include: Permanent, 3 months, 6 months, 12 months, Custom.

- Permission Configuration: The scope of OpenAPI that the token can access, options include:
 - All, Custom.
 - Custom selection can be made by function.
- If you wish to delete a token, click  and enter your platform password to complete the deletion.



12.5.4. Outgoing

12.5.4.1. Outgoing Introduction

Outgoing is the process of sending or transmitting data stored and processed in security products to external environments in a secure and compliant manner.

After deploying security products, the product side obtains security data from hosts, containers, and PCs. In addition to being used by the security products themselves, this data can be shared with other platforms and products for secondary development or business collaboration.

The CWPP data export function is specifically used to export CWPP product data to other external environments, including:

- Receiving Service Management
- Export Connection Management

- Notification Alerts

12.5.4.2. Outgoing Usage

Outgoing involves three typical steps: creating a receiving service, establishing an export connection, and sending data.

- **Receiving Service:** Refers to the sending target, including service name (target name), service type, service address (target address), etc. The receiving service to be used should be created and configured in advance, and connectivity tests should be performed.
- **Export Connection:** An export connection is equivalent to a data channel. The channel needs to be established first, and then data can be exported. It includes configuration information such as connection name, data source, sending target, and export method.
- **Data Sending:** Data is sent from the source to the target through the export connection, following the configured filtering conditions, sending method, sending cycle, and other parameters.

12.5.4.3. Configuration Management Receiving Service

Go to **【Outgoing】 → 【Receiving Service Management】** to view and manage receiving services.

Receiving Service Management							
1 items		Please enter a search term		Q		New Receive Service	
Service Name	↑ ↓	Service Type	▼	Target Address	▼	Connectivity	▼
演示测试	↑ ↓	Kafka	▼	192.168.12.21:9032	▼	Exception	▼
1 items							
Edit Delete Connectivit...							

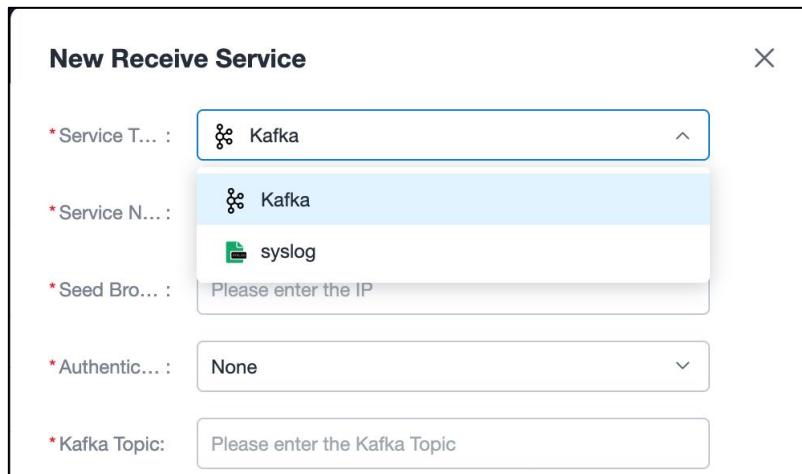
- **Service Name:** The name of the receiving service, which can be customized.
- **Service type:** The type of receiving service, including HTTP, Kafka, Syslog, etc.
- **Target Address:** The address of the receiving service, which can be an IP address or a domain name.

- Connectivity: The connectivity status of receiving services, divided into: normal, abnormal, undetected, and unsupported
Associated outbound connections: which outbound connections reference the receiving service, displayed in the form of a/b, where a represents the number of currently associated and enabled outbound connections, and b represents the number of all currently associated outbound connections
- Creation time: The time when the receiving service was created
- Update time: The time when the operation received the service
- Operator: The account that operates the receiving service
- Operation: Receive service support operations, including editing, deleting, and connectivity testing

12.5.4.3.1. How to Create Receiving Service

Click **【New Receive Service】** to create a new receiving service.

Select the type of receiving service. We support Kafka、Syslog.



The creation methods vary depending on the type of service, please refer to:

- Create a Kafka type receiving service

- Create a Syslog type receiving service

12.5.4.3.1.1. Create a Kafka type receiving service

New Receive Service

* Service Type :

* Service Name :

* Seed Broker :

* Authentication :

Enable SSL:

* Kafka Topic:

* Compression :

Custom Configuration:

```
{
  "client.id": "test",
  "retries": 3,
  "retry.timeout.ms": 1000,
  "acks": 1,
  "max.broker.write.bytes": 1024,
  "max.broker.read.bytes": 1024,
  "max.record.batch.bytes": 1024,
  "max.buffered.records": 1024,
  "max.buffered.bytes": 1024,
  "produce.timeout.ms": 1000,
  "record.retries": 3,
  "delivery.timeout.ms": 1000,
  "linger.ms": 1000,
  "disable.idempotence": false
}
```

DNS Config:

```
{
  "test.kafka": "192.168.1.1"
}
```

Single Data Limit : Fill 0 means no limit; fill a specific number, means when the data exceeds this upper limit, the data will not be sent

- Service type: Kafka
- Service name: Please fill in the service name, choose a simple and memorable name, support 1-64 characters
- Seed Brokers: Please fill in the target address IP + Port. Supports entering multiple addresses.
- Authentication methods: Five authentication methods are supported: None, Plain, SCRAM-SHA-512, SCRAM-SHA-256, and Kerberos.
- Enable SSL: SSL protocol is supported. It is enabled when the toggle is on, and disabled when the toggle is off.
- Login User: Please provide the login account for the target address (if not available, it can be left blank)
- Login password: Please fill in the login password for the target address (if not available, it can be left blank)
- Kafka Topic: Please fill in the Kafka topic you want to use
- Compression method: You can choose gzip, snappy, lz4, zstd, or none.
- Custom configuration: Parameters can be set.
- Single Data Size Limit: Set the maximum size for a single piece of data. Enter 0 to indicate no limit; enter a specific number to mean that the data will not be sent if it exceeds this limit.

12.5.4.3.1.2. Create a Syslog type receiving service

New Receive Service X

* Service T... :

* Service N... :

* IP:

* Port:

* Protocol: UDP TCP

* Tag:

Hostname:

Custom C... :

Single Dat... :

Cancel Save

- Service type: syslog
- Service name: Please fill in the service name, choose a simple and memorable name, support 1-64 characters

- IP: Please fill in the target address IP
- Port: Please fill in the destination address port
- Protocol: Please fill in the network protocol used, which is divided into: UDP、TCP
- Tag: Please fill in the Syslog tag, which will serve as the Syslog identifier for quick identification
- Hostname: Optional. The name of the server that sends syslog, which can be customized to a name that is easy to identify.
- Custom configuration: Parameters can be set.
- Single Data Size Limit: Set the maximum size for a single piece of data. Enter 0 to indicate no limit; enter a specific number to mean that the data will not be sent if it exceeds this limit.

12.5.4.3.2. How to Test Connectivity

On 【Reception Service Management】 interface, click on "Connectivity Test" on the established reception service.

Connectivity testing will check whether the network between the current environment and the target is unobstructed and whether the service is normal.

- If the test passes, it will display "Normal" in the "connectivity" section of the receiving service.
- If the test fails, an "Exception" will be displayed in the "connectivity" section of the receiving service.
- The receiving service with 'abnormal' connectivity is unavailable. It is necessary to first check whether the target address is correct and whether the network firewall is enabled in the target network environment. The problem should be investigated until the connectivity test is passed before using the guidance.

Receiving Service Management							
1 items		Please enter a search term		Q		New Receive Service	
Service Name	↑ ↓	Service Type	↓	Target Address	↓	Connectivity	↓
演示测试	↑ ↓	Kafka	↓	Exception	↓	0/0	↓
1 items							
Edit		Delete		Connectivit...		< 1 > 50 Item/Page	

12.5.4.3.3. How to check the usage of receiving services

On the 'Receive Service Management' interface, you can view the information of outgoing connections using the established receive service through 'Associated Outbound Connections'.

Presentation format: a / b

A represents the number of outgoing connections currently associated and enabled.

B represents the number of all outgoing connections currently associated.

Service Name	↑ ↓	Service Type	↓	Target Address	↓	Connectivity	↓	Associated Outbound Connections	Operation
演示测试	↑ ↓	Kafka	↓	Exception	↓	0/0	↓	Edit Delete Connectivit...	↓

12.5.4.3.4. How to edit the receiving service

During use, if there is a need to adjust or change the configuration content of the receiving service, it can be modified through the "Edit" operation.

- The receiving service is not being used by the external connection and can be edited.
- The receiving service is being used by external connections
 - External connection not enabled, this receiving service is editable
 - External connection enabled, this receiving service cannot be edited.

Receiving Service Management								
1 items <input type="text" value="Please enter a search term"/> <input type="button" value="Search"/> New Receive Service								
Service Name	↑ ↓	Service Type	↓	Target Address	↓	Connectivity	↓	Associated Outbound Connections Operation
演示测试		Kafka		██████████		Exception		0/0 Edit Delete Connectivit...

The edit page is the same as the create page except for:

- In the edit page, "Service type" cant be changed.

12.5.4.3.5. How to delete the receiving service

Click "delete" to clean unused receiving service.

- If the receiving service is not used by any outbound connections, it can be deleted.
- If the receiving service is used by outbound connections, it cannot be deleted.

Receiving Service Management								
1 items <input type="text" value="Please enter a search term"/> <input type="button" value="Search"/> New Receive Service								
Service Name	↑ ↓	Service Type	↓	Target Address	↓	Connectivity	↓	Associated Outbound Connections Operation
演示测试		Kafka		██████████		Exception		0/0 Edit Delete Connectivit...

12.5.4.4. Configure outgoing

In [Outgoing] → [Outgoing Connection Management], you can view and manage outgoing connection.

Outgoing Connection Management													
0 items <input type="text" value="Please enter a search term"/> <input type="button" value="Search"/> New Outbound													
Status	↓	Connection Name	↑ ↓	Outbound Data	↓	Data Source	↓	Send Target	↓	Connection Status	↓	Operation	↓

- Status:** The enabled/disabled status of the outbound connection.
- Connection Name:** A user-defined name for the outbound connection. Choose a simple and memorable name for easier management.
- Outbound Data:** The selected data to be sent out.

- **Data Source:** The applications from which the data originates.
- **Target:** The destination of the data transmission, which is a selected receiving service. Display format: Icon + Receiving Service Name + Receiving Service Target Address.
- **Connection Status:** The current status of the outbound connection, which can be: Normal, Abnormal, or Disabled.
- **Creation Time:** The time when the outbound connection was created.
- **Update Time:** The time when the outbound connection was last modified.
- **Operator:** The account that performed operations on the outbound connection.
- **Operations:** The supported actions for the outbound connection, including: Details, Edit, Delete.

12.5.4.4.1. How to create outgoing connection

Click "New outbound" in 【Outgoing Connection Management】 page.

- **Connection Name :** Enter simple and memorable name for easier manage.
- **Outbound Method :** Choose Full send or Incremental Send.

The screenshot shows the 'Create Outbound Link' dialog box. It contains the following fields:

- * Connection... :
- * Outbound ... : Full Send Incremental Send
- * Outbound ... : >
- * Outbound ... : Once Daily Weekly Expression
- * Send Target: >
- * Sending Ra... : MB/s

Different outbound method means different create method, see more :

- Create outbound with Full Send method
- Create outbound with incremental Send method

12.5.4.4.1.1. Create outbound with Full Send method

The screenshot shows the 'Create Outbound Link' dialog box. It includes the following fields:

- * Connection... : Please enter simple name for easier manage
- * Outbound ... : Full Send Incremental Send
- * Outbound ... : Please select business data >
- * Outbound ... : Once Daily Weekly Expression
- * Send Target: Please select a receiving service >
- * Sending Ra... : 5 MB/s

- **Connection Name:** Enter a simple and memorable name for easier management.
- **Outbound Method:** Full send.
- **Outbound Data:** Select the data to be sent out.
- **Outbound Frequency:** Supports selection of one-time, daily, weekly, or custom expression (using regular expressions).
- **Target:** Select the receiving service.
- **Rate Limit:** Used to limit the sending rate for this outbound connection.

12.5.4.4.1.2. Create outbound with incremental send method

Create Outbound Link

* Connection... : Please enter simple name for easier manage

* Outbound ... : Full Send Incremental Send

* Outbound ... : Please select business data >

* Send Target: Please select a receiving service >

* Sending Ra... : 5 MB/s

- **Connection Name:** Enter a simple and memorable name for easier management.
- **Outbound Method:** Incremental Send
- **Outbound Data:** Select the data to be sent out.
- **Target:** Select the receiving service.
- **Rate Limit:** Used to limit the sending rate for this outbound connection.

12.5.4.4.1.3. Select outgoing Data

Under the full-volume method, the selectable data list displays business data that supports the full-volume method.

Under the incremental method, the selectable data list displays business data that supports the incremental method.

Select Business Data

Available Data (622 items)

Please select filter content

Selected Data (3 items) Clear

Alarm details (Intrusion Detection and Response/Intru... ×)
Host Agent List (Probe Management/Host Agent) ×
Clusterlink List (Probe Management/Clusterlink) ×

APP Name

Intrusion Detection and Response

- ▶ Intrusion alarm
 - Alarm details
- ▶ Probe Management
- ▶ Asset Inventory
- ▶ Event Collect

Select Data Range

Scope of A...: Host

All Hosts

Select from the list

Select Business Group

Cluster

!

Cancel Save

- The selectable data list displays the available business data in a hierarchical structure: by application (first level) and application data (second level). It supports single selection, multiple selections, and full selection.
- After selecting the business data, you need to choose the data scope, which defines the range of endpoints where the selected business data will take effect.
 - The data scope supports selection by host or cluster.
 - You can choose individual, multiple, or all hosts/clusters.

12.5.4.4.2. How to view outgoing connection details

On the "Outgoing connection Management" page, click "details" can check this outgoing connection.

12.5.4.4.2.1. Details of full send method

Connection Details

1111 Edit

资产清点 10.***.***.udp

Send Content: WMI,数据挂载... Total 242 items | Total Data Sent Today: 0 B | IP: 10.***.***.*** | Connection Name: 1111 | 端口: 514 | Outbound Cycle: Once

Execution Records

Associated App	Microservice	Start Time	End Time	Status	Data Volume	Failure Information
资产清点	service-asset	2025-11-11 15:5...	2025-11-11 15:5...	Send Succes...	72.53MB	
资产清点	service-asset	2025-11-11 15:3...	2025-11-11 15:4...	Send Succes...	72.54MB	
资产清点	service-asset	2025-11-11 14:5...	2025-11-11 14:5...	Send Succes...	68.19MB	
资产清点	service-asset	2025-11-11 14:4...	2025-11-11 14:4...	Send Succes...	72.71MB	
资产清点	service-asset	2025-11-11 14:3...	2025-11-11 14:3...	Send Succes...	4.56MB	
资产清点	service-asset	2025-11-11 14:2...	2025-11-11 14:2...	Send Succes...	4.56MB	

Sent Data Volume Statistics

Time range, val1

The chart displays the volume of outbound traffic over a specific time period. The Y-axis represents the data volume in bytes, ranging from 0 to 500,000,000. The X-axis shows dates: 2025-10-27, 2025-11-10, and 2025-11-11. A single blue line with circular markers shows the traffic volume starting at 0 on 2025-10-27, rising sharply to approximately 400,000,000 on 2025-11-10, and then slightly decreasing to about 350,000,000 on 2025-11-11.

Date	Outbound Traffic (Bytes)
2025-10-27	0
2025-11-10	~400,000,000
2025-11-11	~350,000,000

Outbound Traffic

View the name, sent content, outbound cycle, target address, execution records, and statistics of sent data volume for current outbound connections.

The execution records include the App, microservice, start time, end time, data volume, and sending

status corresponding to each full-data transmission execution.

The statistics of sent data volume display traffic based on the selected time period, with the minimum statistical unit being per hour.

12.5.4.4.2.2. Details of incremental send method

Connection Details

test-inc-wzm Edit

探针管理

Send Content: 集群组件列表,主... Total 2 items

Total Data Sent Today: 0 B

Connection Name: test-inc-wzm

地址列表: 10.10.10.10

Latest Error Log

Sent Time	Error Message
2025-11-19 18:30:20	records have timed out before they were able to be produced
2025-11-19 18:28:56	records have timed out before they were able to be produced
2025-11-19 18:28:56	records have timed out before they were able to be produced
2025-11-19 18:28:56	records have timed out before they were able to be produced
2025-11-19 18:28:56	records have timed out before they were able to be produced
2025-11-19 18:28:56	records have timed out before they were able to be produced
2025-11-19 18:28:56	records have timed out before they were able to be produced
2025-11-19 18:27:00	records have timed out before they were able to be produced

Sent Data Volume Statistics

Time range, val1

A line chart titled "Outbound Traffic" showing data volume over time. The Y-axis represents the data volume in bytes, ranging from 0 to 10,000,000. The X-axis represents dates from November 7 to November 13, 2025. The data shows a peak on November 11 followed by a decline and a slight increase towards the end of the period.

Date	Outbound Traffic (val1)
2025-11-07	~500,000
2025-11-10	~2,500,000
2025-11-11	~8,500,000
2025-11-12	~500,000
2025-11-13	~3,500,000

View the name, sent content, outbound cycle, target address, error records, and sent data volume

statistics of current outbound connections.

The error records display the time of occurrence of sending errors and the corresponding error messages.

The statistics of sent data volume display traffic based on the selected time period, with the minimum statistical unit being per hour.

12.5.4.4.3. How to edit outgoing connection

Receiving Service Management						
Items		Please enter a search term		Operations		
Service Name	↑ ↓	Service Type	▼	Target Address	▼	Connectivity
演示测试	↑ ↓	Kafka	▼	192.168.12.21:9032	▼	Exception
1 items						0/0
						Edit Delete Connectivit...

If you need to adjust or change the external connection configuration content when using it, click "Edit".

- The external connection cannot be edited when it's enabled.
- The outbound connection cannot be edited when it's disabled.

The difference between the interface for editi external connections and create new external connections is:

- When editing, the 'outgoing method' does not support modification

12.5.4.4.4. How to delete outgoing connection

Click "delete" to clean unused outgoing connection

- The external connection cannot be deleted when it's enabled.
- The outgoing connection cannot be deleted when it's disabled.

Receiving Service Management								
1 items <input type="text" value="Please enter a search term"/> <input type="button" value="Search"/> <input type="button" value="New Receive Service"/>								
Service Name	↑ ↓	Service Type	↓	Target Address	↓	Connectivity	↓	Associated Outbound Connections
演示测试	↑ ↓	Kafka	↓	██████████	↓	Exception	↓	0/0
1 items								

12.5.5. SMS and Email Configuration

When an intrusion detection alert is generated, the system sends a notification to the user.

Notification configuration allows setting up the platform, account, and sending frequency for notifications.

12.5.5.1. Service Configuration

Click "Configure Service," modify the relevant information, and click "Save" to complete the changes.

System Management > SMS and Email Configuration > Service Configuration

Service Configuration

Email service configuration

Platform Configuration

Platform: SMTP

Host: -

SMTP Acc...: -

SMTP Pas...: -

Port: -

Encryption...: -

Auth Type: -

Skip SSL V...: -

Sender Email: -

Sender Na...: -

BCC: -

Send Frequency

Interval (se...: -

Sending Li...: -

SMS service configuration

Platform Configuration

Platform: Submail

Domestic SMS Configuration

Enabled: -

Platform URL: -

APP ID: -

Secret: -

Template ID: -

Content Key: -

International SMS Configuration

Enabled: -

Platform URL: -

APP ID: -

Secret: -

Template ID: -

Content Key: -

Send Frequency

Interval (se...: -

Sending Li...: -

SMS Configuration Notes:

SMS service configuration

Platform Configuration

Platform: Submail

Domestic SMS Configuration

* Enabled:

* Platform URL...:

* APP ID:

* Secret: 

* Template ID:

* Content Key: 

* Test Phone N...: +86 (China Mainland) Please enter the test phone nu
The test phone number is only used for testing connections and will not be saved

International SMS Configuration

* Enabled:

Send Frequency

* Interval (sec...):

* Sending Limit:




- Platform refers to the SMS platform through which the system sends messages. Currently, Submail is supported.
- After the user activates the SMS service on the platform, the platform will create an application for sending SMS. After successful creation, the user can obtain the SMS key.

- Platform URL, SMS platform address
- APP ID uniquely identifies the APP and is used for SMS WEB API requests. Generally, the SMS service platform automatically creates it.
- After applying for the SMS template service on the SMS platform, the user can obtain the template ID and template content key to ensure the correct template correspondence.
- The test phone number is used as the recipient for connection testing.
- Domestic SMS configuration: used to configure parameters of domestic SMS platforms for sending SMS to domestic mobile phones.
- International SMS configuration: used to configure parameters of foreign SMS platforms for sending SMS to foreign mobile phones.
- Sending Frequency
 - Interval: Set the interval time.
 - Sending limit: The maximum number of SMS messages that can be sent within the interval. If this limit is exceeded, the sending will fail and be recorded in the notification failure records.
 - The above two parameters are used to set the upper limit of the sending frequency. For example, an interval of 60 and a limit of 100 means that a maximum of 100 messages can be sent within 60 seconds.

Email Service Configuration:

Email service configuration

SMTP Password: 

* Port:

Encryption Me...: 

* Auth Type ⓘ: 

* Skip SSL Veri...:

Enable Insecur...:

* Sender Email:

* Sender Name:

BCC ⓘ:

* Test Email:
The test email is only used for testing the connection and will not be saved

Proxy Configur...: Direct Socks5 proxy Http proxy

* Proxy address:

Username:

Password: 

Send Frequency

* Interval (seco... :

* Sending Limit:

- Currently, the email service supports the SMTP protocol. Users need to set up their own SMTP server to send emails. The server address and port can be found on the service provider's official page to correctly correspond to the email service.
- Encryption methods are used to protect email information from being stolen, including

SSL/TLS, STARTTLS, or no encryption.

- Authentication verifies whether the user has the right to access the email system. Currently supported authentication methods include AUTH LOGIN, AUTH PLAIN, and AUTH CRAMMDS. Users can set them up themselves.
- SSL certificates are electronic certificates used for server identity verification and data transmission encryption to protect electronic communication security. Users can enable them when setting up the email service platform.
- The system will send emails in the name of the sender's email and name filled in by the user.
- BCC (Blind Carbon Copy) sends a copy of the email to multiple recipients, where each recipient can only see their own address and not others. BCC should be turned off if the user's email server does not allow anonymous sending.
- The test email is used as the recipient email for connection testing.
- Proxy Configuration: Supports direct connection, SOCKS proxy, and HTTP proxy. When a proxy mode is enabled, enter the proxy server address and port, along with the account and password.
- Sending Frequency
 - Interval: Set the interval time.
 - Sending limit: The maximum number of emails that can be sent within the interval. If this limit is exceeded, the sending will fail and be recorded in the notification failure records.
 - The above two parameters are used to set the upper limit of the sending frequency. For example, an interval of 60 and a limit of 100 means that a maximum of 100 emails can be sent within 60 seconds.

Click "Clear Configuration" to clear the original configuration content.

The screenshot shows two side-by-side configuration panels. On the left is the 'Email service configuration' panel, which includes fields for Platform (SMTP), Host, SMTP Account, SMTP Password, Port, Encryption, Auth Type, Skip SSL Verification, Sender Email, Sender Name, and BCC. It also has a 'Send Frequency' section with Interval and Sending List fields, and two buttons: 'Configure Service' and 'Clear Configuration'. The 'Clear Configuration' button is highlighted with a red box. On the right is the 'SMS service configuration' panel, which includes sections for 'Platform Configuration', 'Domestic SMS Configuration', and 'International SMS Configuration'. It has similar fields for Platform (Submail), Enabled, Platform URL, APP ID, Secret, Template ID, Content Key, and Send Frequency. It also has 'Configure Service' and 'Clear Configuration' buttons, with the 'Clear Configuration' button highlighted with a red box. There are also two small circular icons with speech bubbles in the top right corner of the right panel.

12.5.5.2. Notification Failure Records

You can search and filter notification failure records by tenant, message type, message level, title, recipient, and sending status fields.

The screenshot shows a 'Failure Records' interface with a search bar at the top. The search bar includes a note 'Display only the last 7 days of data by default', a 'Click to edit search tags' button, and a date range 'First sending time: 2025-06-24 18:39:24 ~ 2025-07-01 18:39:24'. Below the search bar is a table with 293837 items. The table has columns for ID, Message Type, Message Sub-Type, Tenant Name, Receiver, Error Message, Send Count, First sending time, Recent send time, Send Status, and Operation. The 'Operation' column contains buttons for 'Partially F...', 'Details', 'Resend', and 'Delete'. The table is filtered by several tags: Malicious Process, Driver Anomaly AI, Suspicious Comm., Agent Self Defense, Invalid phone number, and code:19007. A note at the bottom left says '发现共有 1 ...' (Found a total of 1 ...).

Clicking on the search box will display search tags, allowing you to search by tags, including:

- Search message records by tenant name.

- Search message records by complete ID.
- Filter message records by selecting message type, message subtype, message level, and sending status.
- Search message records by keywords in the title or recipient.
- Search message records by selecting the recent sending time range.

12.5.6. Audit Logs

Records user activities, saves log content, and supports unified query, statistics, and analysis.

Audit Logs									
⚠ Display only the last 7 days of data by default									
112164 items	Please select the filtering content			Export All					
Operation Time	Operator	Log Content	Source IP	Request URL	Belongs to Service	Result	Operation		
2025-02-24 09:55:56	admin	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	Success	Details		
2025-02-24 09:55:53	admin	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	Success	Details		
2025-02-24 09:55:53	admin	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	Success	Details		
2025-02-24 09:55:53	admin	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	Success	Details		

Steps:

- By default, the log displays data from the last 7 days.
- To view detailed information of a specific log entry, click the "Details" button. On the details page, you can also copy the original log text.

The screenshot shows the "Log Details" interface. It includes sections for Summary, Details, Source, Conclusion, and Original Log. The Original Log section displays a JSON log entry with line numbers from 1 to 14. The log content is as follows:

```
1 {
2   "id": "019535ab-0a7f-7ec3-9e6b-ad86a7399bd0",
3   "user_uuid": "effbfbca66d1dfb0cad72",
4   "username": "admin",
5   "role_names": [
6     "Admin",
7     "DeployAdmin"
8   ],
9   "app": "com.qt.os.kernel",
10  "app_display_name": "系统内核",
11  "service_name": "kernel",
12  "api": "16153b490baa24d6",
13  "api_name": "获取获取审计日志所属服务列表",
14  "uri": "/api/com/qt-os-kernel/kernel/console/v1/audit-logs/services?_t=1740362156672",
15 }
```

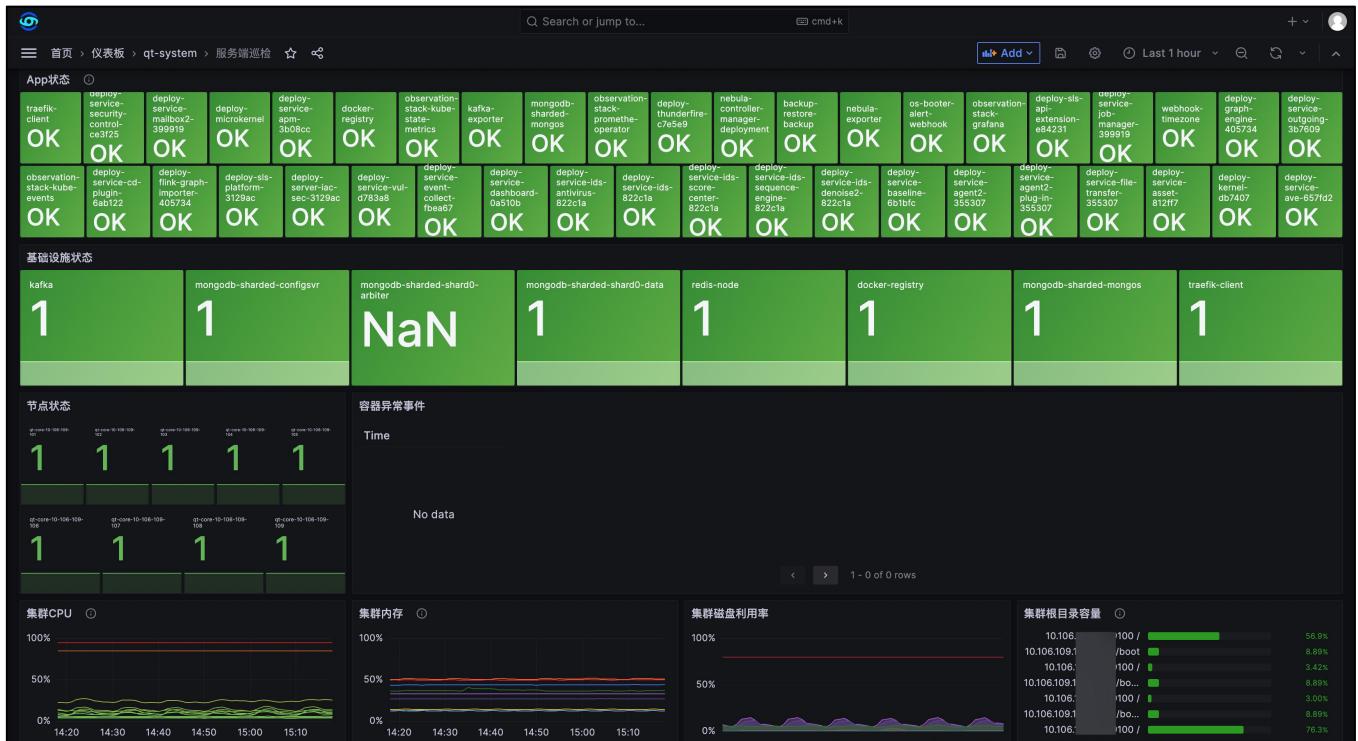
- The system supports batch export of logs.

12.5.7. System Monitor

Allows viewing of operational status, performance metrics for the product's server-side and agent-side components, supporting daily operational maintenance and troubleshooting.

12.5.7.1. Monitor information

Access the system backend to inspect real-time operational status and logs of applications and services.



12.5.7.2. Log Analysis

Query and analyze application logs in the system backend using common troubleshooting keywords

to identify root causes.

The interface allows users to configure log analysis parameters and start the process.

- Log analysis configuration:** Includes sections for Application classification, Pre-set keywords, and File download.
- Application classification:** Classify by application app for easier query.
- Pre-set keywords:** Provide common keywords for one-click analysis.
- File download:** Save the analysis results as a file for easy download.
- Start analyzing:** A blue button to initiate the log analysis process.

The screenshot shows a list of common log filters under the '常见日志筛选' (Common Log Filter) section. Each item includes a star icon for favoriting. The filters listed are:

- [常见错误日志]com.qt.app.asset-service-asset qt-system
- [常见错误日志]com.qt.app.baseline-service-baseline qt-system
- [常见错误日志]com.qt.app.eventcollect-service-event-collect qt-system
- [常见错误日志]com.qt.app.ids-service-ids qt-system
- [常见错误日志]com.qt.app.outgoing-service-outgoing qt-system
- [常见错误日志]com.qt.app.vulnerable-service-vul qt-system
- [常见错误日志]com.qt.os.agent-service-agent2 qt-system
- [常见错误日志]com.qt.os.data-service-dashboard qt-system
- [常见错误日志]com.qt.os.kernel-kernel qt-system

12.5.7.3.dump Log

The dump log records the log information of the client Agent's crash. You can download the file to analyze the specific cause.

The screenshot shows the 'dump Log' page under 'System Management > System Monitor'. On the left, there is a sidebar with categories: 'crash' (selected), 'driver_dump', 'agent_quit', and 'diaglog'. The main area displays a table of dump logs with the following columns: File Name, Size, Report Time, and Operation (Download). There are 5 items listed:

File Name	Size	Report Time	Operation
e04...11-agent.core.info.23104-windows-x86_64-3.11.0.0-250616.63.x86_64.debug-a8703eaa.gz	14.43KB	2025-09-08 11:34:07	Download
e04...e9-agent.core.info.31285-linux-aarch64-3.13.0.0-250902.113.aarch64_1756803242.gz	45.75KB	2025-09-03 17:38:10	Download
9e3...da-agent.core.info.1349853-linux-x86_64-3.13.0.0-250829.102.x86_64_1756747284.gz	143.54KB	2025-09-02 01:21:11	Download
bb5...0f1-agent.core.info.30718-linux-x86_64-3.13.0.0-250829.102.x86_64_1756458129.gz	80.97KB	2025-08-29 17:32:15	Download
0e2...bf1d-agent.core.info.854383-linux-x86_64-3.13.0.0-250825.80.x86_64_1756195734.gz	206.77KB	2025-08-26 16:10:50	Download

12.6. Tenant Management

Tenant: CWPP operate and provide service in a SaaS pattern, with each customer purchasing products and services on a rental basis. Such customers are called tenants.

- Each tenant has a unique identifier, including tenant ID, tenant account, and password.
- CWPP products are used by multiple tenants simultaneously.

The tenant management function can assist administrators in comprehensive management based on the tenant dimension, including:

- Tenant Information Overview
- Tenant Agent Management
- Tenant Data Outbound Configuration

12.6.1. Tenant Overview

The Tenant Overview section allows viewing tenant information, managing tenant accounts, and configuring tenant authorizations.

The tenant list displays summary information, including: number of tenants, tenant activation/deactivation status, and tenant details.

12.6.1.1. Query Tenants

Click the search box to display search tags, which can be used for single-item searches, including:

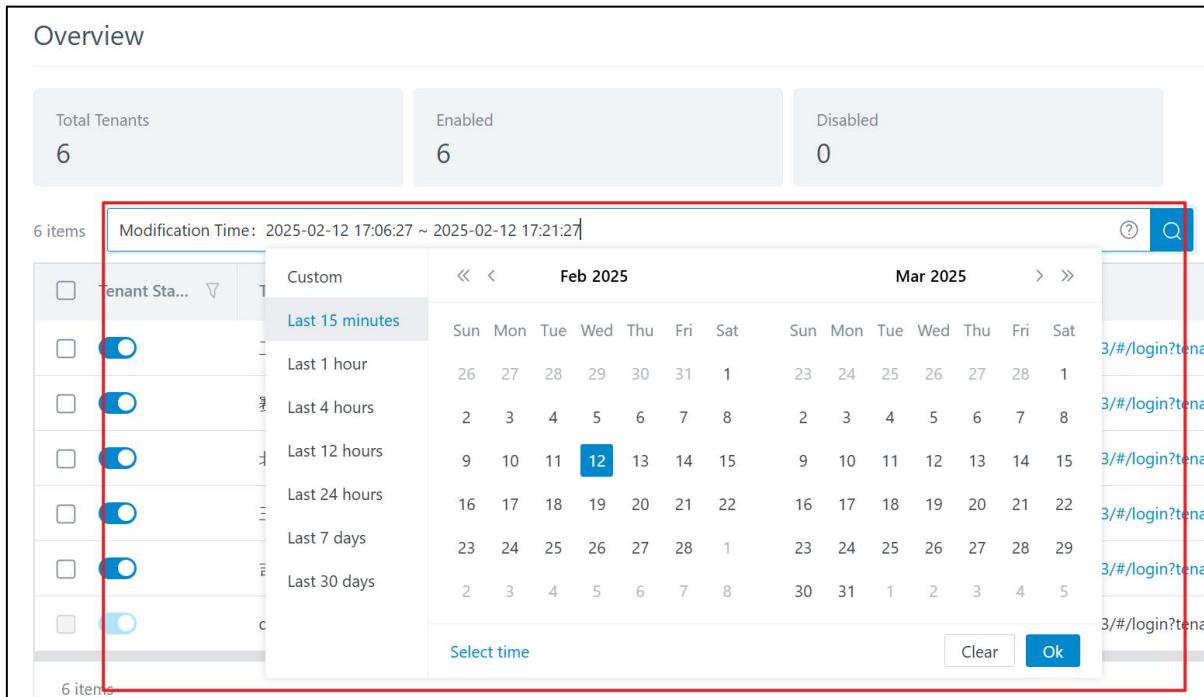
- Filter tenants by activation or deactivation status
- Search tenants by **keyword** in tenant name
- Search tenants by **complete** Tenant ID
- Search tenants by primary account name
- Search tenants by creation time within a specified range
- Search tenants by modification time within a specified range

Click  to view the search box instructions.

Note:

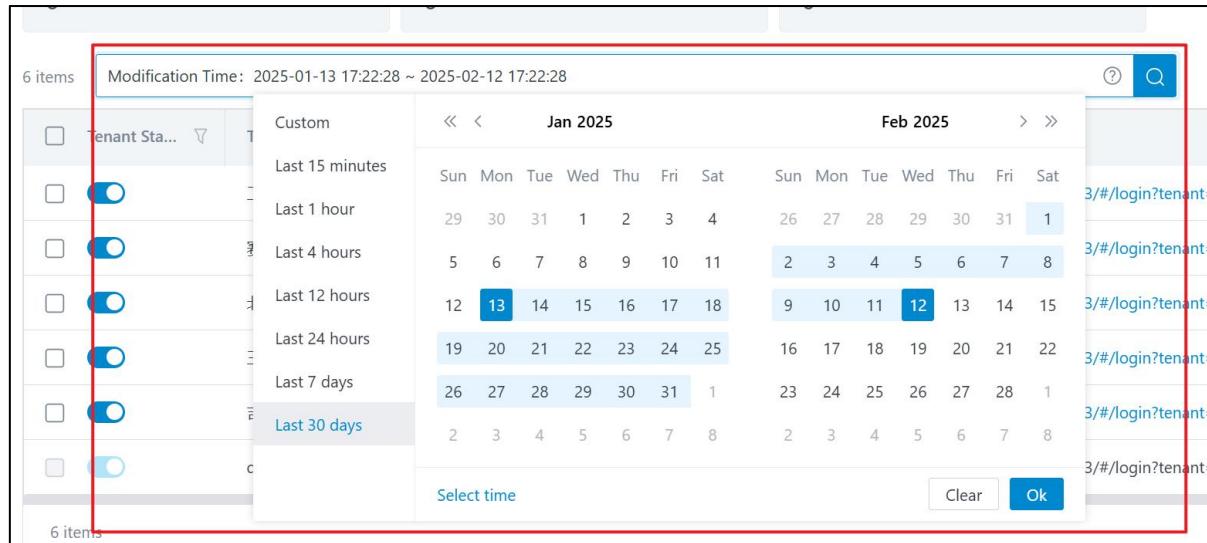
- When using "Creation Date" and "Modification Time" tags, you need to select the desired time range.

- The system will automatically display the date selection page, using the current time as the default endpoint for the range.
- For example, if you select the last 15 minutes, the system will set the range to the 15 minutes before the current search time (e.g., 17:21:27).

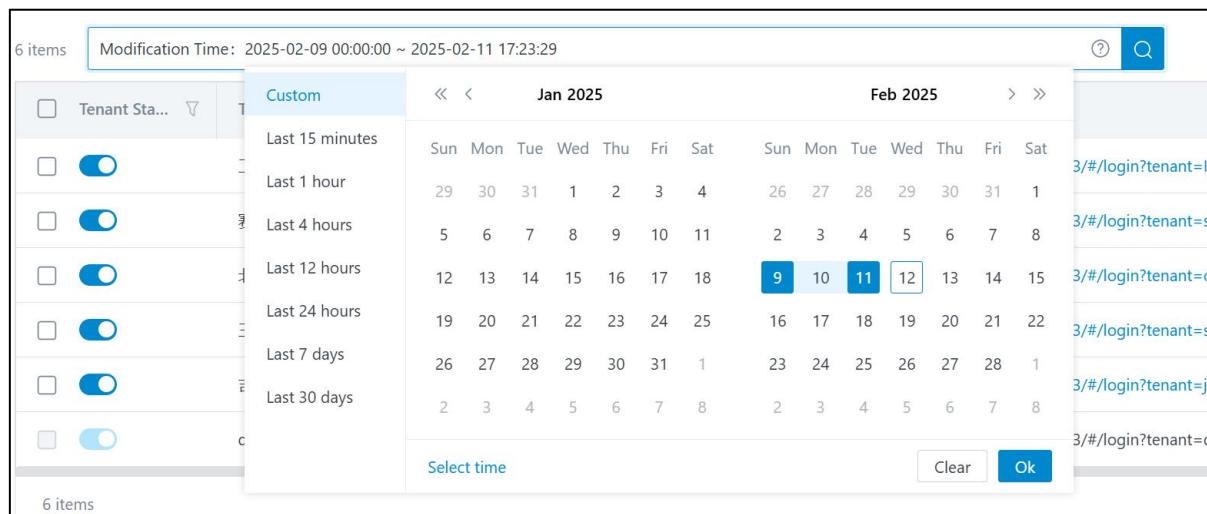


•

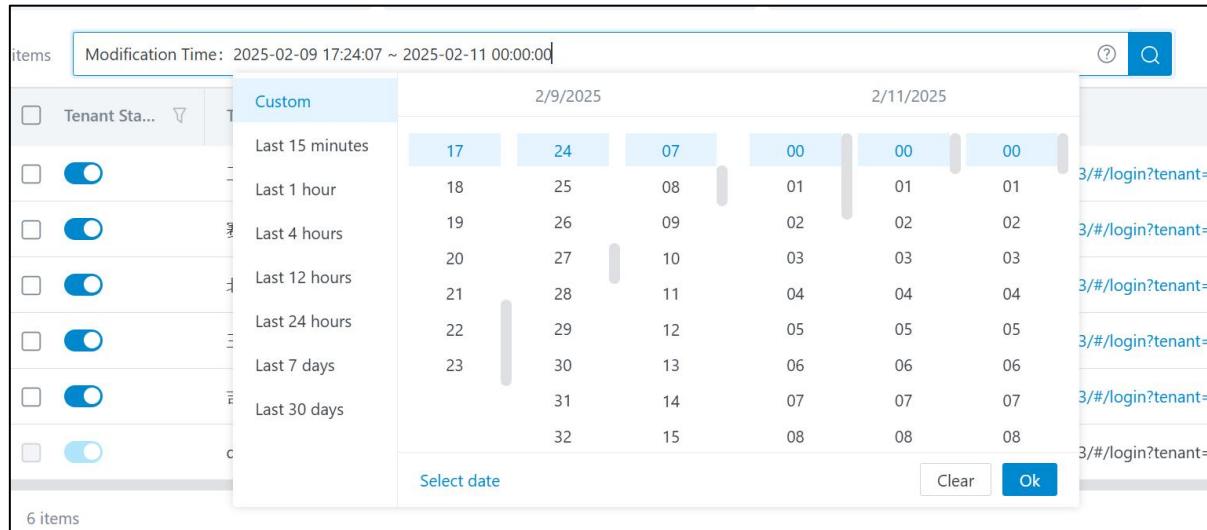
- Similarly, when you select the last 30 days, the system will set the interval to the first 30 x 24 hours of the time you searched (example time is 16:00:44) and highlight the time interval:



- If you need to specify a time node, you can choose the "Custom" option and first select the specified date:



- Click on 'Select Time' again and set the start and end times for two date nodes separately:



-

- If you need the same date node as the preset option and only want to change the start and end times of the date node, you can also choose to click on the corresponding date option and then click "Select Time" to change the start and end times of the two dates.

12.6.1.2. Manage Tenants

- Create New Tenant
- View/Modify Tenant Information
- View/Modify Quota Policy

12.6.1.2.1. Create New Tenant

Click "Create New Tenant," fill in the information, and save. The system will generate a random password. The newly created tenant will appear in the tenant list.

The screenshot shows the 'Create Tenant' dialog box. It has the following sections and fields:

- Tenant Information:**
 - Tenant ...: Click to Enter Tenant Name
 - Tenant ...: Official Test
 - Remarks: Click to Enter Remarks
- Primary Account Information**:
 - Primary A...: Click to Enter Primary Account Name
 - Name: Click to Enter Name
 - Email: Click to Enter Email
 - Mobile N... : Click to Enter Mobile Number
- Login Entry**:
 - Tenant Identifi...: Click to Enter Tenant Identifier
 - Account Login...: https://119.45.37.163:40443/#/login?tenant= !

At the bottom are two buttons: **Cancel** and **Save**.

Note:

- The primary account name will be used as the login account and cannot be changed after confirmation. It is usually the user's valid email and will also be the destination email for notifications.
- The tenant identifier is the identity assigned after purchasing the product service, used for login. It is a default code but can be changed to something more memorable, such as:
 - Tenant email (company email) or email suffix. For example, <xxx@mxtv.com>, use mxtv as the tenant identifier.
 - Tenant website or website abbreviation. For example, http://www.sdwa.com, use sdwa as the tenant identifier.
 - Initials of the tenant's full name. For example, for "Xindi Real Estate," use xddc as the tenant identifier.

- The login URL is the SaaS platform URL available to the tenant, defaulting to <https://cloud.qingteng.cn/#/login?tenant=> + tenant identifier.

12.6.1.2.2. View or Modify Tenant Information

- Click "Details" in the tenant list to view tenant details, including user information, primary account information, and login entry information.

This screenshot shows the 'Overview' section of the Sentry CWPP tenant management interface. At the top, it displays statistics: 'Total Tenants' (6), 'Enabled' (6), and 'Disabled' (0). Below this is a search bar with placeholder text 'Please select the filtering content'. A blue 'Create Tenant' button is located in the top right. The main area is a table with columns: Tenant Status, Tenant Name, Tenant ID, Primary Account, Account Login Address, Tenant Type, Authorization Status, Operation, and a timestamp column. The 'Operation' column contains a red-bordered 'Details' link for each row. The entire interface has a light gray background with white and blue UI elements.

- Click "Edit" to modify the information and save to update tenant details.

This screenshot shows a detailed view of a specific tenant. It includes a profile picture placeholder, a 'Reset Password' button, and an 'Edit' button. The 'Tenant Information' section contains fields: 'Tenant ...:' (Enabled), 'Tenant ...:' (Test), and 'Remarks: -'. Below this, there is a timestamp 'Creatio...: 2025-01-04 18:19:58'. The overall layout is clean with a white background and standard black text.

- Click "Reset Password" to reset the tenant password, and the tenant will receive a notification via email.

This screenshot is identical to the previous one, showing the tenant detail page. However, the 'Reset Password' button is highlighted with a red border, indicating it is the target of the current step in the process.

12.6.1.2.3. Modify Tenant Quota Policy

Quota policy refers to the number of CWPP product services allocated to the tenant and the product usage period.

Click "Quota Policy" under the operation column to view the quotas for each product.

The screenshot shows the Sentry CWPP Overview page. At the top, there are three boxes: 'Total Tenants' (6), 'Enabled' (6), and 'Disabled' (0). Below these are sections for filtering: 'Please select the filtering content' with a search icon, and a table with columns: Tenant Status, Tenant ID, Primary Account, Account Login Address, Tenant Type, Authorization status, Operation, and a date range from 'Test' to 'Expired'. A red box highlights the 'Quota Po...' button in the 'Operation' column.

Go to "Quota Policy" page and click "edit", you can change the useful quantity of Agent, begin time and useful duration.

The screenshot shows the Quota Policy page. It has tabs for 'Sentry' (selected) and 'Valid'. Under 'Console', it shows 'QT Multi-Tenant Console' with a start/end time of '2025-07-01 ~ 2025-08-15'. Under 'CWPP', it shows 'Host Security Posture' with a number of 20 and a start/end time of '2025-07-01 ~ 2025-08-15'. A red box highlights the 'Edit' button next to the 'Valid' tab.

Note:

- When entering the number of Agents, you can type the number or use the increment/decrement buttons, with a range of 0~999999. The number of Agents should match the purchase points in the customer order.

The screenshot shows the Quota Policy edit page. It lists products with their configurations: Host Security Posture (Quantity: 20, Time Period: 45 days, Start Time: 2025-07-01), Host Intrusion Detection and Response (Quantity: 20, Time Period: 45 days, Start Time: 2025-07-01), and Host Antivirus (Quantity: 20, Time Period: 45 days, Start Time: 2025-07-01). The 'Quantity' field for all three products is highlighted with a red box.

- When setting the usage duration, the default unit is "years," but you can change it to "months" or "days." Generally, the usage periods for all products should be consistent.

Product Name	Quantity	Time Period	Start Time
<input checked="" type="checkbox"/> Host Security Posture	20	45 day	2025-07-01
<input checked="" type="checkbox"/> Host Intrusion Detection and Response	20	45 day	2025-07-01
<input checked="" type="checkbox"/> Host Antivirus	20	45 day	2025-07-01

- The time cycle and start date should match the product validity period in the customer order.
- Click "Unify Start Time" to set the same start date for all products.
- The start time defaults to 00:00 on the start date, and the end time is 24:00 on the end date.
- All changes must be saved to take effect.

12.6.2. Probe Management

Tenants install Agent probes on hosts to continuously collect host process, port, and account information, monitor process and network connection behaviors in real-time, and communicate with the Server to execute tasks and proactively detect host issues. Probes can automatically adapt to virtual machines, physical machines, and cloud environments.

Probe management helps users manage Agents used by tenants, including:

- Tenant Agent task management
- Tenant Agent operation management
- Tenant Agent version management

12.6.2.1. Task Management

Management tasks are created by users to batch restart, upgrade, set operation levels, or enable/disable drivers for existing tenant Agents.

The task management page allows querying specific tasks, viewing task information, creating new management tasks, and viewing task execution records.

The task list displays summary information, including task status and execution progress.

12.6.2.1.1. Query Tasks

Click the search box to display search tags, which can be used for searches, including:

- Filter tasks by status (enabled or disabled)
- Search tasks by **keyword** in task name
- Search tasks by **complete** task ID
- Search tasks by task type
- Search tasks by probe type
- Filter tasks by whether they are scheduled
- Search tasks by creation time within a specified range
- Search tasks by operation time within a specified range
- Search tasks by **complete** operator name

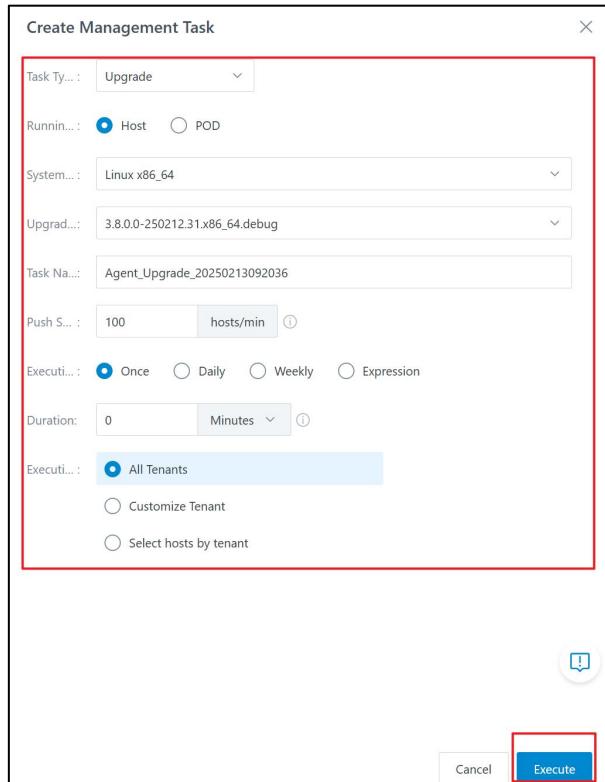
Click  to view the search box instructions.

12.6.2.1.2. Create New Management Task

Click "Create Management Task."

Agent Tasks												Create Management Task	
173 items		Please Select Filtering Content										<input type="checkbox"/> View only manually created tasks	Export All
<input type="checkbox"/>	Sta...	Task Name	Task Ty...	Probe T...	Total Execut...	Executed	Successes	Failures	Creation Time	Operation			
<input type="checkbox"/>	<input checked="" type="checkbox"/> Disab	auto_Agent_升级_20250115022052	Upgrade	Agent	1	1	1	0	2025-01-15 02:21:09	Execution Results	Delete		

Fill in the information and click "Execute" to activate the task.

**Note:**

- The execution scope must include at least one subject; otherwise, the task cannot be saved.
- The push speed refers to the rate at which the task is delivered to hosts, with a maximum of 600 hosts per minute. Entering 0 will use the system default configuration.
- The duration refers to the time the task runs at the set speed. Entering 0 or leaving it blank means no limit.

Upgrade Task Notes:

- Operation mode refers to the environment in which the task runs. You can choose to run it on hosts or containers.
- System type refers to the host system on which the task runs. A single task can only be set for one system type. Agent operation systems include: Linux x86_64, Linux aarch64, Windows x86_64; Pod operation systems include: Kubernetes x86, Kubernetes aarch64, Openshift x86, Openshift aarch64.
- Upgrade version refers to the target probe version for this task.

Set Operation Level Task Notes:

- Operation level refers to setting the Agent operation status to normal or disabled.

12.6.2.1.3. Delete Task

View task execution results of created managed tasks or delete tasks by clicking the options under the operation column.

Agent Tasks													Create Management Task			
<input type="checkbox"/> View only manually created tasks Export All																
<input type="checkbox"/>	Sta...	<input type="button" value="▼"/>	Task Name	<input type="button" value="▼"/>	Task Ty...	<input type="button" value="▼"/>	Probe T...	<input type="button" value="▼"/>	Total Execut...	Executed	Successes	Failures	Creation Time	<input type="button" value="▼"/>	Operation	<input type="button" value="▼"/>
<input type="checkbox"/>	<input checked="" type="radio"/>	Disable	auto_Agent_升级_20250115022052	Upgrade	Agent	1	1	1	0	2025-01-15 02:21:09	Execution Results	Delete				

Note:

- Deleting a task only removes the task record and does not affect the executed results.

12.6.2.1.4. Export Task Data

Select the tasks to export, click "Export All" to download the task data in CSV format. The file name will be "Task List_Date + Time," and each export will be recorded in the download center.

Agent Tasks													Create Management Task			
<input type="checkbox"/> View only manually created tasks Export All																
<input type="checkbox"/>	Sta...	<input type="button" value="▼"/>	Task Name	<input type="button" value="▼"/>	Task Ty...	<input type="button" value="▼"/>	Probe T...	<input type="button" value="▼"/>	Total Execut...	Executed	Successes	Failures	Creation Time	<input type="button" value="▼"/>	Operation	<input type="button" value="▼"/>

12.6.2.2. Operation Management

Operation management allows statistics on the distribution and current operation status of Agents across tenants.

The top of the page displays the total number of Agents for all tenants and the count by system type.



12.6.2.2.1. Query Tenant Agent Operation Status

Click the search box to display search tags, which can be used for queries, including:

- Query Agents by **keyword** in tenant name
- Query Agents by **complete** tenant ID
- Filter Agents by driver configuration status (enabled or disabled)
- Query Agents modified within a specified time range by operation time
- Query Agents modified by a specific user by last operator

12.6.2.2.2. Query Tenant Agent Version and Configuration Details

Select a tenant and click "View Details" to check the actual versions of all Agents, cluster component main programs, and various APPs of the tenant, as well as the differences in configuration versions, which is used to identify and troubleshoot problems. It supports quick download of logs and operation reports.

Version Detail																			
Agent	Cluster Agent																		
Please Select Filtering Content <input type="text"/> <input type="button" value="Search"/>																			
4 items																			
Agent ID	Host	Actual version of probe main...	Probe main program configu...	Is the main ...	Actual version of APP	APP configuration version	Operation												
6e ⁸ AZPU8SERPAPP	8.4 AZPU8SERPAPP	3.10.0.1-250619.86.x86_64	3.10.0.1-250619.86.x86_64	Yes	Asset Inventory: v2.16.0-20250521...	Asset Inventory: v2.16.0-20250521..	Download ... Download the operat...												
65 ⁸ AZPU8SERPDB	8.5 AZPU8SERPDB	3.10.0.1-250619.86.x86_64	3.10.0.1-250619.86.x86_64	Yes	Asset Inventory: v2.16.0-20250521...	Asset Inventory: v2.16.0-20250521..	Download ... Download the operat...												
98 AZTU8SERPAPP1	8.6 AZTU8SERPAPP1	3.10.0.1-250619.86.x86_64	3.10.0.1-250619.86.x86_64	Yes	Asset Inventory: v2.16.0-20250521...	Asset Inventory: v2.16.0-20250521..	Download ... Download the operat...												

12.6.2.2.3. Export Agent Operation Data

Select the Agent information to export, click "Export All" to download the data in CSV format. Each download will be recorded in the download center.

Agent Runtime											Create Management Task					
This feature counts the types and quantities of Agents for each tenant, with data updated every 5 minutes.																
Statistical Range		Number of Agents	Linux-Server	Windows-Server	Linux-PC	Windows-PC										
All Tenants		116/494	60/267	16/94	8/77	32/55										
87 items Please Select Filtering Content <input type="text"/> <input type="button" value="Search"/>																
<input type="checkbox"/> Tenant ... <input type="checkbox"/> Total Agents <input type="checkbox"/> Agent Online ... <input type="checkbox"/> Number of Ag... <input type="checkbox"/> Number of Ag... <input type="checkbox"/> Linux-Server <input type="checkbox"/> Linux-PC <input type="checkbox"/> Windows-Server <input type="checkbox"/> Windows-PC <input type="checkbox"/> Driver Conf... <input type="checkbox"/> <input type="button" value="Export All"/>																
<input type="checkbox"/> 0 <input type="checkbox"/> 0 <input type="checkbox"/> 0 <input type="checkbox"/> 0 <input type="checkbox"/> 0/0 <input type="checkbox"/> 0/0 <input type="checkbox"/> 0/0 <input type="checkbox"/> 0/0 <input type="checkbox"/> <input type="checkbox"/>																

12.6.2.2.4. Default Connection Address Configuration

The connection address is the network address where the Agent connects to the server. You can configure the connection address as needed to ensure normal communication between the Agent and the server.

Parameter description:

- **Basic information:** Filled in by default and does not support editing.
- **Connection method:**
 - **Communication protocol :** Choose based on the network protocol you are using.
 - **Direct connection:** The Agent directly establishes a network connection with the server, which is suitable for scenarios such as internal networks and networks without strict exit restrictions.
 - **Proxy:** The Agent relays traffic through the Socket5 proxy server and then connects to the server. It is suitable for scenarios where the real IP of the Agent needs to be hidden and the enterprise network restricts direct external connections.
- **Connection address:** The address for connecting to the server. Multiple addresses can be filled in. The newly installed Agent will randomly select an available address from the filling list to connect to the server.

Default Connection Address Configuration ×

Basic Information

*Config...:

Description...: Agent connection server default address configuration, effective for all tenants
80/100

Connection Method

Commu...: IPv4 IPv6

Connec...: Direct Connection Proxy

Connection address

The newly installed Agent will randomly select a valid address from the configuration list to connect to the server. Please ensure network connectivity before installation.

Connect IP/Domain name	Port
10.106.110.34	: 8443
10.106.110.55	: 8443
10.106.110.54	: 8443

+ Add Delete

Cancel Save

12.6.3. Outgoing

12.6.3.1. Outgoing Configuration

Provides a tenant-level toggle for the data egress feature, allowing administrators to enable it for specific tenants as needed. When the toggle is activated, tenants gain visibility and access to the data egress interface.

The screenshot shows a user interface for managing tenant configurations. At the top, there is a breadcrumb navigation: 'Outgoing Configuration'. Below this is a search bar labeled 'Please Select Filtering Content' and a magnifying glass icon. A tooltip explains the function of the outsourcing configuration switch: 'The outsourcing configuration switch controls whether the tenant as a whole can use the data outsourcing function, and whether the data outsourcing function interface is visible'. The main area displays a table with four rows, each representing a tenant. The columns are 'Tenant Name' and 'Tenant ID'. The 'Outsourced configuration' column contains a switch that is turned on for all tenants except 'ws5', where it is turned off. The tenant names listed are 'yhtest', 'testcreate', 'zhongyangli2', and 'ws5'.

Tenant Name	Tenant ID	Outsourced configuration
yhtest	01-XXXXXX	On
testcreate	01-XXXXXX	On
zhongyangli2	01-XXXXXX	On
ws5	01-XXXXXX	Off

13. Tools

13.1. Download Center

During the use of the product, all exported reports and documents are recorded in the Download Center for querying and downloading.

The screenshot shows a table with the following data:

File name	Task ID	File size	Task name	Source APP	Generation time	Status	Operation
Agent_log_2025021617...	67b3071bb743d800bdef7e5f	223.58KB	主机运行日志	Probe Management	2025-02-17 17:53:31	Success	Download Delete
[REDACTED]	[REDACTED]	7.17KB	[REDACTED]	Shift Left Security Manageme...	2025-02-17 14:36:26	Success	Download Delete

- Download records are displayed in reverse chronological order, including: file name, task ID, file size, task name, source APP, generation time, and status.
- You can search download records by file name or generation time.
- Click "Download" to save the file generated by this record to your local device.
- For download records that are no longer needed, click "Delete" to remove them.

13.2. Feedback Tool

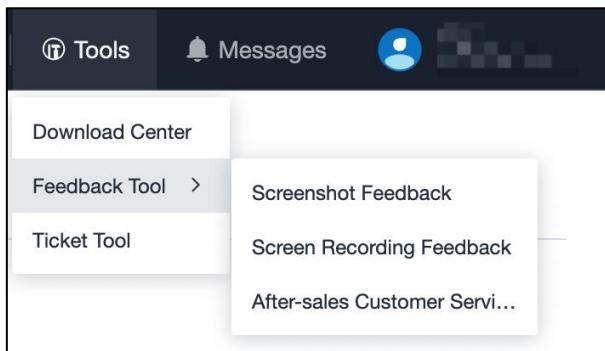
The feedback tool allows users to submit issues encountered during product usage to the product backend via screenshots or screen recordings, facilitating quick analysis and resolution of problems.

Alternatively, users can access the after-sales customer service channel for assistance.

Includes:

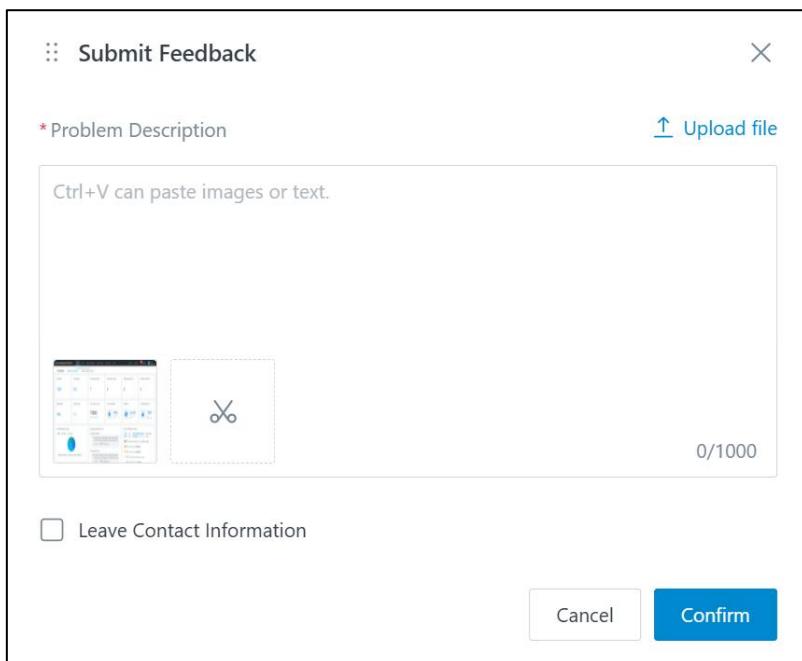
- Screenshot Feedback
- Screen Recording Feedback

- After-sales customer service



13.2.1. Screenshot Feedback

Screenshot feedback captures the current screen and generates feedback suggestions in the form of image attachments.



13.2.2. Screen Recording Feedback

Screen recording feedback captures the entire screen and generates feedback suggestions in the form of video attachments.

- Click "Screen Recording Feedback" to start recording, and a recording bar will appear at the

bottom of the screen.

- Click the "End Recording" in the recording bar to end the recording, and you can preview the recorded video.

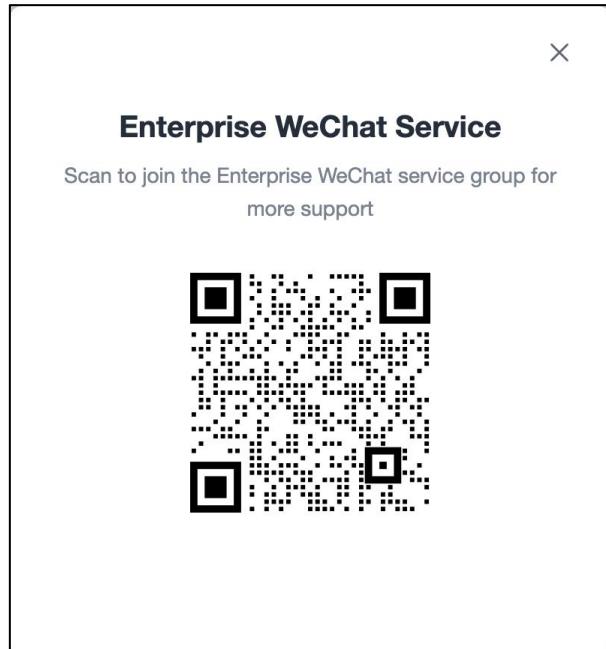


A screenshot of the "Preview Screen Recording" interface. It features a header with tabs like "Security Management Platform", "Home", "Asset", "Intrusion Detection", "Risk Discovery", "Compliance", and "More". Below the header are several data cards: "Total Agent" (1367), "Online Agent" (812), "Host New Pending..." (7), "Host New Process..." (0), "Host New Confirm..." (0), "Host New Ignored..." (0); "Offline Agent" (555), "Disabled Agent" (11), "Total number of risks" (70880, affected objects: 1077), "Host Vulnerability" (3885, affected host: 733); "Host Patch" (65597, affected host: 697), "Host Weak Passwords" (1398, affected objects: 542). On the left, there's a "Host TOP 10 Detection Type" pie chart and a "Host Real-time Detection List" section showing two entries from 2025-02-24. On the right, there's a "Host Top 10 Detection Devices" table with five rows. At the bottom, there's a playback bar showing "00:00 / 00:05", a "Cancel" button, and a "Next" button.

Click "Next" to submit feedback.

13.2.3. After-sales customer service

Scan the WeChat QR code to join the WeCom after-sales customer service group.



13.3. Ticket Tool

Click "Work Order Tool" to open a new browser tab, where a dynamic QR code will be displayed.

Scanning this QR code via the "Work Order System Robot" on the Feishu mobile app will automatically create a work order and populate it with the deployment configuration information of the current environment. This enables a more convenient and efficient way to create work orders on mobile phones.

Figure 1-1 Quick Work Order Creation by Scanning QR Code

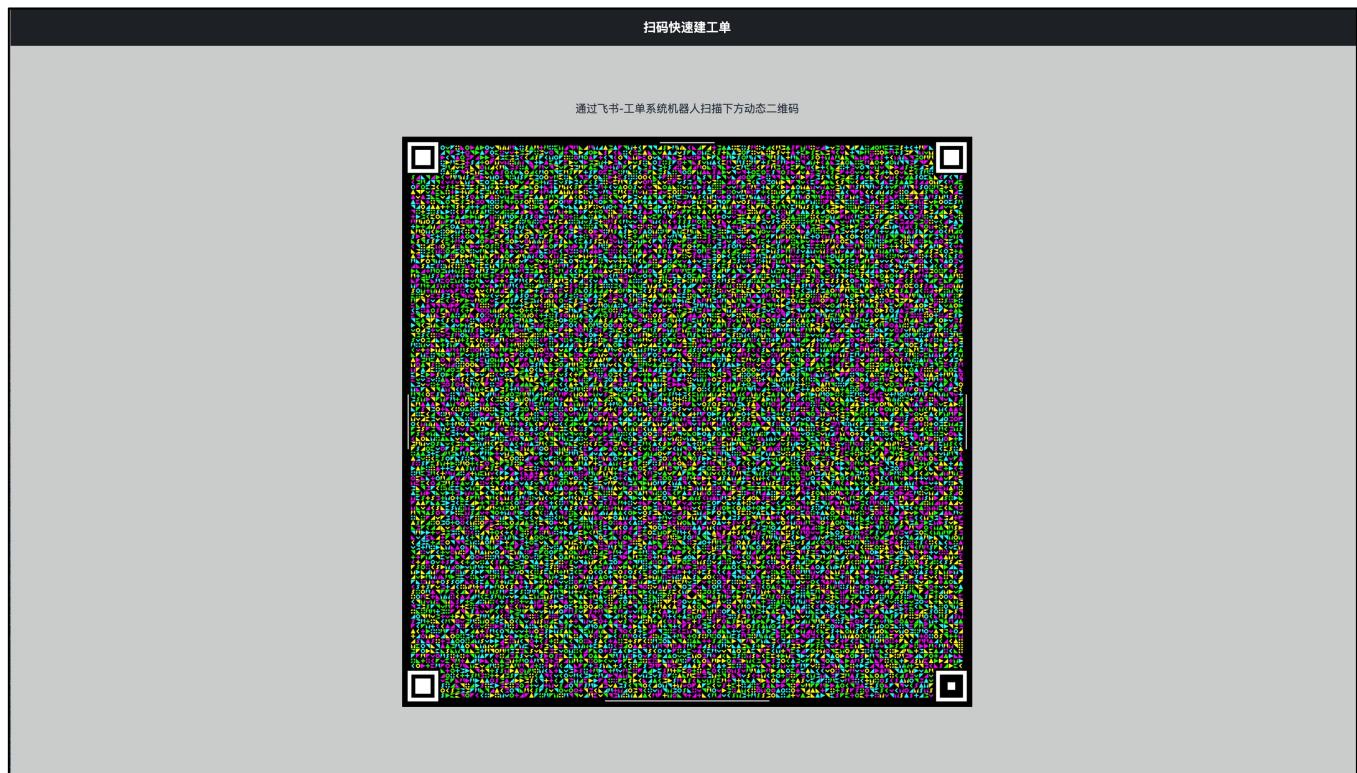


Figure 1-2 "Work Order System Robot" on Feishu Mobile App

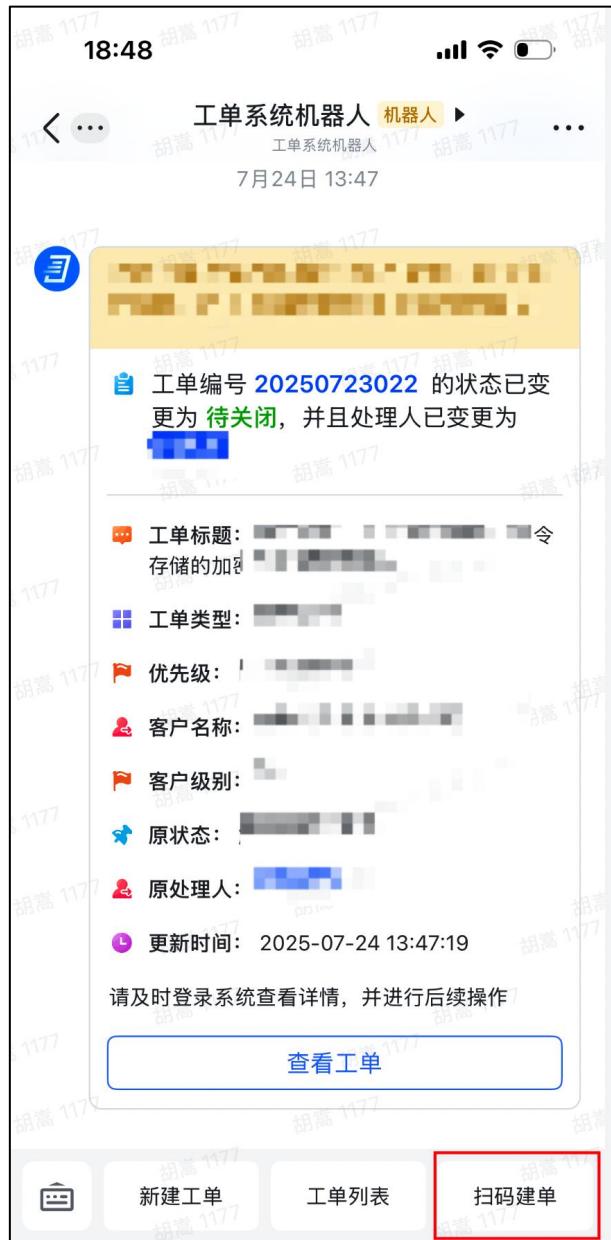


Figure 1-3 Automatic Work Order Creation

After scanning the QR code, the deployment ID will be automatically filled in, and the deployment configuration information will be obtained.



14. Message Center

The Message Center helps users view system notifications and configure message receiving methods, recipients, and group bots, enabling timely awareness of host security status.

14.1. Message Notification

14.1.1. Message List

In this list, users can select options to view all notifications, intrusion notifications, system notifications, and their details.

Steps:

- Click an option in the list, and the corresponding notifications will appear on the right.
- Click the title of each notification to enter the notification details page.

Message Notifications

The screenshot shows the 'Message Notifications' page. At the top, there's a message stating 'Display only the last 7 days of data by default'. Below this are several categories: 'All messages' (370), 'Intrusion No...' (358), 'Image Security', 'System Monit...' (11), and 'System Updat...'. A red box highlights the 'All messages' section and the list of notifications below it. The notifications table has columns for Title, Message Type, Message Sub-Type, and Send Time. Three notifications are listed, all from 'localhost.localdomain(10.108.108.28)' with different timestamps.

Title	Message Type	Message Sub-Type	Send Time
[高危]主机localhost.localdomain(10.108.108.28)于2025-02-24 10:15:02检测到自定义可疑进程告警:发...	Intrusion Notification	Suspicious Process Param...	2025-02-24 10:15:02
[高危]主机localhost.localdomain(10.108.108.28)于2025-02-24 08:35:37检测到自定义可疑进程告警:发...	Intrusion Notification	Suspicious Process Param...	2025-02-24 08:35:37
[高危]主机localhost.localdomain(10.108.108.28)于2025-02-24 08:30:21检测到自定义可疑进程告警:发...	Intrusion Notification	Suspicious Process Param...	2025-02-24 08:30:22

14.1.2. Message Search

14.1.2.1. Level Filter

Click the message level option to select the desired message level for filtering notifications.

The screenshot shows the same 'Message Notifications' page as before, but with a red box highlighting the 'Message Level: All' dropdown menu. This menu includes options for 'Urgent', 'Important', and 'Normal'.

14.1.2.2. General Query

Click the search box to display search tags. Notifications can be searched by title keywords, message subtype, and send time, including:

- Search notifications by title **keywords**
- Search notifications by selecting message subtypes
- Search notifications sent within a specified time range

The system provides usage instructions for the search box input method. Click

the  button to view.

Note:

- Query results under any search tag are sorted by message send time from newest to oldest.



14.2. Message Configuration

14.2.1. Receiving Configuration

14.2.1.1. Single Setting

Click  to expand the notification type, then click the "Edit" button to configure receiving settings.

Receive Configuration

⚠ SMS、Email Service not configured, cannot send SMS、Email message. Please contact the super administrator to configure related services

⚠ The default recipient's Phone Number、Email not configured, unable to receive Phone Number、Email message, please go to Account Center configure

Intrusion Notification

Batch Set Receiving Method Batch Set Receiver Batch Set Group Robot

Aggregated Alert

All medium-risk alarms will be sent an email for every 20 accumulated alarms

Receive Met...: Website Message、Group Robot Receiver: admin

Receive Gro...: -

14.2.1.2. Batch Setting

For multiple messages with the same receiving requirements, batch settings for receiving methods, recipients, and group bots can be configured. Notifications can also be enabled or disabled in bulk.

Click "Batch Set Receiving Method" for intrusion or system notifications to display a secondary page.

Fill in the information and click save to complete the settings.

Batch Set Receiving Method

* Select message sub-type

Aggregated Alert +49

Select Receiving Method

Website Message Email SMS Message Group Robot

Note:

- In-site messages refer to notifications within the product webpage.
- System notifications cannot be set to receive via in-site messages and email through group bots.

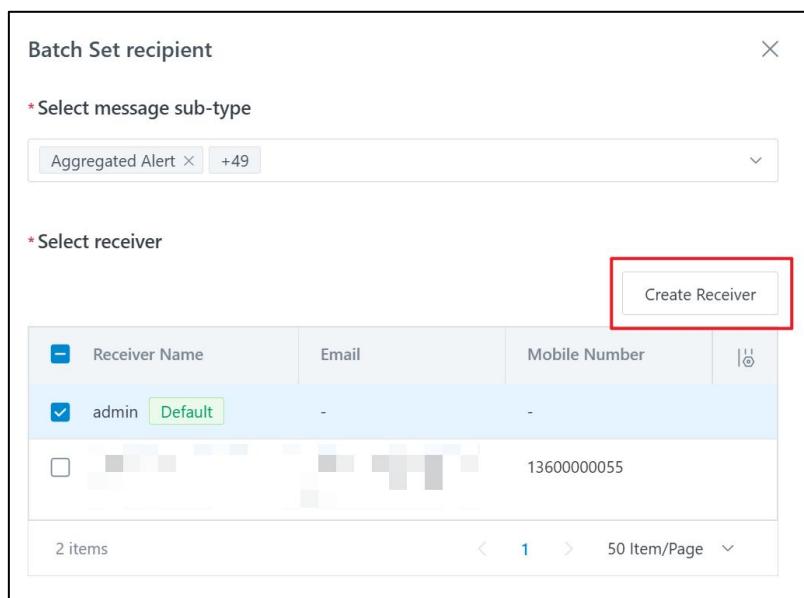
Click "Batch Set Recipients" for intrusion or system notifications to display a secondary page. Fill in the information and click save to complete the settings.

If all intrusion or system notifications are not needed, click to enable or disable the notifications.

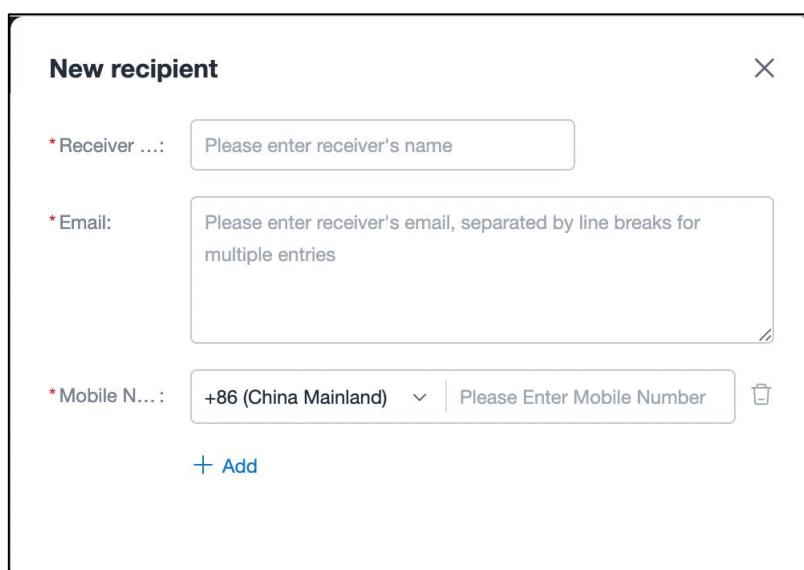
14.2.1.3. New Receiver

When the existing recipient list does not include the needed recipient, a new recipient can be created.

Method 1: Click "Batch Set Recipients," select the required message subtype, and click the "New Receiver" button.



Fill in the new recipient's name, phone, and mobile number, then click save. The new recipient will appear in the recipient list.



Method 2: On the recipient page, click "New Receiver," fill in the information, and save.

The screenshot shows a table with columns: 'Receiver Name', 'Email', 'Mobile Number', and 'Operation'. There are two items listed: 'admin' (with a 'Default' status). At the top, there is a message: 'The default recipient's phone/email is not configured, unable to receive SMS/email messages, please configure it'. Below the table are 'Edit' and 'Delete' buttons.

14.2.1.4. New Group Bot

When the existing group bot list does not include the needed group bot, a new group bot can be created.

Click the "Create Group Robot" button.

The dialog box has sections for 'Select message type' (set to 'Aggregated Alert') and 'Select Group Robot'. The 'Group Robot Name' field is empty. At the bottom right is a 'Create Group Robot' button.

Fill in the information, click test and save, and the new group bot will appear in the group bot list.

New group robot X

i Configuration belongs to this account only.

*Group Robot Name i

Please enter the group robot name, up to 50 characters

Select Platform

DingDing Lark Enterprise WeChat

*Webhook Address : Please enter the Webhook address

Key: Please enter the key i
The string displayed in the 'Signature' column of the robot security settings page

Proxy Config... : Direct socks5 proxy http proxy

Note:

- The system currently supports setting bots on Feishu, WeCom, and DingTalk.
- After configuring a bot in an account, the bot's configuration can only be viewed and edited by that account.
- Webhook is a service that controls user-authorized devices via HTTP calls, created and obtained by the user.
- The Webhook address key is typically used to ensure the security of Webhook requests, preventing unauthorized access. Users obtain it along with the address when creating a bot on the platform.
- Group robots support direct connection and proxy methods.
 - Proxy methods supported: socks5 proxy, http proxy.

14.2.2. Recipient Configuration

For existing recipients, click the "Edit" button to modify recipient information or the "Delete" button to delete the recipient. The logged-in account is automatically set as the default recipient and cannot be deleted.

The screenshot shows a 'Contact' section with a table containing two items: 'admin' and 'Default'. The 'Default' row has a red box around its 'Edit' and 'Delete' buttons. A yellow warning bar at the top states: '⚠ The default recipient's phone/email is not configured, unable to receive SMS/email messages, please configure it'.

Receiver Name	Email	Mobile Number	Operation
admin			Edit Delete

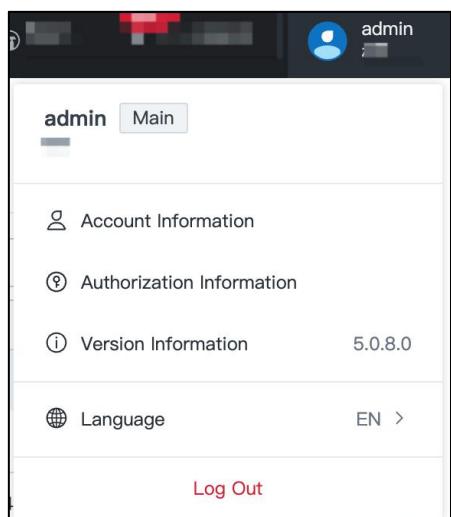
14.2.3. Group Bot Configuration

For existing group bots, click the "Edit" button to modify group bot information or the "Delete" button to delete the group bot. All group bots can be deleted.

15. Personal Center

The personal center displays personal account information, authorization information, version information, and can perform system management, including:

- account information
- Authorization Information
- Version information
- Language switching



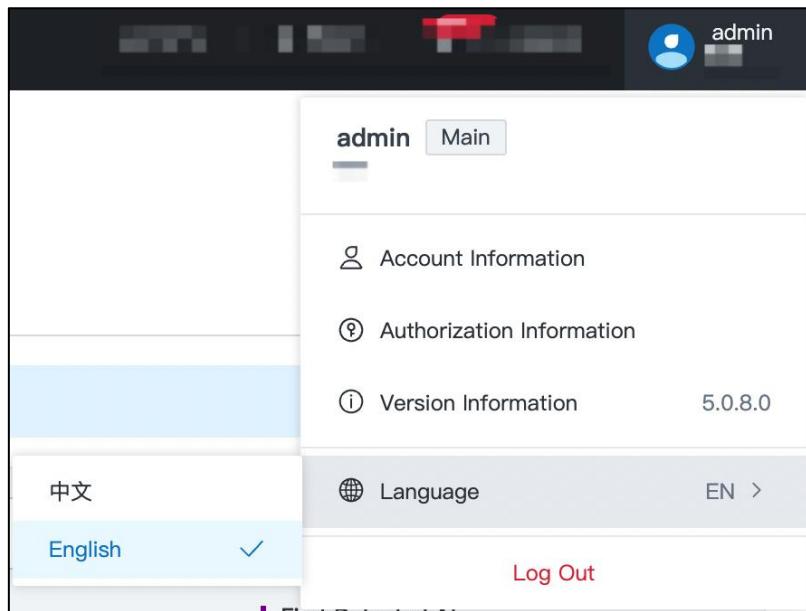
15.1. Authorization Information

Display detailed authorization information for the current login account, including: activated products, product features, Agent authorization points, and authorization validity period

License Info		
Sentry	Valid	
Sentry	Valid	
Console		
QT Multi-Tenant Console		Start and end time: 2024-05-17 ~ 2027-05-17
CWPP		
Host Security Posture	Number: 2000	Start and end time: 2024-05-17 ~ 2027-05-17
Host Intrusion Detection and Response	Number: 2000	Start and end time: 2024-05-17 ~ 2027-05-17

15.2. Language Switch

The language can switch to Chinese and English.



15.3. Account Information

Display detailed information of the currently logged in account, including:

- Basic Information: Name, Email, Mobile Number, Company Name, Department, Position, Account Creation Time, Recent Login Time, Remarks
- Password setting: Change password
- Authentication login information: account authentication, two factor verification
- Permission information: account role, user group to which it belongs

Account Information

Avatar



Basic Information

Name:	Admin	Email:	-
Mobile Nu... :	-	Company N...:	-
Department:	-	Position:	-
Account Cr... :	2024-12-09 17:15:10	Last Login T...:	2025-02-13 09:41:12 Login History
Remarks:	-		

15.4. Version information

Can view the full product name and version number.

