Cloud Workload Protection Platform

Operation Guide

Product Documentation

©2013-2022 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

©2013-2022 Tencent Cloud. All rights reserved.

Operation Guide
Security Dashboard

Last updated：2023-12-26 16:20:21

This document describes how to use Security Dashboard.

Overview

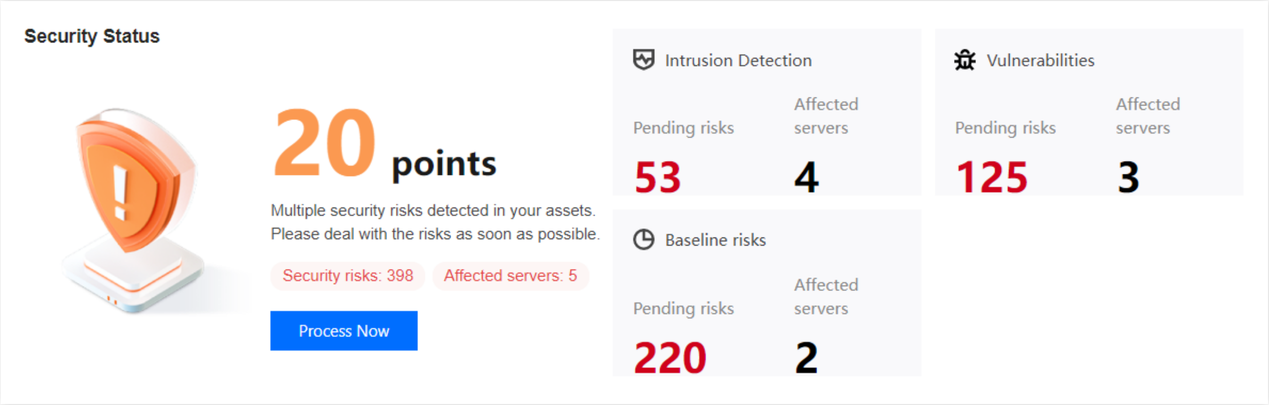
As the homepage of Cloud Workload Protection Platform (CWPP), Security Dashboard displays security score, pending risks, security protection status, risk trend, and new security events; pushes security notices to keep you updated with the latest threat intelligence of CWPP; provides documentation and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

Operation Guide

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

Security Status

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



Security Status

20 points

Multiple security risks detected in your assets. Please deal with the risks as soon as possible.

Security risks: 398 Affected servers: 5

Intrusion Detection: Pending risks 53, Affected servers 4

Vulnerabilities: Pending risks 125, Affected servers 3

Baseline risks: Pending risks 220, Affected servers 2

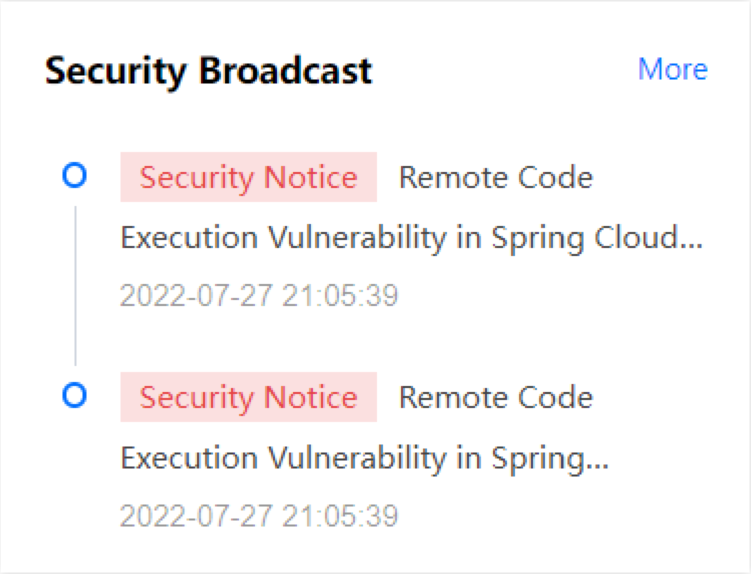
Security score: The score is calculated based on the number of security events and their threat level. For more information about the scoring rules, see Security Score Overview.

©2013-2022 Tencent Cloud. All rights reserved.

Risk information: It contains three categories of information: detected intrusions, vulnerability risks, and baseline risks, and shows the number of pending risks and the number of affected servers.
Intrusion Detection: Malicious File Scan, Unusual Login, Password Cracking, Malicious Requests, Reverse Shell, Local Privilege Escalation, and High-Risk Commands.
Vulnerability Risks: Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities in Vulnerability Management.
Baseline Risks: Only risks in Baseline Management.

Security Intelligence

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



Security Broadcast

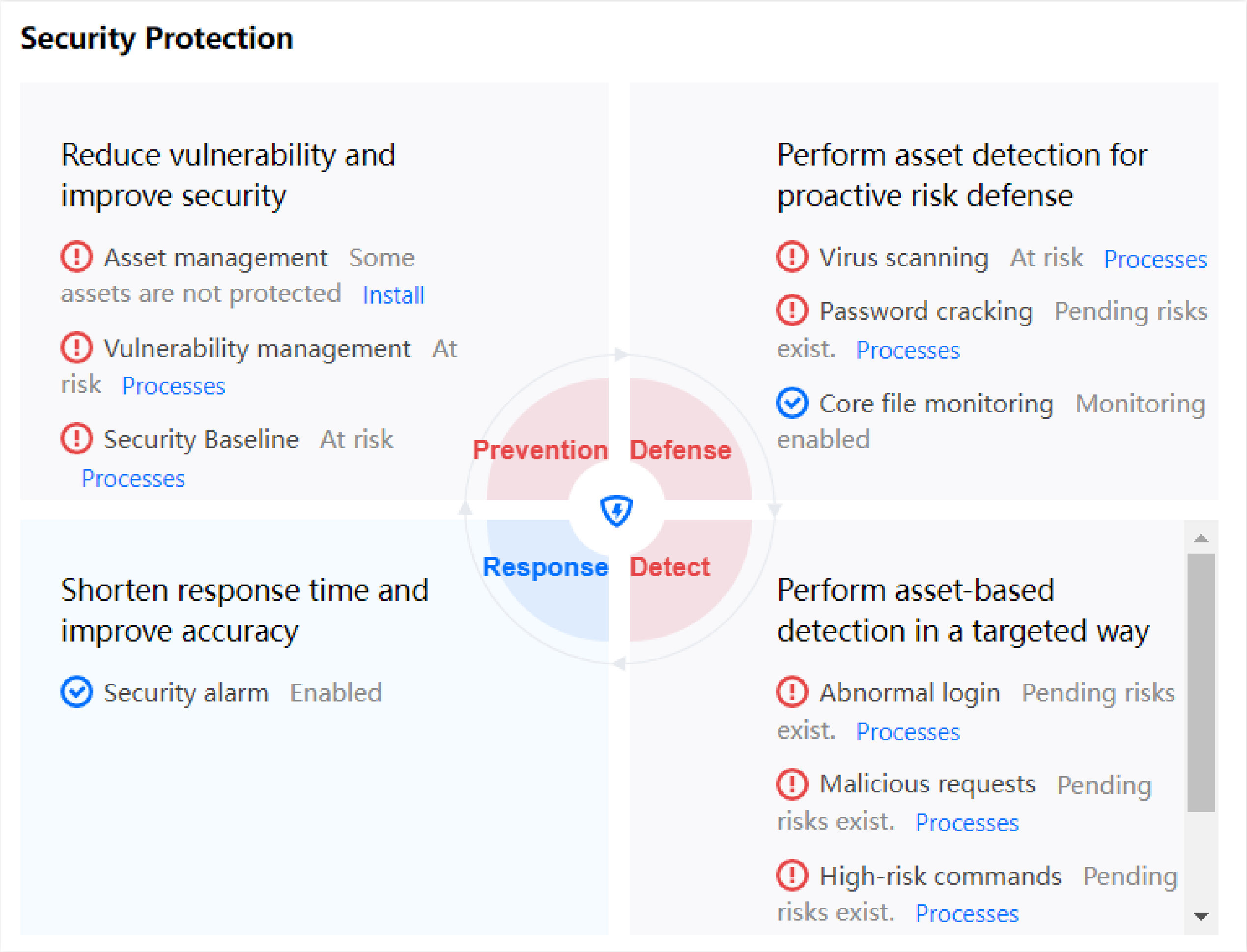
- Security Notice Remote Code Execution Vulnerability in Spring Cloud...
  2022-07-27 21:05:39
- Security Notice Remote Code Execution Vulnerability in Spring...
  2022-07-27 21:05:39

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

Security Protection

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

©2013-2022 Tencent Cloud. All rights reserved.



Security Protection

Reduce vulnerability and improve security

Asset management Some assets are not protected Install

Vulnerability management At risk Processes

Security Baseline At risk Processes

Perform asset detection for proactive risk defense

Virus scanning At risk Processes

Password cracking Pending risks exist. Processes

Core file monitoring Monitoring enabled

Shorten response time and improve accuracy

Security alarm Enabled

Perform asset-based detection in a targeted way

Abnormal login Pending risks exist. Processes

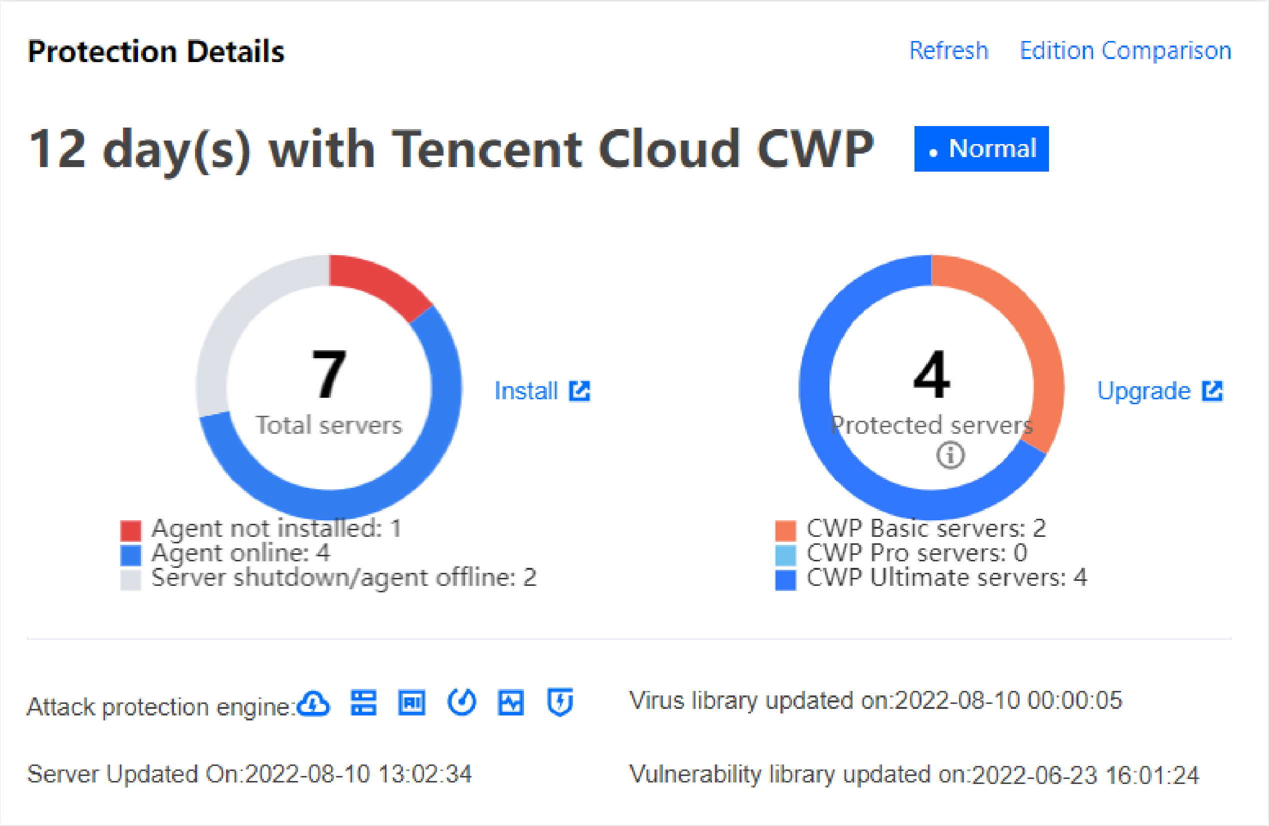
Malicious requests Pending risks exist. Processes

High-risk commands Pending risks exist. Processes

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

Protection Details

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



Protection Details

12 day(s) with Tencent Cloud CWP • Normal

7 Total servers

- 🟥 Agent not installed: 1
- 🟦 Agent online: 4
- ⬜ Server shutdown/agent offline: 2

4 Protected servers

- 🟧 CWP Basic servers: 2
- 🟦 CWP Pro servers: 0
- 🟦 CWP Ultimate servers: 4

Attack protection engine:

Virus library updated on:2022-08-10 00:00:05

Server Updated On:2022-08-10 13:02:34

Vulnerability library updated on:2022-06-23 16:01:24

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

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

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

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

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

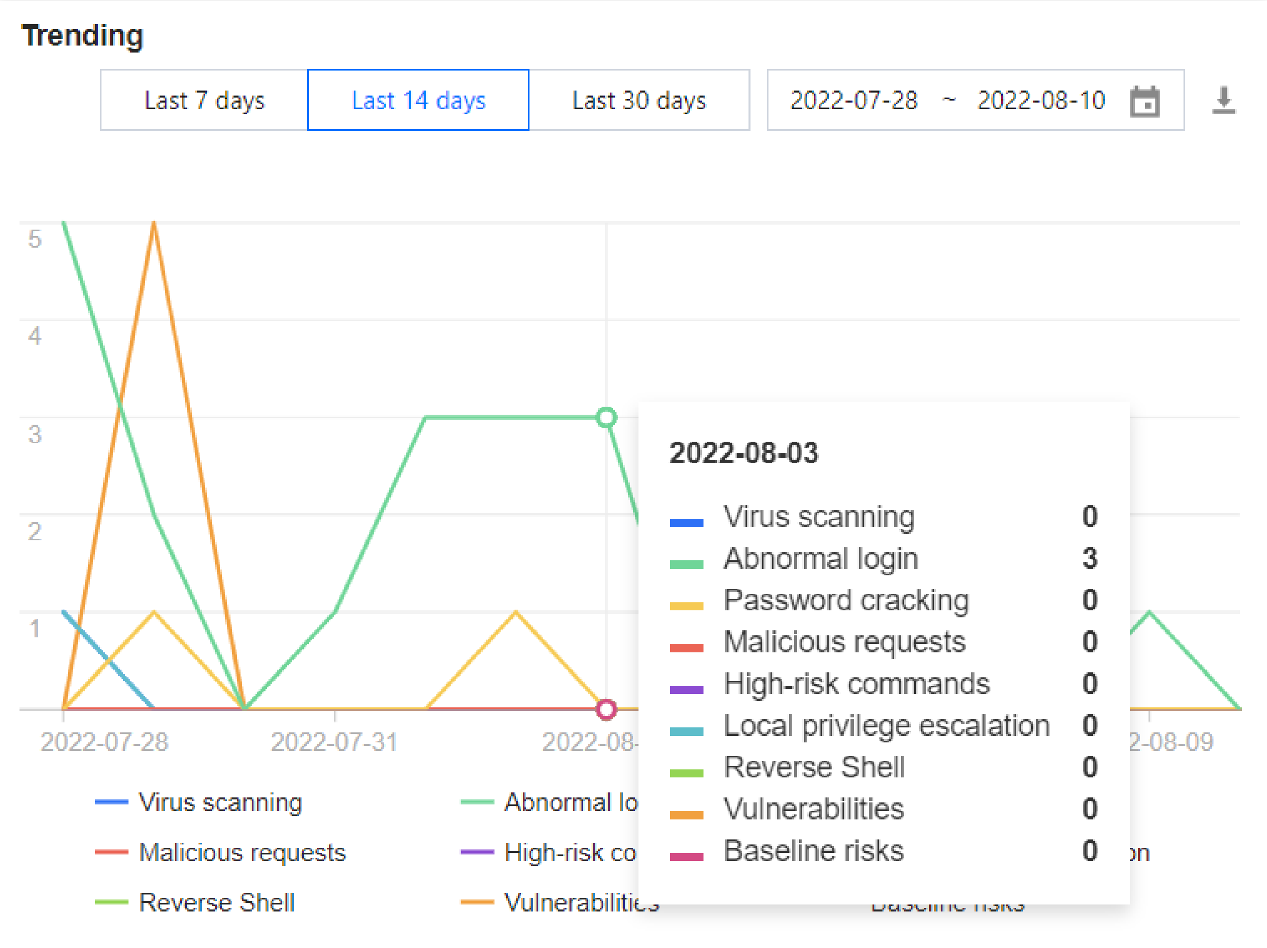
Server update time: Click **Update now** in the upper right corner to manually update the server list.

Vulnerability Library Update Time: From time to time.

Risk Trend

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

©2013-2022 Tencent Cloud. All rights reserved.



2022-08-03

Virus scanning	0
Abnormal login	3
Password cracking	0
Malicious requests	0
High-risk commands	0
Local privilege escalation	0
Reverse Shell	0
Vulnerabilities	0
Baseline risks	0

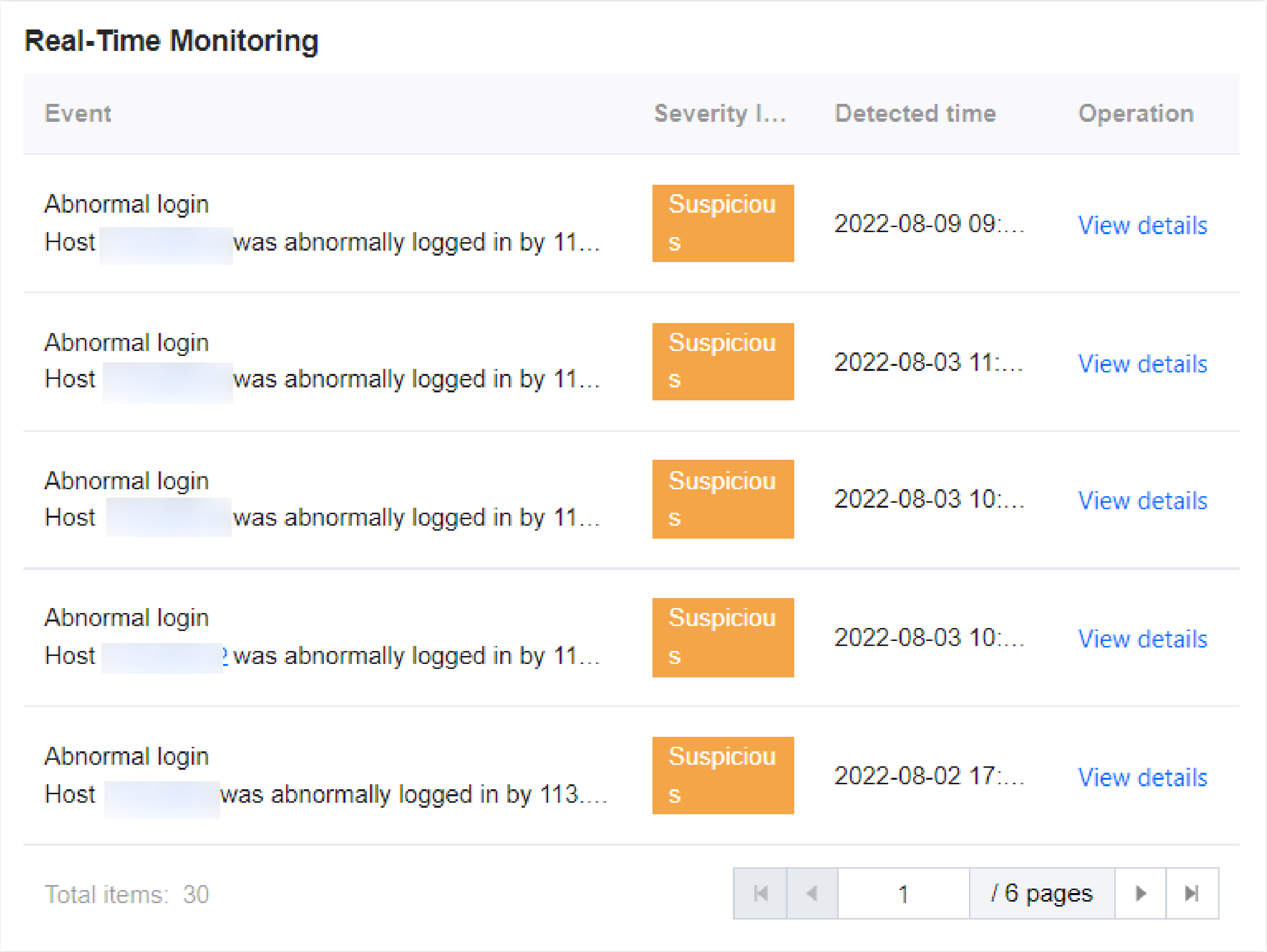
You can view the risk statistics for the last 7 days, the last 14 days, the last 30 days, or a custom date range. Click **Download** to export the risk statistics for the selected date range.

Note:

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

Real-time monitoring

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



Real-Time Monitoring

Event	Severity l...	Detected time	Operation
Abnormal login Host [redacted] was abnormally logged in by 11...	Suspicious	2022-08-09 09:...	View details
Abnormal login Host [redacted] was abnormally logged in by 11...	Suspicious	2022-08-03 11:...	View details
Abnormal login Host [redacted] was abnormally logged in by 11...	Suspicious	2022-08-03 10:...	View details
Abnormal login Host [redacted] was abnormally logged in by 11...	Suspicious	2022-08-03 10:...	View details
Abnormal login Host [redacted] was abnormally logged in by 113....	Suspicious	2022-08-02 17:...	View details

Total items: 30

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

©2013-2022 Tencent Cloud. All rights reserved.

Asset Overview

Last updated：2024-03-11 15:19:24

This document describes how to use Assets Dashboard.

Overview

Assets Dashboard presents the data of your servers and 15 key asset fingerprint items in a visualized form to give you a picture of your server assets.

Important Notes

Asset Dashboard is available to all Tencent Cloud users. The collected asset fingerprint items vary with different CWPP editions, so the data displayed in Assets Dashboard varies with the editions, as shown below.

CWPP Edition	Supported Asset Types
CWPP Basic (free)	N/A
CWPP Pro	10 items: Resource Monitoring, Accounts, Ports, Processes, Software Applications, Databases, Web Applications, Web Services, Web Frameworks, and Websites
CWPP Ultimate	15 items: Resource Monitoring, Accounts, Ports, Processes, Software Applications, Databases, Web Applications, Web Services, Web Frameworks, Websites, JAR Archive Files, Startup Services, Scheduled Tasks, Environment Variables, and Kernel Modules

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

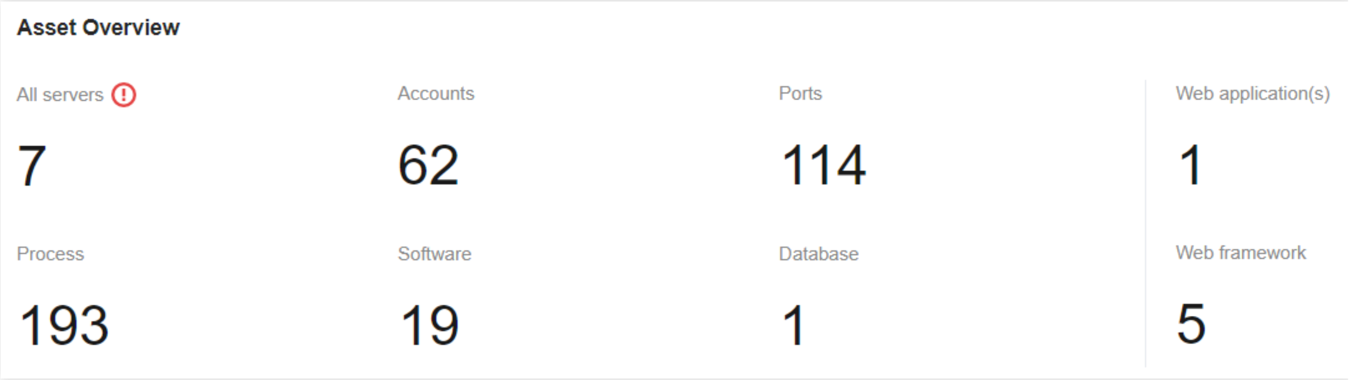
Operation Guide

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

Assets Dashboard

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

©2013-2022 Tencent Cloud. All rights reserved.



Asset Overview

All servers ⓘ
7

Accounts
62

Ports
114

Web application(s)
1

Process
193

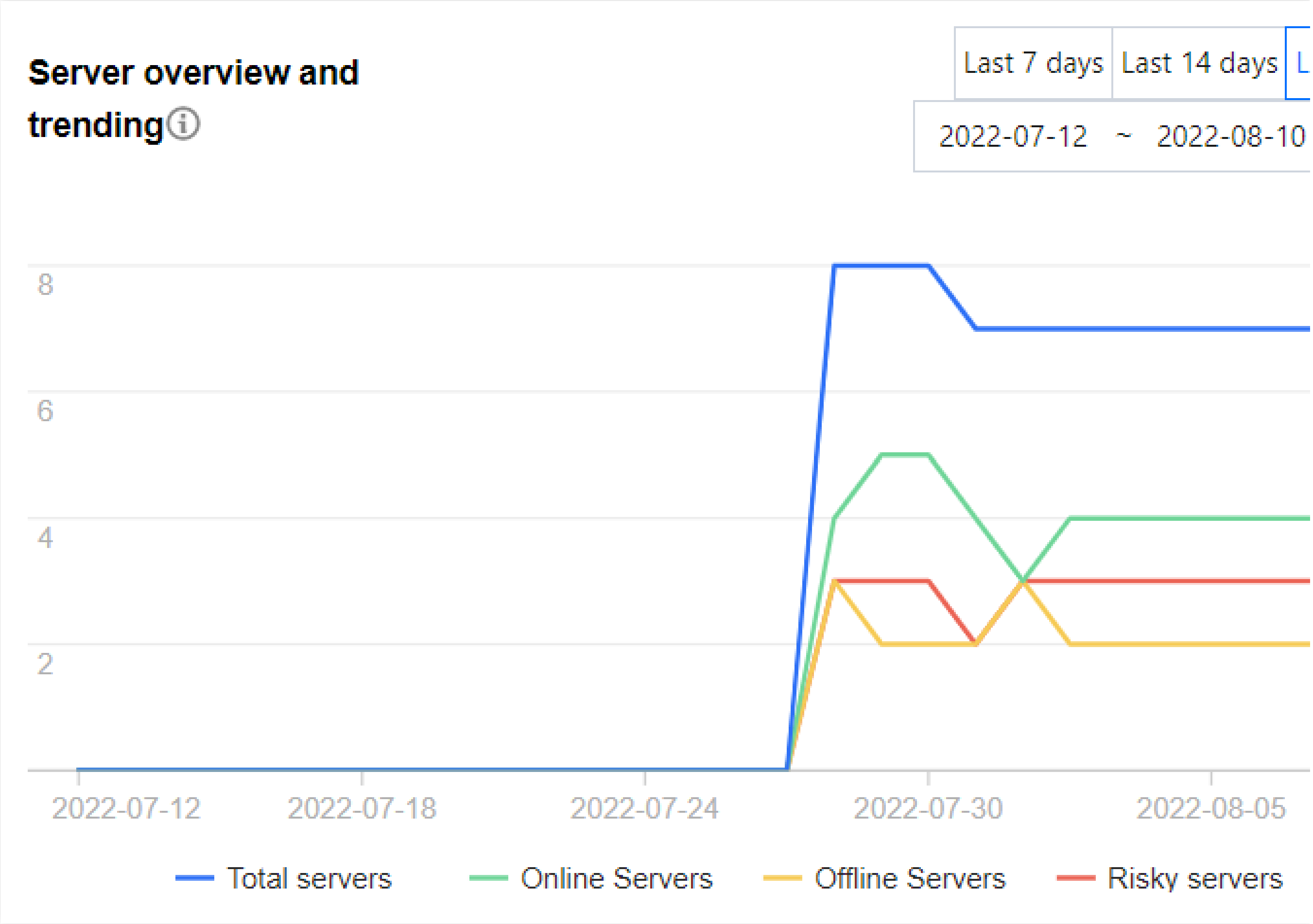
Software
19

Database
1

Web framework
5

Server Overview and Trending

Server Trend shows the changes in the total number of servers, the number of online servers, the number of offline servers, and the number of risky servers in a line graph.



Server overview and trending

2022-07-12 ~ 2022-08-10

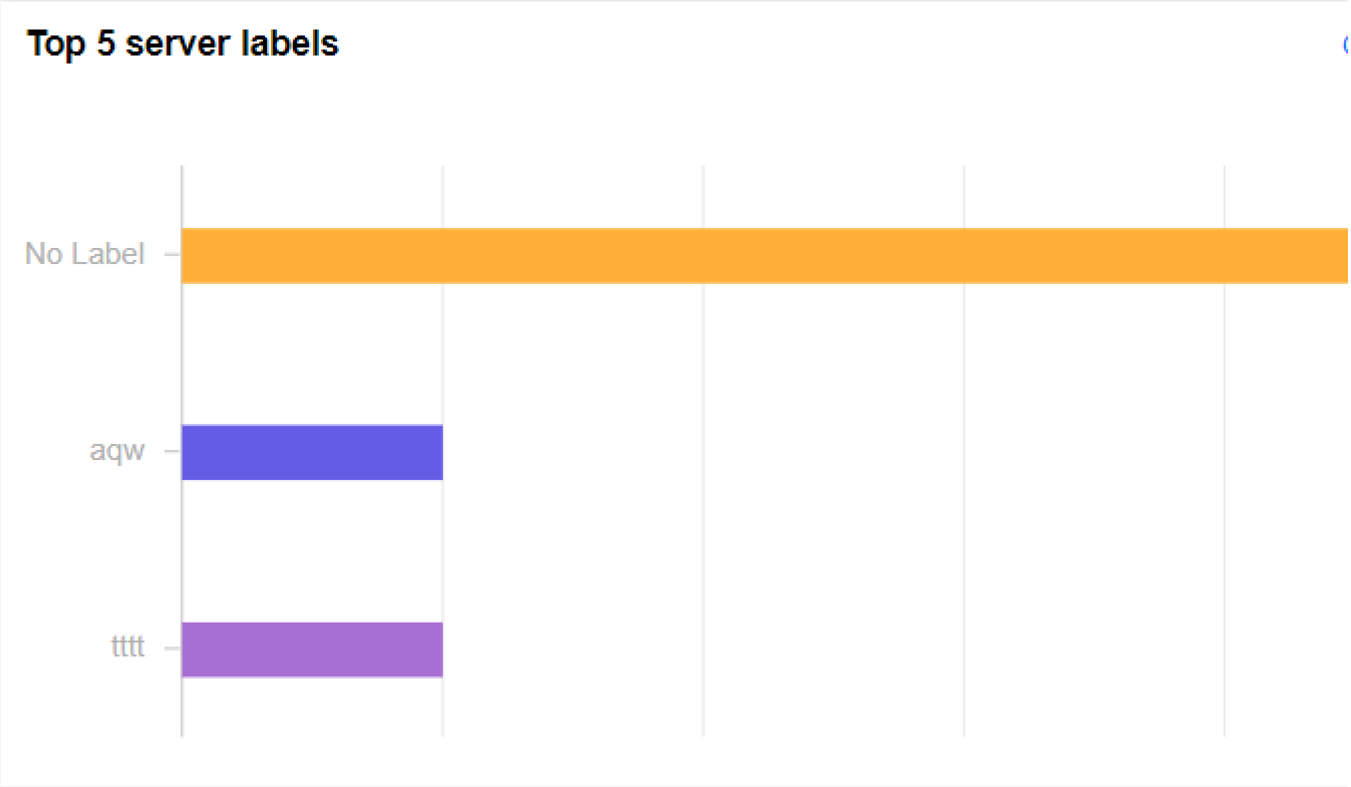
You can view the statistics for the past 7/14/30 days, or a custom period . The data generated 3 months ago is not displayed.

Click **Download** to export the daily data of the server for the selected date range.

©2013-2022 Tencent Cloud. All rights reserved.

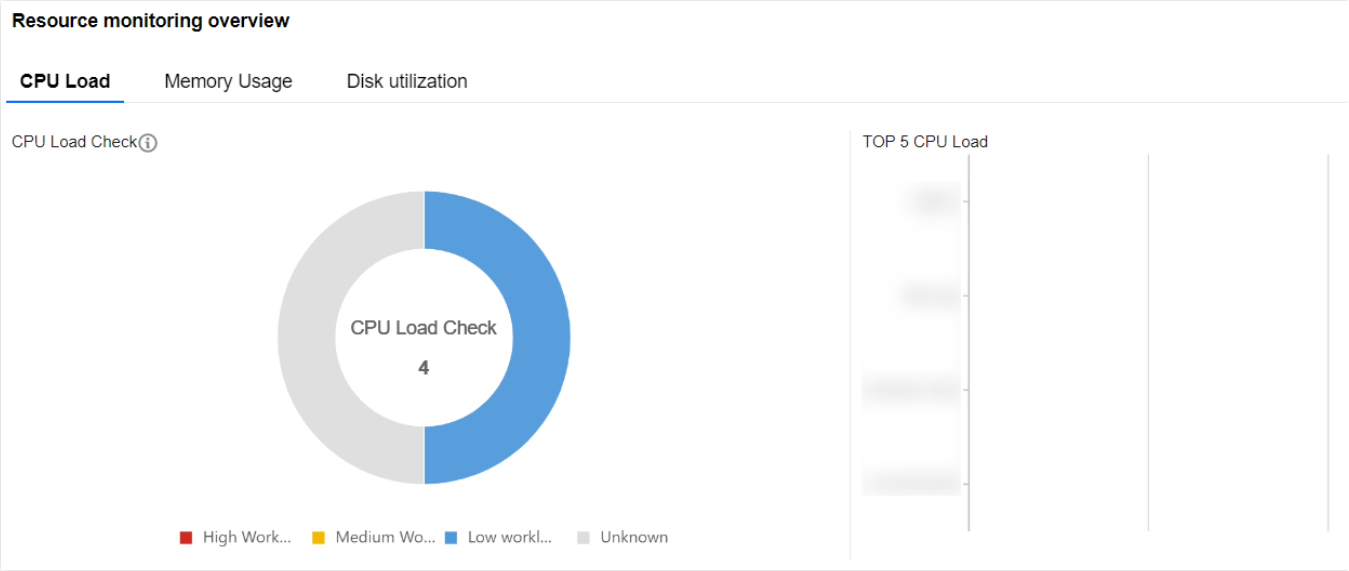
Top 5 Server Tags

The **Top 5 Server Tags** section displays the top 5 most used server tags in CWPP.



Resource Monitoring

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

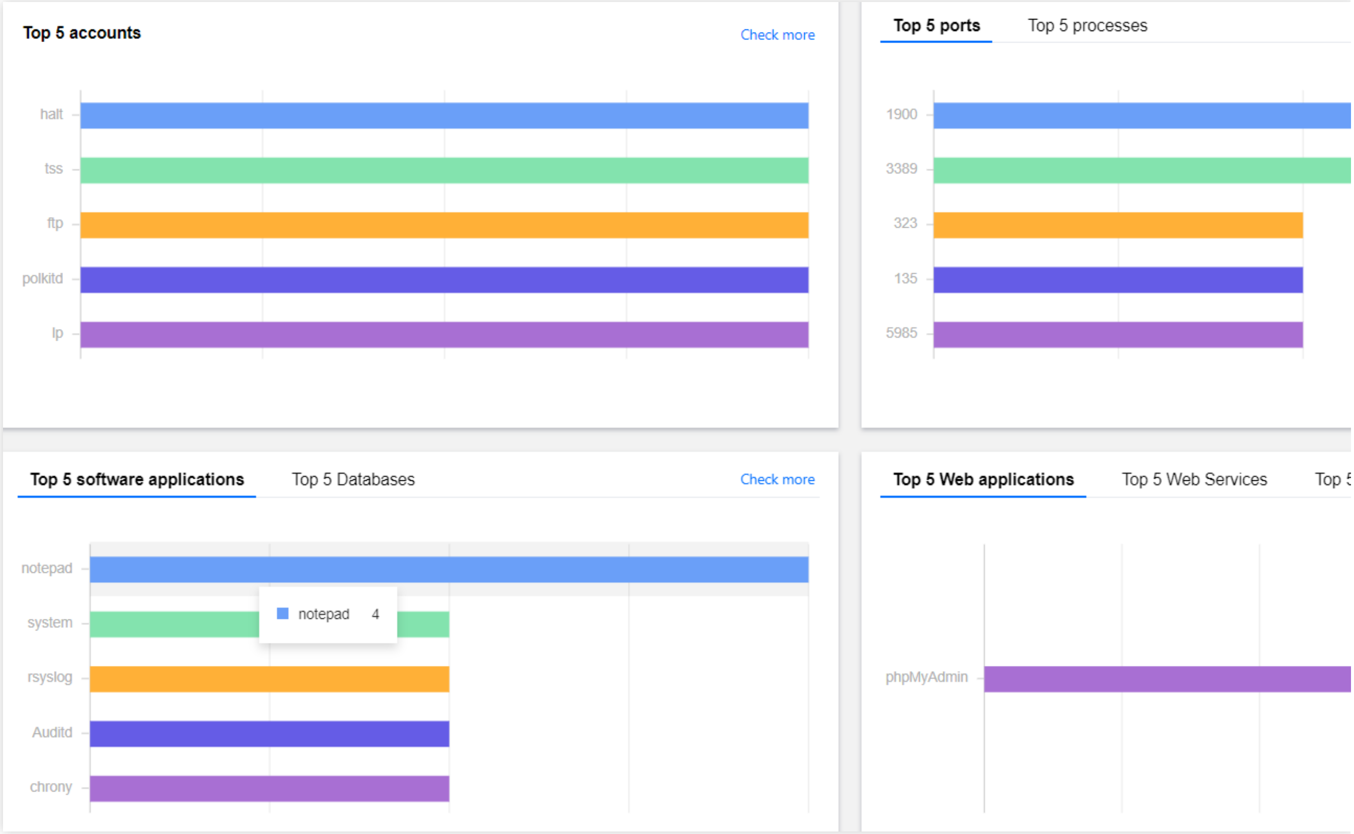


Note:

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

TOP 5 Asset Fingerprints

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



Server List

Last updated：2023-12-26 16:20:59

This document describes how to use Server List.

Overview

Server List presents the information of all servers on which CWPP is installed to give you a full picture of the security of your assets.

Important Notes

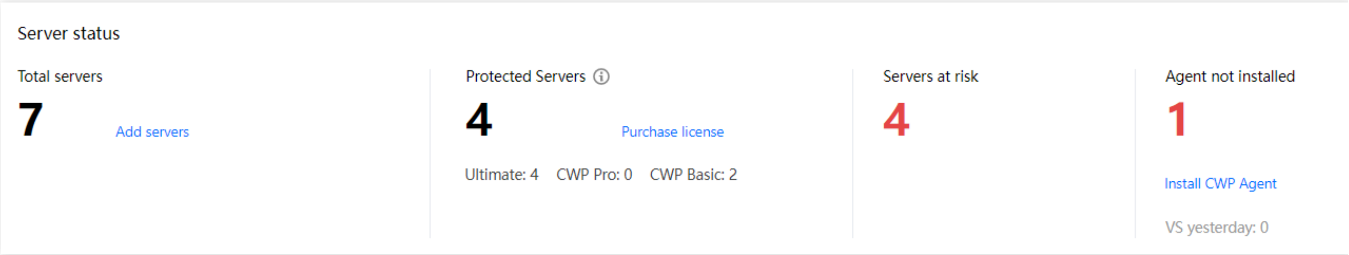
Server List is available to all Tencent Cloud users.
Servers running in a hybrid cloud environment are supported.
Tencent Cloud: CVMs, Lighthouse servers, and ECMs.
Non-Tencent Cloud: Third-party cloud servers and IDC servers.

Operation Guide

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

Server Status

The **Host Status** section shows the total number of servers, the number of protected servers, the number of servers at risk, the number of unprotected servers, and the number of servers with licenses that are about to expire.



Server status

Total servers 7

Protected Servers 4

Ultimate: 4 CWP Pro: 0 CWP Basic: 2

Servers at risk 4

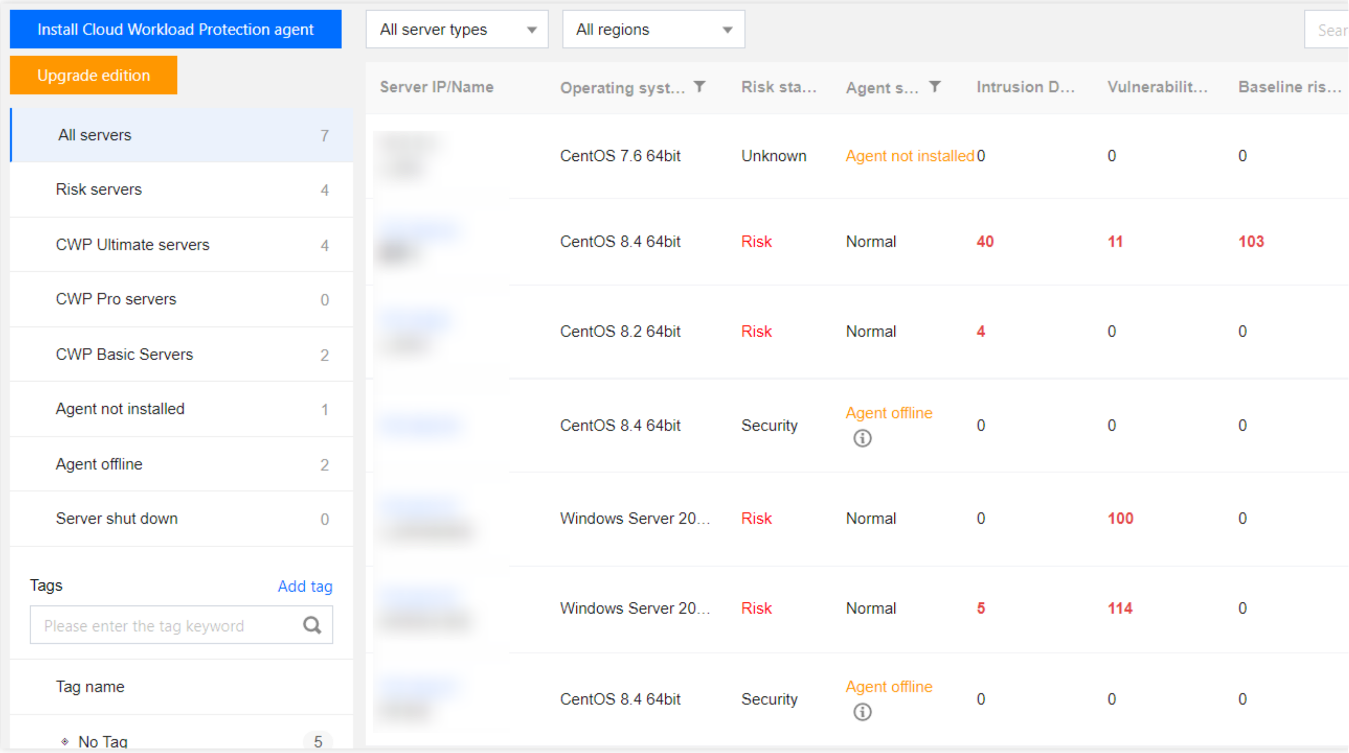
Agent not installed 1

VS yesterday: 0

Click **Connect to Multiple Servers** or **Install CWPP Agent** to open the CWPP Agent installation guide pop-up window. For more information, see Installing Agent.
Click **Purchase License** to go to the CWPP Purchase Page to purchase licenses.

Server List

Server List shows the servers on which CWPP is installed, as well as the statistics of the servers by risk and tag.



All servers	7
Risk servers	4
CWP Ultimate servers	4
CWP Pro servers	0
CWP Basic Servers	2
Agent not installed	1
Agent offline	2
Server shut down	0

Tags Add tag

Please enter the tag keyword

Tag name	
No Tag	5

Server IP/Name	Operating syst...	Risk sta...	Agent s...	Intrusion D...	Vulnerabilit...	Baseline ris...
[redacted]	CentOS 7.6 64bit	Unknown	Agent not installed	0	0	0
[redacted]	CentOS 8.4 64bit	Risk	Normal	40	11	103
[redacted]	CentOS 8.2 64bit	Risk	Normal	4	0	0
[redacted]	CentOS 8.4 64bit	Security	Agent offline ⓘ	0	0	0
[redacted]	Windows Server 20...	Risk	Normal	0	100	0
[redacted]	Windows Server 20...	Risk	Normal	5	114	0
[redacted]	CentOS 8.4 64bit	Security	Agent offline ⓘ	0	0	0

Click **Install CWPP Agent** to open the CWPP agent installation guide pop-up window. For more information, see Installing Agent.

Click **Upgrade Edition** to go to License Management, where you can bind the purchased licenses to your servers and upgrade CWPP edition for the servers.

Click **the navigation pane on the right** to filter servers by risk and tag:

Dimension	Description
Risk	All Servers: All servers on which CWPP is installed. Servers at Risk: The servers where intrusion risks, vulnerability risks, baseline risks, or network risks were detected. Servers with CWPP Ultimate: The servers bound to a CWPP Ultimate license. Servers with CWPP Pro: The servers bound to a CWPP Pro license. Servers with CWPP Basic: The servers that have CWPP Agent installed but are not bound to a license. Server Without CWPP Agent (unprotected): The servers on which CWPP Agent is not installed. Offline: The servers where CWPP is offline. Shutdown: The servers that have been shut down (only applicable to Tencent Cloud servers).
Tag	You can set tags to be associated with servers. The servers are listed by tag here.

You can filter servers by availability zone, region, server IP, and server name.

Click **Refresh** to get the latest server list.

Click **Download** to export the list of filtered servers.

Field description:

Server IP/Name: Private IP and name of the server.

Operating System: Windows, Linux (CentOS, Debian, Gentoo, RedHat, Ubuntu, TencentOS, CoreOS, FreeBSD, SUSE)

Risk Status: Safe, Risky, and Unknown.

Protection Status

Unprotected: CWPP agent is not installed on the server.

Protected: CWPP agent is installed on the server and is online.

Offline: CWPP agent is installed on the server but is offline.

Shutdown: The server is shut down (only applicable to Tencent Cloud servers).

Risk Count

Intrusion Detection: The total of risks detected in Malicious File Scan, Anti-Unusual Login, Anti-Password Cracking, Anti-Malicious Requests, High-risk Command Detection, Anti-Local Privilege Escalation, and Anti-Reverse Shell.

Vulnerability Risks: The total number of Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities.

Baseline Risks: The total number of failed baseline check items.

Network Risks: The total number of attack events detected.

Tags: The tags to be associated with servers (a tag can be associated with multiple servers).

Operation

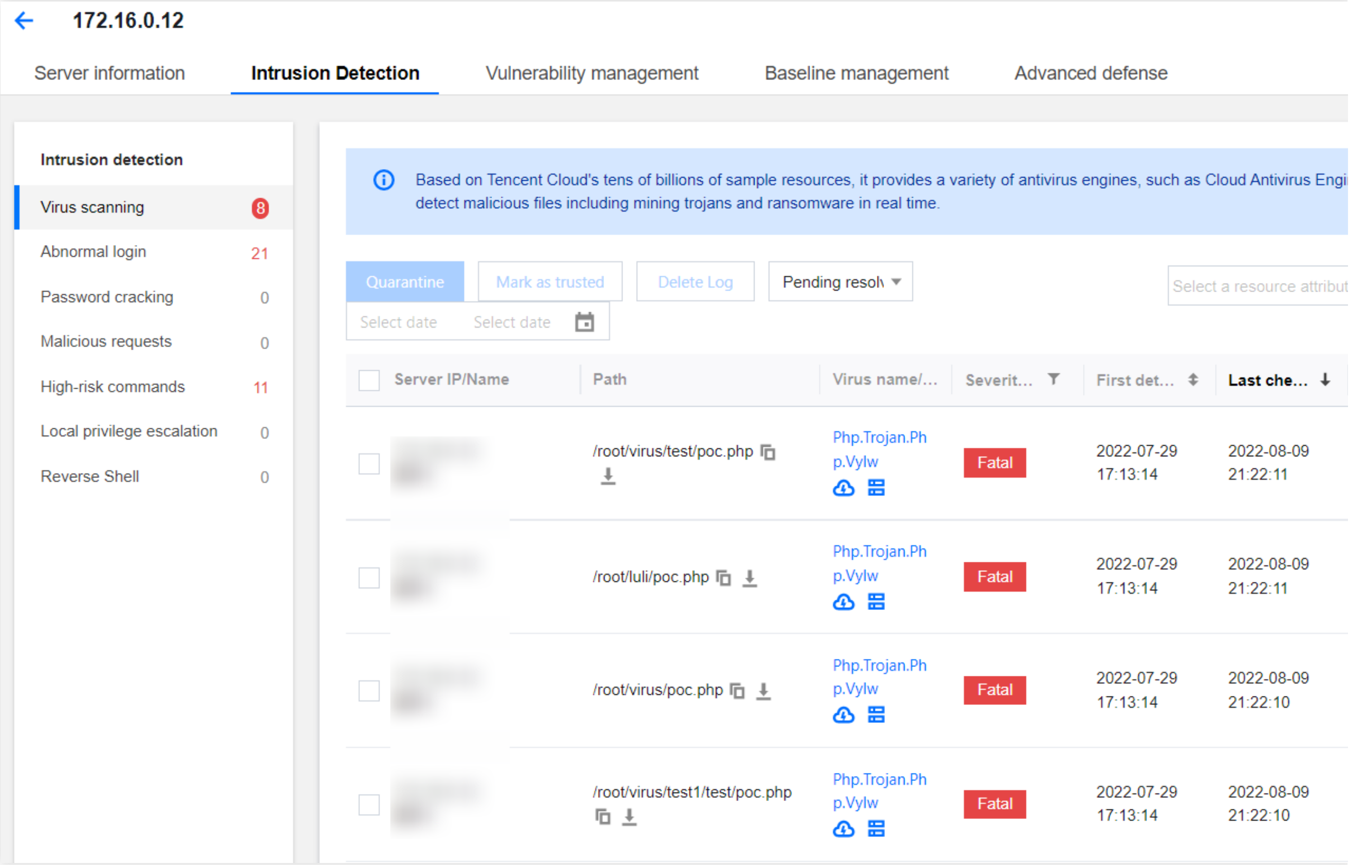
License Management: Click to go to License Management.

Reinstall: Click to open the CWPP Agent installation guide pop-up window. For more information, see Installing Agent.

Uninstall: Open a confirmation pop-up window. It takes about 10 minutes to synchronize CWPP agent status after you confirm uninstallation. (For a server bound to a CWPP license, it must be unbound from the license before CWPP can be uninstalled.)

Server Details

Server Details shows the risk information of the server.



Based on Tencent Cloud's tens of billions of sample resources, it provides a variety of antivirus engines, such as Cloud Antivirus Engi
detect malicious files including mining trojans and ransomware in real time.

Server IP/Name	Path	Virus name/...	Severit...	First det...	Last che...
	/root/virus/test/poc.php	Php.Trojan.Php.Vylw	Fatal	2022-07-29 17:13:14	2022-08-09 21:22:11
	/root/luli/poc.php	Php.Trojan.Php.Vylw	Fatal	2022-07-29 17:13:14	2022-08-09 21:22:11
	/root/virus/poc.php	Php.Trojan.Php.Vylw	Fatal	2022-07-29 17:13:14	2022-08-09 21:22:10
	/root/virus/test1/test/poc.php	Php.Trojan.Php.Vylw	Fatal	2022-07-29 17:13:14	2022-08-09 21:22:10

Asset Fingerprint

Last updated：2023-12-26 16:21:11

This document describes how to use the Asset Fingerprints feature.

Overview

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

Quota and Limits

You have at lease one server bound with a CWPP Pro/Ultimate license.

The following lists the asset fingerprint items collected in different CWPP editions.

CWPP Edition	Supported Asset Types
CWPP Basic (free)	N/A
CWPP Pro	10 types of assets: Resource Monitoring, Accounts, Ports, Processes, Software Applications, Databases, Web Applications, Web Services, Web Frameworks, and Websites
CWPP Ultimate	15 types of assets: Resource Monitoring, Accounts, Ports, Processes, Software Applications, Databases, Web Applications, Web Services, Web Frameworks, Websites, JAR Archive Files, Startup Services, Scheduled Tasks, Environment Variables, and Kernel Modules

Note:

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

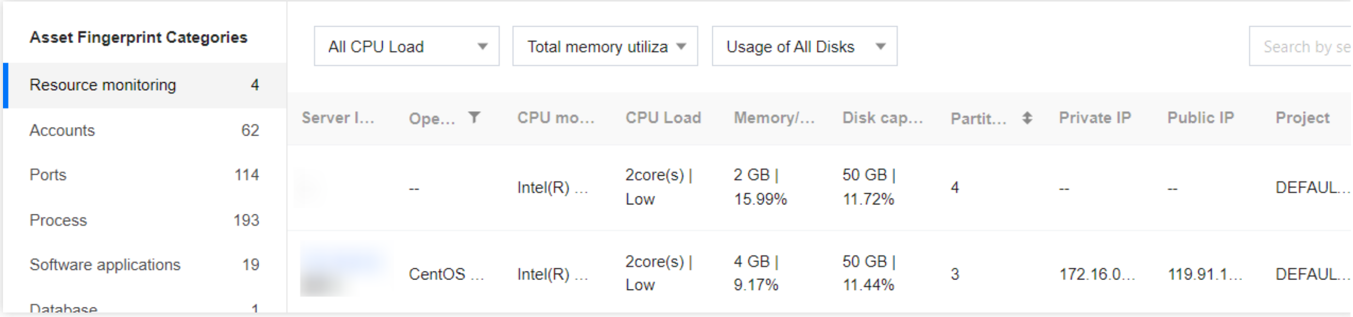
Operation Guide

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

©2013-2022 Tencent Cloud. All rights reserved.

Resource Monitoring

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



Asset Fingerprint Categories

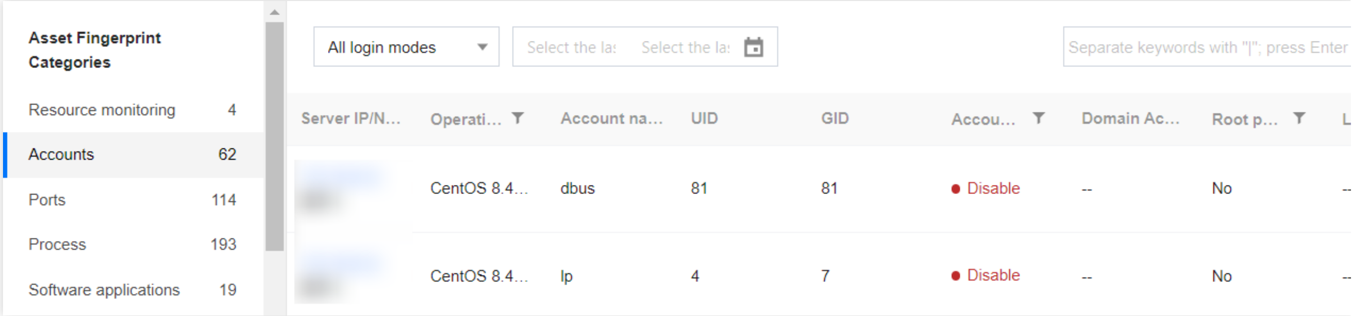
Resource monitoring	4
Accounts	62
Ports	114
Process	193
Software applications	19
Database	1

All CPU Load ▾ | Total memory utiliza ▾ | Usage of All Disks ▾ | Search by se

Server I...	Ope...	CPU mo...	CPU Load	Memory/...	Disk cap...	Partit...	Private IP	Public IP	Project
[redacted]	--	Intel(R) ...	2core(s) | Low	2 GB | 15.99%	50 GB | 11.72%	4	--	--	DEFAUL...
[redacted]	CentOS ...	Intel(R) ...	2core(s) | Low	4 GB | 9.17%	50 GB | 11.44%	3	172.16.0...	119.91.1...	DEFAUL...

Accounts

Collects the data of all accounts on the server.



Asset Fingerprint Categories

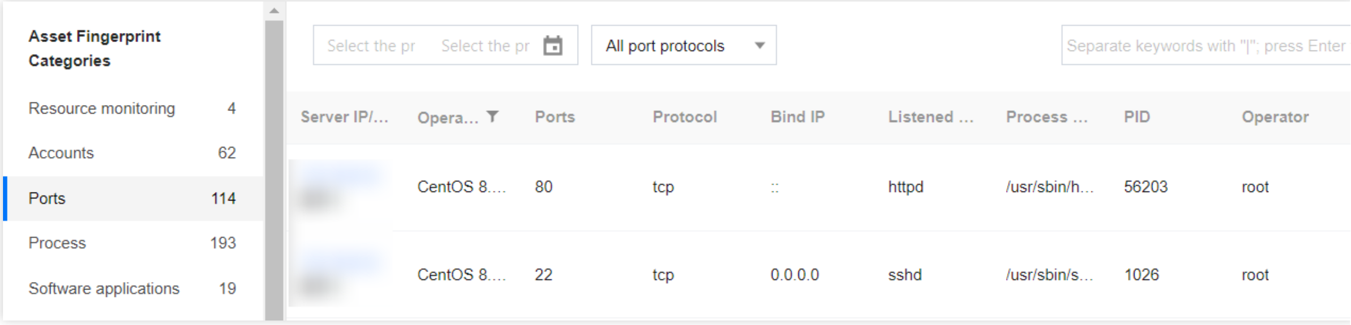
Resource monitoring	4
Accounts	62
Ports	114
Process	193
Software applications	19

All login modes ▾ | Select the la: Select the la: | Separate keywords with "|"; press Enter

Server IP/N...	Operati...	Account na...	UID	GID	Accou...	Domain Ac...	Root p...	L
[redacted]	CentOS 8.4...	dbus	81	81	● Disable	--	No	--
[redacted]	CentOS 8.4...	lp	4	7	● Disable	--	No	--

Ports

Collects the data of all used ports of the server.



Asset Fingerprint Categories

Resource monitoring	4
Accounts	62
Ports	114
Process	193
Software applications	19

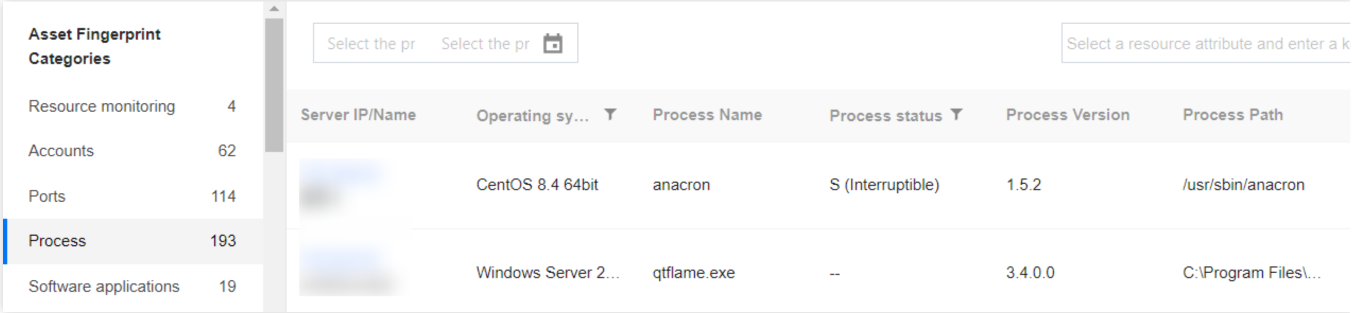
Select the pr Select the pr | All port protocols ▾ | Separate keywords with "|"; press Enter

Server IP/...	Opera...	Ports	Protocol	Bind IP	Listened ...	Process ...	PID	Operator
[redacted]	CentOS 8....	80	tcp	::	httpd	/usr/sbin/h...	56203	root
[redacted]	CentOS 8....	22	tcp	0.0.0.0	sshd	/usr/sbin/s...	1026	root

Processes

Collects the data of all processes running on the server.

©2013-2022 Tencent Cloud. All rights reserved.



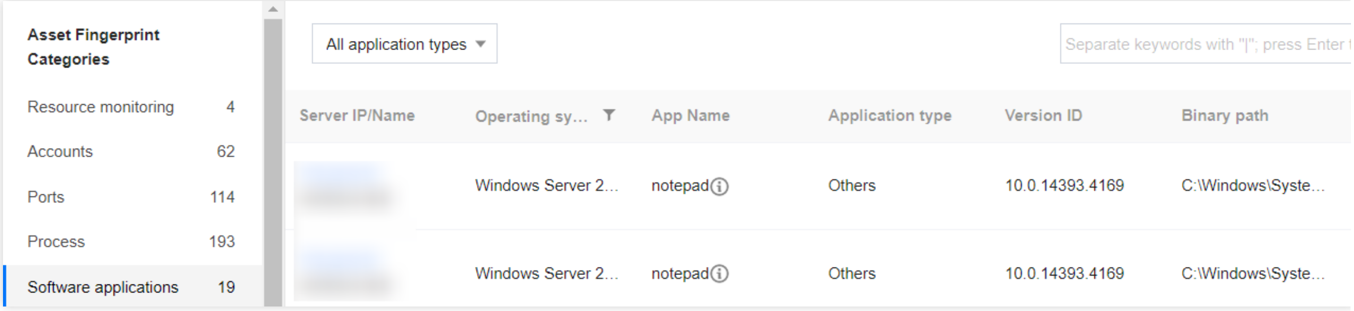
Asset Fingerprint Categories

Resource monitoring	4
Accounts	62
Ports	114
Process	193
Software applications	19

Server IP/Name	Operating sy...	Process Name	Process status	Process Version	Process Path
[redacted]	CentOS 8.4 64bit	anacron	S (Interruptible)	1.5.2	/usr/sbin/anacron
[redacted]	Windows Server 2...	qtflame.exe	--	3.4.0.0	C:\Program Files\...

Software Applications

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



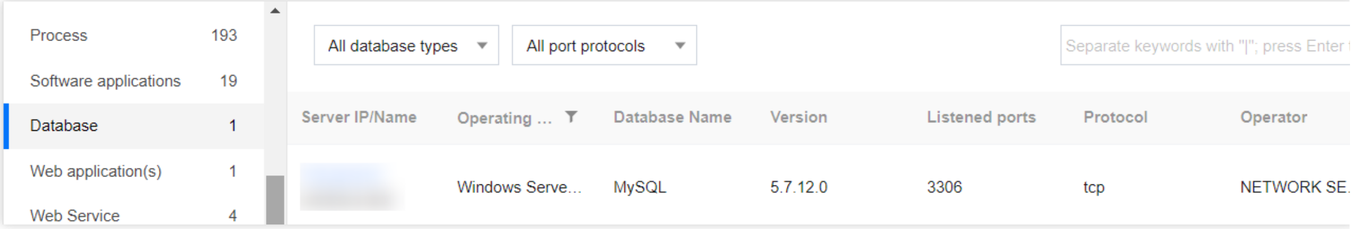
Asset Fingerprint Categories

Resource monitoring	4
Accounts	62
Ports	114
Process	193
Software applications	19

Server IP/Name	Operating sy...	App Name	Application type	Version ID	Binary path
[redacted]	Windows Server 2...	notepad	Others	10.0.14393.4169	C:\Windows\Syste...
[redacted]	Windows Server 2...	notepad	Others	10.0.14393.4169	C:\Windows\Syste...

Databases

Collects the data of all databases running on the server.



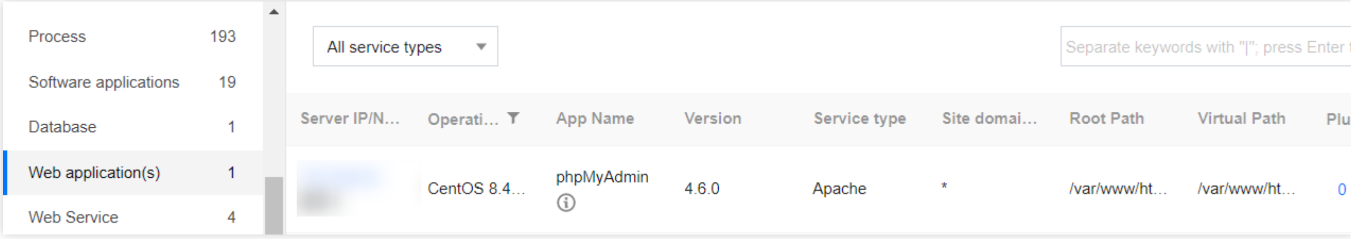
Process	193
Software applications	19
Database	1
Web application(s)	1
Web Service	4

Server IP/Name	Operating ...	Database Name	Version	Listened ports	Protocol	Operator
[redacted]	Windows Serve...	MySQL	5.7.12.0	3306	tcp	NETWORK SE

Web Applications

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

©2013-2022 Tencent Cloud. All rights reserved.



Process	193
Software applications	19
Database	1
Web application(s)	1
Web Service	4

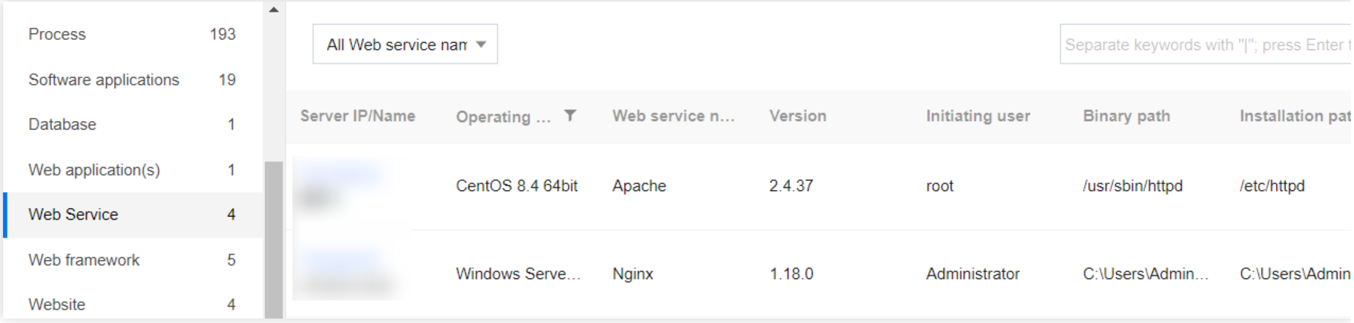
All service types

Separate keywords with "|"; press Enter t

Server IP/N...	Operati...	App Name	Version	Service type	Site domai...	Root Path	Virtual Path	Plu
[redacted]	CentOS 8.4...	phpMyAdmin ⓘ	4.6.0	Apache	*	/var/www/ht...	/var/www/ht...	0

Web Services

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



Process	193
Software applications	19
Database	1
Web application(s)	1
Web Service	4
Web framework	5
Website	4

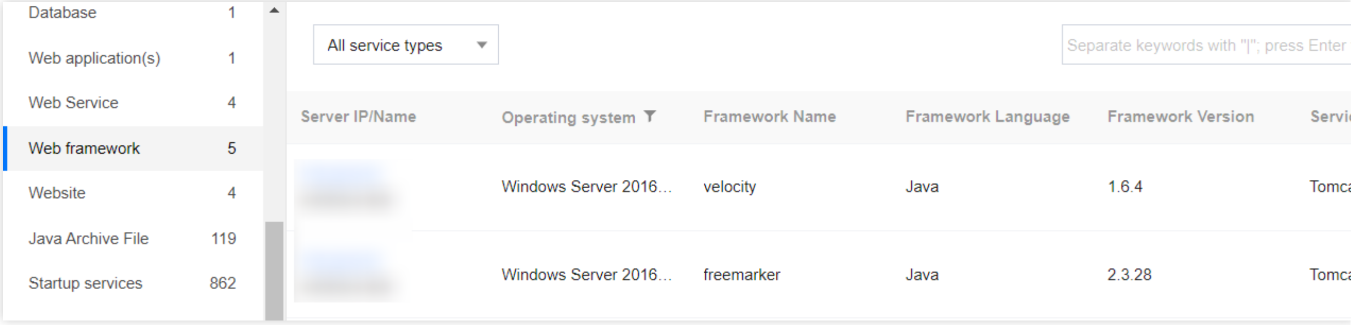
All Web service nan

Separate keywords with "|"; press Enter t

Server IP/Name	Operating ...	Web service n...	Version	Initiating user	Binary path	Installation pat
[redacted]	CentOS 8.4 64bit	Apache	2.4.37	root	/usr/sbin/httpd	/etc/httpd
[redacted]	Windows Serve...	Nginx	1.18.0	Administrator	C:\Users\Admin...	C:\Users\Admin

Web Frameworks

Collects all Web frameworks applied on the server.



Database	1
Web application(s)	1
Web Service	4
Web framework	5
Website	4
Java Archive File	119
Startup services	862

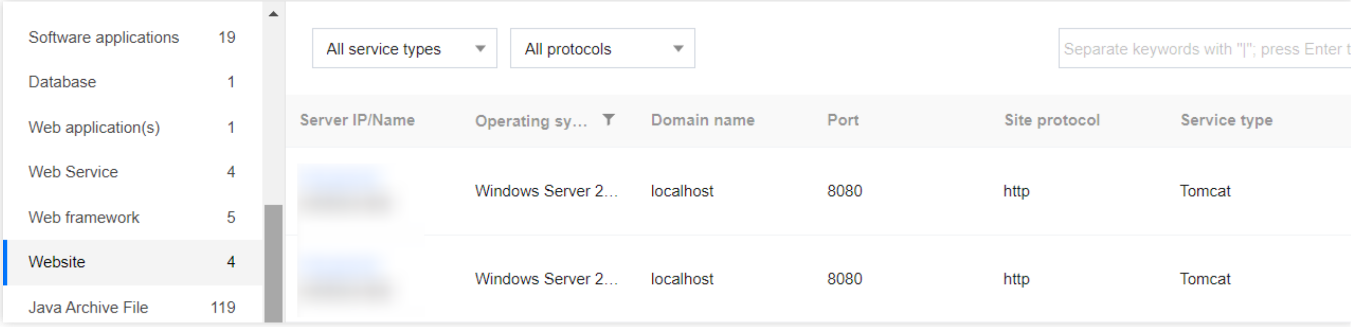
All service types

Separate keywords with "|"; press Enter

Server IP/Name	Operating system	Framework Name	Framework Language	Framework Version	Servi
[redacted]	Windows Server 2016...	velocity	Java	1.6.4	Tomca
[redacted]	Windows Server 2016...	freemarker	Java	2.3.28	Tomca

Websites

Collect the data of all websites deployed on the server.

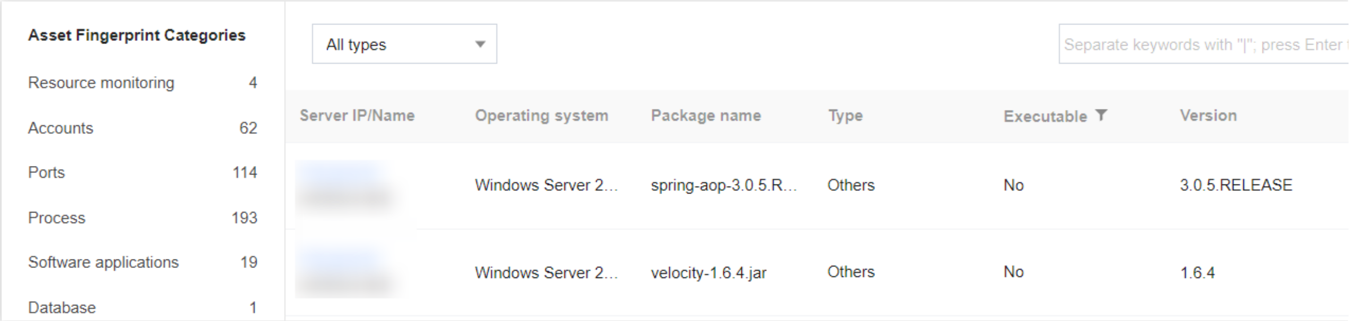


Software applications	19
Database	1
Web application(s)	1
Web Service	4
Web framework	5
Website	4
Java Archive File	119

Server IP/Name	Operating sy...	Domain name	Port	Site protocol	Service type
[redacted]	Windows Server 2...	localhost	8080	http	Tomcat
[redacted]	Windows Server 2...	localhost	8080	http	Tomcat

Java Archive Files

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

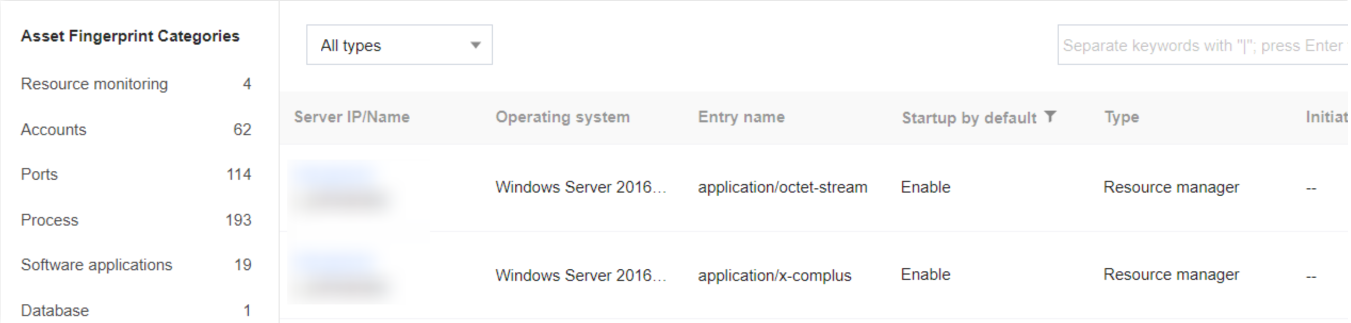


Asset Fingerprint Categories	
Resource monitoring	4
Accounts	62
Ports	114
Process	193
Software applications	19
Database	1

Server IP/Name	Operating system	Package name	Type	Executable	Version
[redacted]	Windows Server 2...	spring-aop-3.0.5.R...	Others	No	3.0.5.RELEASE
[redacted]	Windows Server 2...	velocity-1.6.4.jar	Others	No	1.6.4

Startup Services

Collect the data of all startup services on the server.



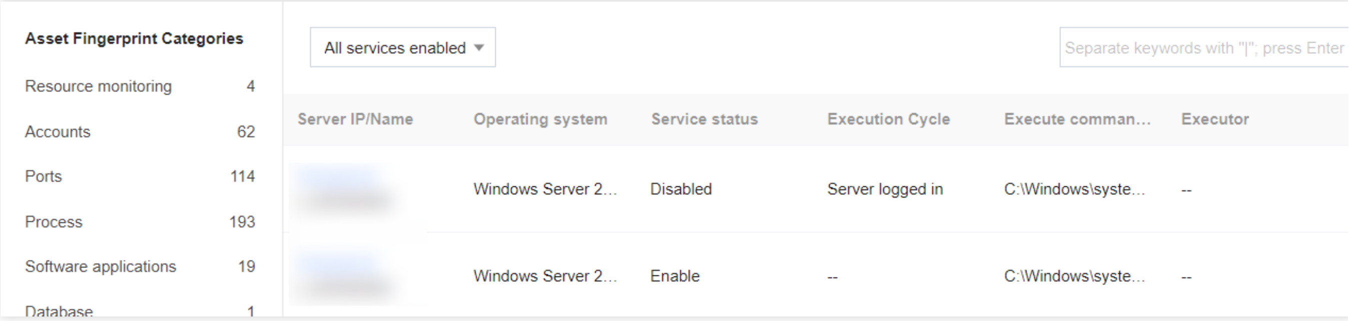
Asset Fingerprint Categories	
Resource monitoring	4
Accounts	62
Ports	114
Process	193
Software applications	19
Database	1

Server IP/Name	Operating system	Entry name	Startup by default	Type	Initiat
[redacted]	Windows Server 2016...	application/octet-stream	Enable	Resource manager	--
[redacted]	Windows Server 2016...	application/x-complus	Enable	Resource manager	--

Scheduled Tasks

Collect the data of all scheduled tasks on the server.

©2013-2022 Tencent Cloud. All rights reserved.

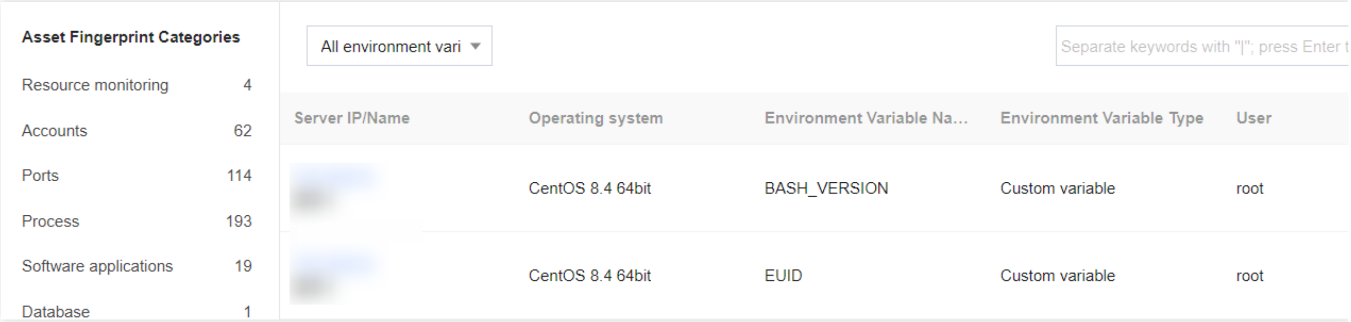


Asset Fingerprint Categories	
Resource monitoring	4
Accounts	62
Ports	114
Process	193
Software applications	19
Database	1

Server IP/Name	Operating system	Service status	Execution Cycle	Execute comman...	Executor
[redacted]	Windows Server 2...	Disabled	Server logged in	C:\Windows\syste...	--
[redacted]	Windows Server 2...	Enable	--	C:\Windows\syste...	--

Environment Variables

Collect the data of all environment variables of the server.

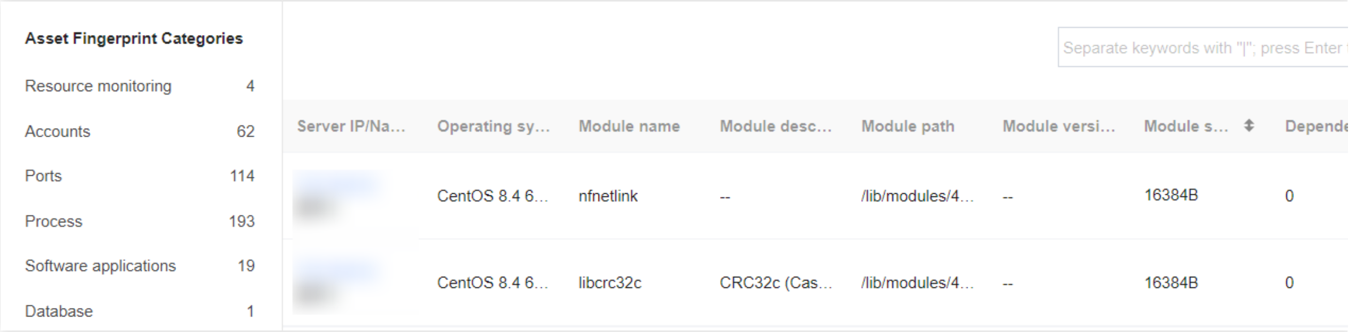


Asset Fingerprint Categories	
Resource monitoring	4
Accounts	62
Ports	114
Process	193
Software applications	19
Database	1

Server IP/Name	Operating system	Environment Variable Na...	Environment Variable Type	User
[redacted]	CentOS 8.4 64bit	BASH_VERSION	Custom variable	root
[redacted]	CentOS 8.4 64bit	EUID	Custom variable	root

Kernel Modules

Collect the data of all kernel modules of the server.



Asset Fingerprint Categories	
Resource monitoring	4
Accounts	62
Ports	114
Process	193
Software applications	19
Database	1

Server IP/Na...	Operating sy...	Module name	Module desc...	Module path	Module versi...	Module s...	Depende
[redacted]	CentOS 8.4 6...	nfnetlink	--	/lib/modules/4...	--	16384B	0
[redacted]	CentOS 8.4 6...	libcrc32c	CRC32c (Cas...	/lib/modules/4...	--	16384B	0

©2013-2022 Tencent Cloud. All rights reserved.

Malicious File Scan

Last updated：2023-12-26 16:21:25

This document describes how to use the Malicious File Scan feature.

Overview

Based on Tencent Cloud's tens of billions of samples, Malicious File Scan supports the detection of malicious files such as mining Trojans and Ransomware by using such engines as Cloud Security, Anti-Webshell, and TAV.

Important Notes

The Malicious File Scan feature is available only if you have at least one server bound to a (CWPP Pro/Ultimate) license.

Detection method.

Webshell detection: Detects common Webshells in languages such as ASP, PHP, JSP, and Python.

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

Operation Guide

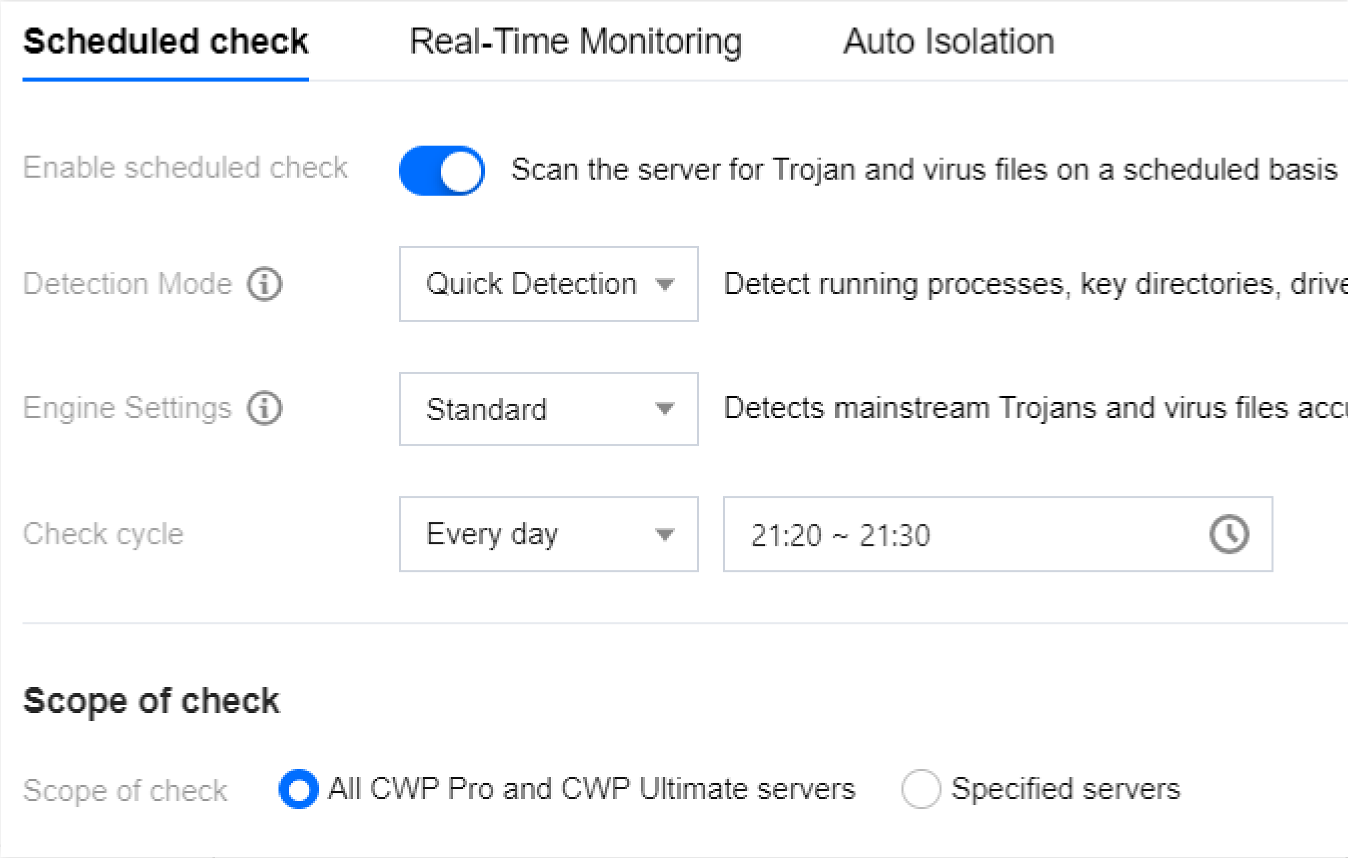
1. Log in to the CWPP console.
2. Click **Intrusion Detection** > **Malicious File Scan** on the left sidebar. The fields and operations related to the feature are described as follows.

File Scan Settings

Click the **File Scan Settings** button in the upper right corner to set **Scheduled Check**, **Real-Time Monitoring**, and **Auto Isolation**.

Scheduled Check: You can enable or disable scheduled checks, and set check mode, engine, check interval, and covered servers.

©2013-2022 Tencent Cloud. All rights reserved.



Scheduled check | Real-Time Monitoring | Auto Isolation

Enable scheduled check: ● Scan the server for Trojan and virus files on a scheduled basis

Detection Mode: Quick Detection ▾ Detect running processes, key directories, drive

Engine Settings: Standard ▾ Detects mainstream Trojans and virus files acc

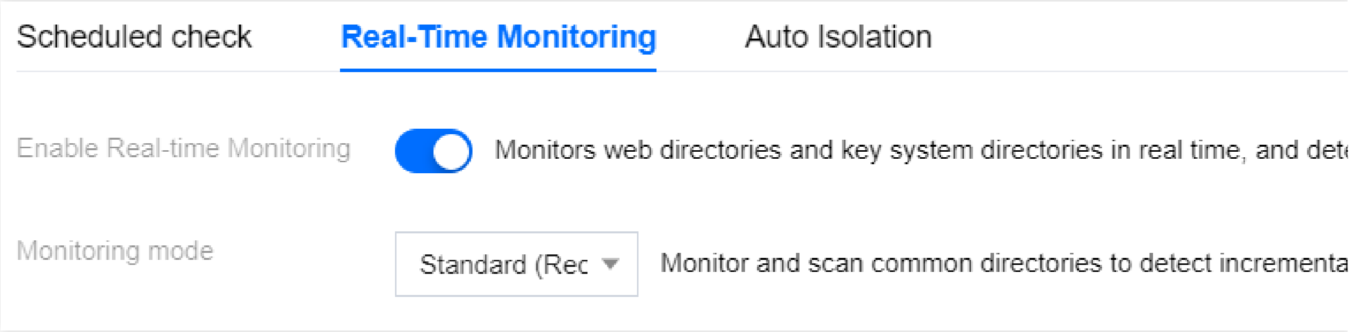
Check cycle: Every day ▾ 21:20 ~ 21:30

Scope of check

Scope of check: ● All CWP Pro and CWP Ultimate servers ○ Specified servers

Item	Description
Enable Scheduled Check	Enables or disables scheduled checks. You can regularly scan Trojan virus files on servers to enhance security.
Check Mode	Set check mode to define the check scope. Quick Check: Checks running processes, key directories, drive loading, etc. Overall Check: Checks all partitions of the system besides the scope of Quick Check.
Engine Mode	Increase detection rate by adjusting the engine mode. Standard: Detects mainstream Trojans and virus files accurately and efficiently.
Check Interval	Performs a check daily, every 3 days, and every 7 days.
Covered Servers	Servers with CWPP Pro/Ultimate or Selected Servers.

Real-time Monitoring: Monitors Web directories and key system directories, and scans & removes Trojan virus files. You can set the monitoring mode.



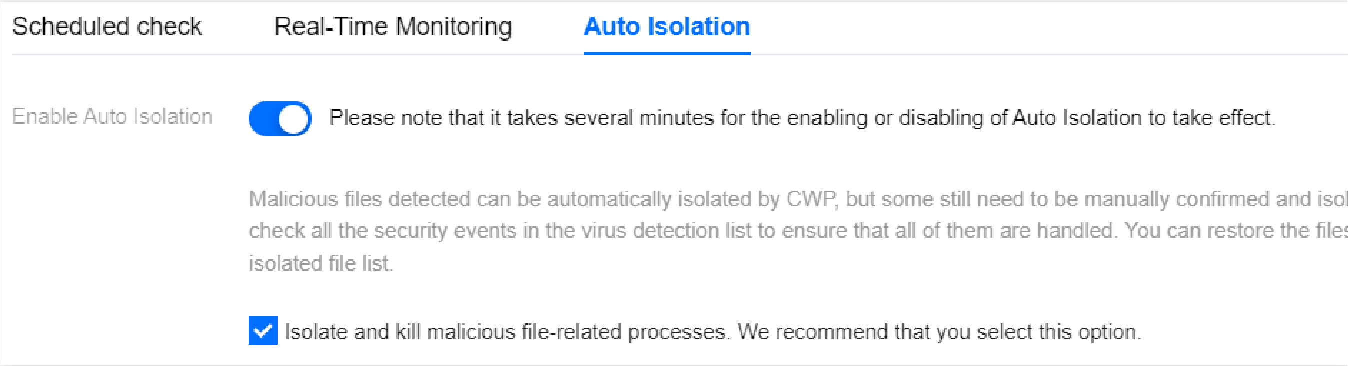
Scheduled check | Real-Time Monitoring | Auto Isolation

Enable Real-time Monitoring: Monitors web directories and key system directories in real time, and det

Monitoring mode: Standard (Rec ▾ Monitor and scan common directories to detect incrementa

Item	Description
Enable Real-time Monitoring	Enables/disables real-time monitoring of Web directories and key system directories, and scans & removes Trojan virus files.
Monitoring Mode	Set monitoring mode to define the scope of monitored files. Standard (recommended): Monitors and scans incremental files in common directories. Enhanced: Monitors and scans incremental files in all directories.

Auto Isolation: Automatically isolates detected malicious files. Some malicious files still need to be manually confirmed and isolated. We recommend that you check all the security events in the file scan list to ensure that all of the files are handled. You can de-isolate the files that are isolated by mistake in the list of isolated files.



Scheduled check | Real-Time Monitoring | Auto Isolation

Enable Auto Isolation: Please note that it takes several minutes for the enabling or disabling of Auto Isolation to take effect.

Malicious files detected can be automatically isolated by CWP, but some still need to be manually confirmed and isol check all the security events in the virus detection list to ensure that all of them are handled. You can restore the files isolated file list.

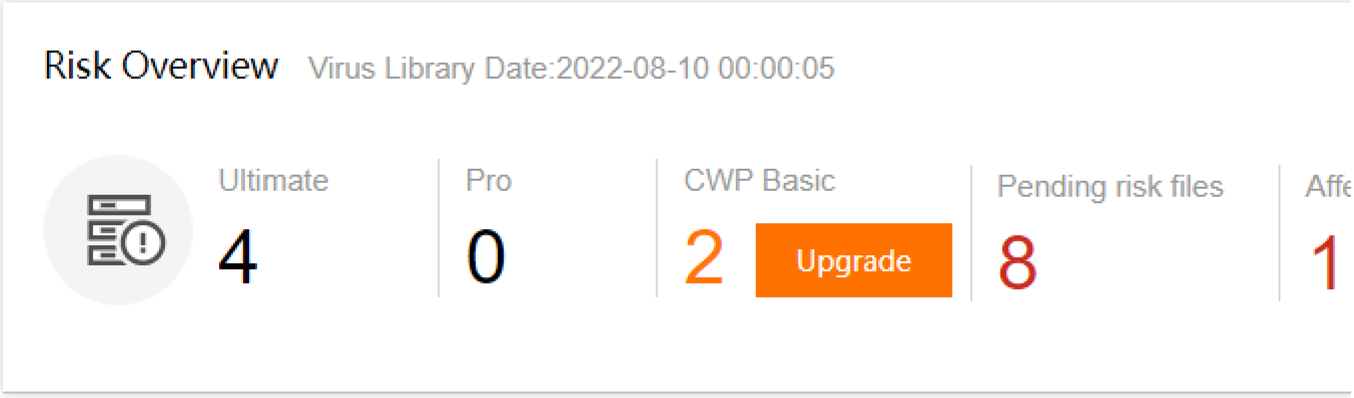
☑ Isolate and kill malicious file-related processes. We recommend that you select this option.

Item	Description
Enable Auto Isolation	Enables/disables auto isolation of detected malicious files. (It takes several minutes for the enabling or disabling of Auto Isolation to take effect)
Isolate and Kill Process	In the actual scenario, the file process may be still running after the file is isolated. It is recommended to select this option to kill the process related to the malicious file while isolating the file automatically.

Risk Overview

©2013-2022 Tencent Cloud. All rights reserved.

The **Risk Overview** shows the statistics of servers with different CWPP editions, as well as the pending risk files and the number of affected servers.

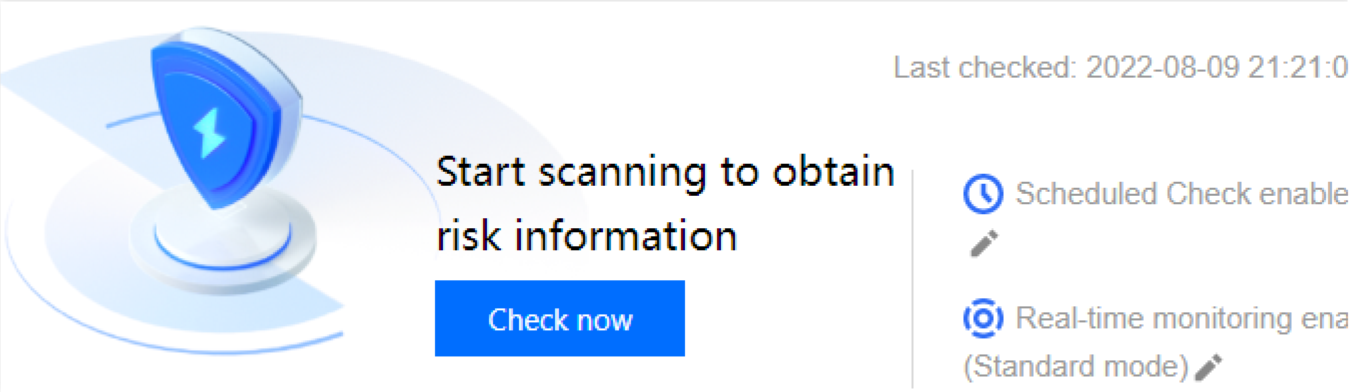


Risk Overview Virus Library Date:2022-08-10 00:00:05

Ultimate 4 | Pro 0 | CWP Basic 2 | Pending risk files 8 | Affe 1

Quick Check

Click the **Quick Check** button to set the check mode, engine, covered servers, and timeout threshold.



Last checked: 2022-08-09 21:21:0

Start scanning to obtain risk information

Scheduled Check enable

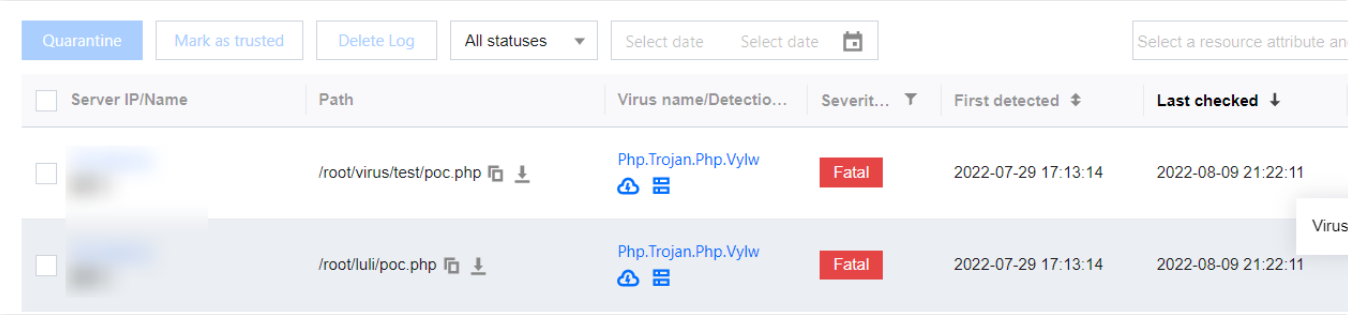
Real-time monitoring ena (Standard mode)

Note:

The possible reason for timeout: A long scan duration due to a large number of files and directories.

Event List

The **Event List** section shows the servers protected by CWPP and the malicious files detected.



□ Server IP/Name	Path	Virus name/Detectio...	Severit...	First detected	Last checked
□ [redacted]	/root/virus/test/poc.php	Php.Trojan.Php.Vylw	Fatal	2022-07-29 17:13:14	2022-08-09 21:22:11
□ [redacted]	/root/luli/poc.php	Php.Trojan.Php.Vylw	Fatal	2022-07-29 17:13:14	2022-08-09 21:22:11

Field description:

Server IP/Name: The server where a suspicious file was detected.

Path: The path of the suspicious file, which can be copied for downloading the file.

Virus Name/Detection Engine: The name of the virus affecting the suspicious file, and the engine that detected the virus.

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

First Detected: The time when the suspicious file was first detected.

Last detected: The time when the file risk was last detected.

Status

Pending: The status of the file and process when the file was last scanned.

Isolated: The file has been isolated automatically or manually.

Trusted: The file is trusted.

Cleared: The file and process no longer exist in the latest scan.

Isolating: The file is being isolated.

De-isolating: An isolated file is being de-isolated.

Operation

Isolate: Isolate the virus file to prevent hackers from launching it again. This allows you to locate and remove the virus file. In Windows, isolation may fail if this file is running. It is recommended to select the option of "Isolate and Kill Process".

Trust: If a file is confirmed to be non-malicious, you can select Trust so that the CWPP will no longer scan the file. You can filter and manage trusted files.

Delete Record: This action only deletes log records, rather than the file. Once deleted, the log information cannot be recovered. It is recommended to select "Isolate" or "Trust" first, or locate the file in the path and delete it manually.

Details: View event details, including virus file information, risk description, solutions, etc.

Unusual Login

Last updated：2023-12-26 16:23:44

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

Overview

When unusual login attempts such as login from an unusual location, login with an unusual user name, login at an unusual time, login from an unusual IP are detected, CWPP will mark the login records as "Suspicious" or "High-risk" based on intelligent algorithms, and send alerts to you in real time.

Important Notes

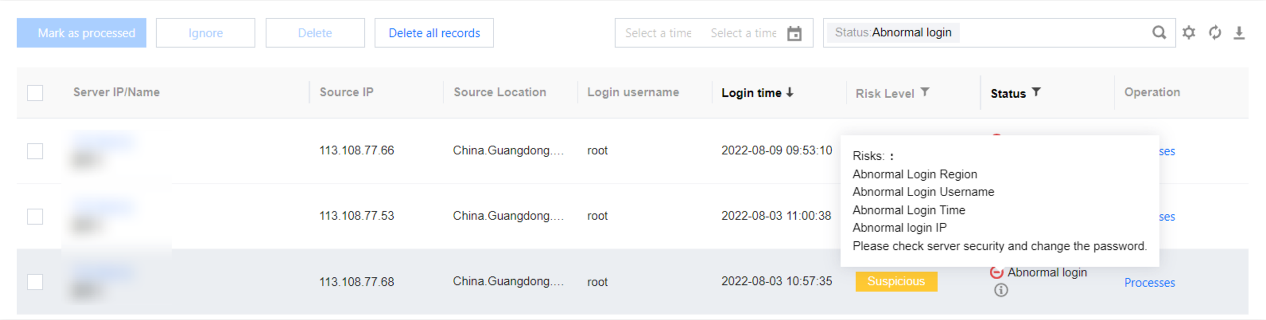
The Anti-Unusual Login feature is available for the servers on which the CWPP Agent is installed and is online.
The CWPP console only retains the unusual login events for the last 6 months, and the event data generated 6 months ago is not displayed.

Operation Guide

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

Event List

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



□	Server IP/Name	Source IP	Source Location	Login username	Login time ↓	Risk Level	Status	Operation
□	[redacted]	113.108.77.66	China.Guangdong....	root	2022-08-09 09:53:10			ses
□	[redacted]	113.108.77.53	China.Guangdong....	root	2022-08-03 11:00:38			ses
□	[redacted]	113.108.77.68	China.Guangdong....	root	2022-08-03 10:57:35	Suspicious	Abnormal login	Processes

Risks: :
Abnormal Login Region
Abnormal Login Username
Abnormal Login Time
Abnormal login IP
Please check server security and change the password.

Field description:

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

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

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

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

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

Threat Level: Suspicious/High.

Status

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

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

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

Ignored: This alert event has been ignored.

Operation

Actions

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

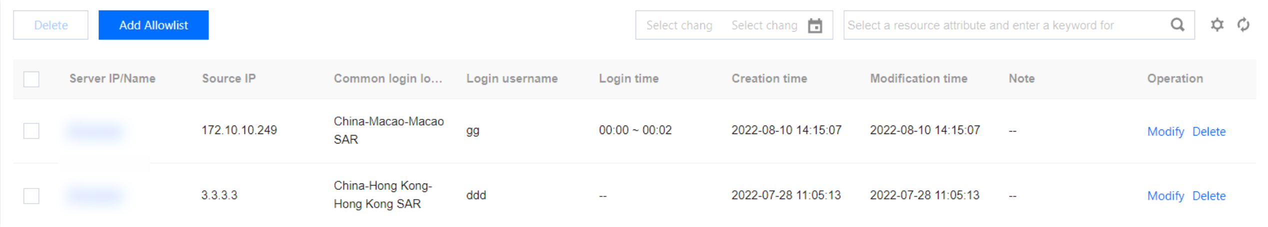
Add to Allowlist: Once an event is added to the allowlist, no alert will be sent if the same event occurs again.

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

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

Allowlist Management

In **Allowlist Management**, you can add/delete items to/from the allowlist of unusual logins, or check and edit the allowlist.



□	Server IP/Name	Source IP	Common login lo...	Login username	Login time	Creation time	Modification time	Note	Operation
□	[redacted]	172.10.10.249	China-Macao-Macao SAR	gg	00:00 ~ 00:02	2022-08-10 14:15:07	2022-08-10 14:15:07	--	Modify Delete
□	[redacted]	3.3.3.3	China-Hong Kong-Hong Kong SAR	ddd	--	2022-07-28 11:05:13	2022-07-28 11:05:13	--	Modify Delete

Field description:

Server IP/Name: The server on which the allowlist takes effect.

Source IP: The source IP added to the allowlist.

Usual Login Location: The login location added to the allowlist.

Login Username: The username added to the allowlist.

Login Time: The login time added to the allowlist.

Creation time: The time when the allowlist was created.

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

Operation

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

Delete: Delete items from the allowlist.

©2013-2022 Tencent Cloud. All rights reserved.

Password Cracking

Last updated：2023-12-26 16:23:52

This document describes how to use the Anti-Password Cracking feature.

Overview

CWPP's Anti-Password Cracking feature monitors brute force cracking of passwords for servers in real time and blocks the attacks automatically based on Tencent Cloud's network security defense and server intrusion detection capabilities.

Limits

Anti-Password Cracking is available for the servers on which the CWPP Agent is installed and online (except for automatic blocking).

Global blocking only takes effect on the servers bound to a (CWPP Pro/Ultimate) license.

The CWPP console only retains the password cracking events for the last 6 months, and the event data generated 6 months ago is not displayed.

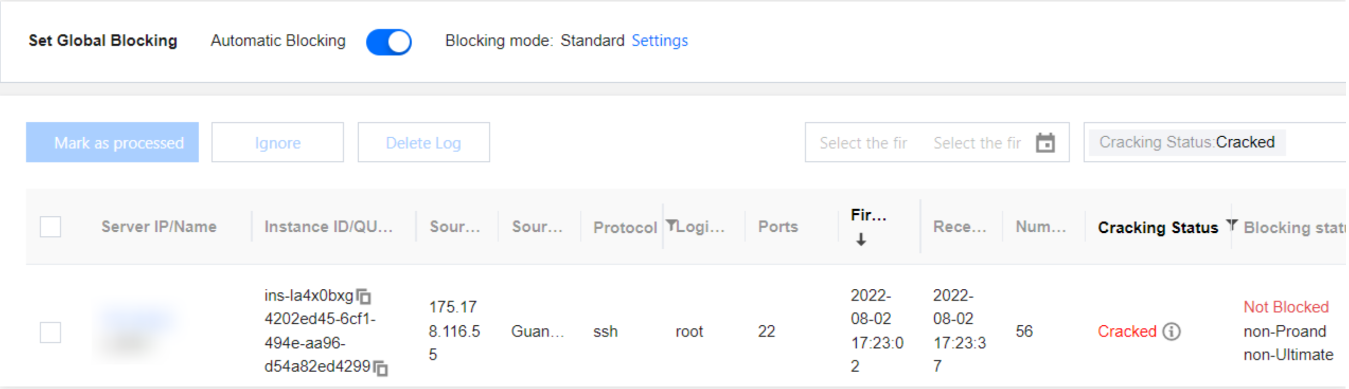
Operation Guide

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

Event List

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

©2013-2022 Tencent Cloud. All rights reserved.



Set Global Blocking Automatic Blocking Blocking mode: Standard Settings

Mark as processed | Ignore | Delete Log | Select the fir | Select the fir | Cracking Status:Cracked

□	Server IP/Name	Instance ID/QU...	Sour...	Sour...	Protocol	Logi...	Ports	Fir... ↓	Rece...	Num...	Cracking Status	Blocking stat
□	[redacted]	ins-la4x0bxg 4202ed45-6cf1-494e-aa96-d54a82ed4299	175.178.116.55	Guan...	ssh	root	22	2022-08-02 17:23:02	2022-08-02 17:23:37	56	Cracked	Not Blocked non-Proand non-Ultimate

You can enable **Auto Blocking**, which has two modes.

Blocking Mode	Description
Standard	Intelligently identifies brute-force cracking based on the brute force rules you set, and automatically blocks the source IP of brute-force cracking not in the allowlist.
Enhanced	Automatically blocks the source IP not in the allowlist based on the "Allowlist - Allowlist only" policy (only ports 22 and 3389 are supported). Enhanced blocking covers standard blocking.

Field description:

Server IP/Name: The server where password cracking was detected.

Source IP: Source IP address of the attack.

Origin: The region where the source IP of the attack is located.

Protocol: The protocol used by the attacker, including SSH/RDP, FTP, MsSQL, MySQL, SMB, MongoDB, Kafka, and RabbitMQ.

Login username: The username used by the attacker for login.

Port: The port used by the attacker for login.

First attack: The time when the password cracking behavior was first detected by CWPP.

Latest attack: The time when the event last occurred.

Number of attempts: The number of password cracking attempts made by the attacker IP.

Cracking Status: Whether password cracking on the current server is successful.

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

Event Status: Pending, Allowlisted, Handled, or Ignored

Operation

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

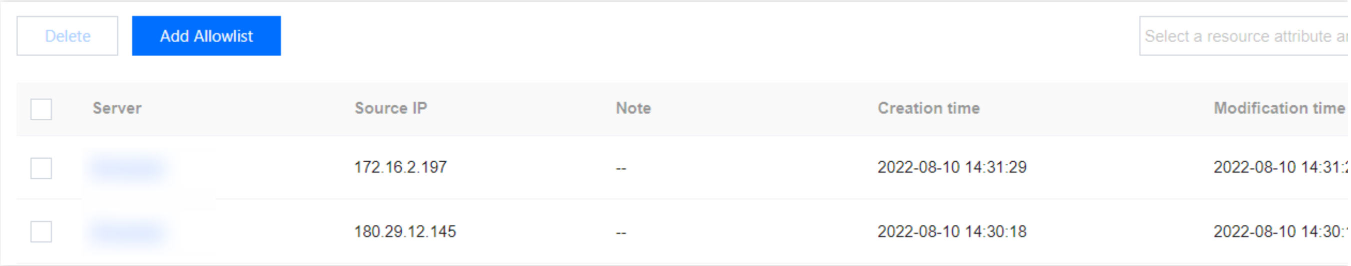
Add to Allowlist: Once an event is added to the allowlist, no alert will be sent if the same event occurs again.

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

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

Allowlist Management

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



☐	Server	Source IP	Note	Creation time	Modification time
☐	[redacted]	172.16.2.197	--	2022-08-10 14:31:29	2022-08-10 14:31:
☐	[redacted]	180.29.12.145	--	2022-08-10 14:30:18	2022-08-10 14:30:

Field description:

Server IP/Name: The server on which the allowlist takes effect.

Source IP: The source IP added to the allowlist.

Usual Login Location: The login location added to the allowlist.

Login Username: The username added to the allowlist.

Login Time: The login time added to the allowlist.

Creation time: The time when the allowlist was created.

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

Operation

Edit: Edit the source IP, covered servers, and remarks.

Delete: Delete items from the allowlist.

Malicious Requests

Last updated：2023-12-26 16:23:59

This document describes how to use the Anti-Malicious Requests feature.

Overview

The Anti-Malicious Requests feature monitors requests sent to the external domains in real time to identify and handle the requests to malicious domains. If a request sent to a malicious domain is detected, you will receive an alert in real time.

Limits

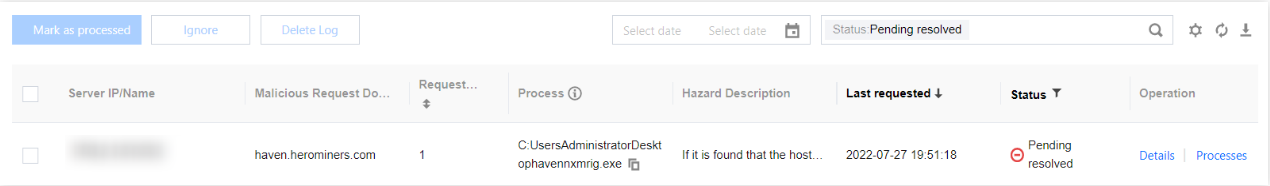
The Anti-Malicious Requests feature is available only if you have at least one server bound to a (CWPP Pro/Ultimate) license.

Operation Guide

1. Log in to the CWPP console.
2. Click **Intrusion Detection** > **Anti-Malicious Requests** on the left sidebar. The fields and operations related to the feature are descibed as follows.

Event List

In the **Event List**, you can view and handle the requests sent to malicious domains that are detected by CWPP.



□	Server IP/Name	Malicious Request Do...	Request...	Process	Hazard Description	Last requested	Status	Operation
□	[redacted]	haven.herominers.com	1	C:UsersAdministratorDesktophavennxmrig.exe	If it is found that the host...	2022-07-27 19:51:18	Pending resolved	Details | Processes

Field description:

Server IP/Name: The server which sent a request to a malicious domain.

Malicious Domain: The malicious domain to which a request was sent.

©2013-2022 Tencent Cloud. All rights reserved.

No. of Requests: The number of the requests sent to the malicious domain.

Process: Only supported for Windows system.

Description: The risk description of the malicious domain.

Last requested: The time when the last request was sent to the malicious domain.

Status: **Pending processed**, **Added to allowlist**, **Processed** and **Ignored**

Operation

Details: You can view more information about the request to the malicious domain, such as process information, command lines, and risk description.

Actions

Mark as processed: Please handle the risk manually by referring to "Solutions" in the event details, and then mark the event as "Handled".

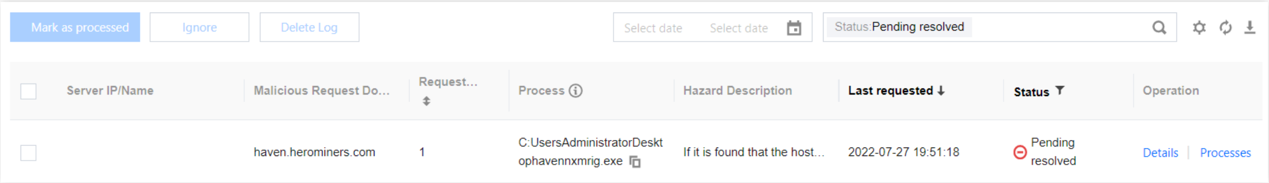
Add to Allowlist: Once an event is added to the allowlist, no alert will be sent if the same event occurs again.

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

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

Allowlist Management

In **Allowlist Management**, you can add/delete items to/from the allowlist, or edit and check the allowlist.



□	Server IP/Name	Malicious Request Do...	Request...	Process	Hazard Description	Last requested	Status	Operation
□		haven.herominers.com	1	C:UsersAdministratorDesktophavennxmrig.exe	If it is found that the host...	2022-07-27 19:51:18	Pending resolved	Details | Processes

Field description:

Allowed Domain Name: It can be an exact domain name or a wildcard domain name. When a request to this domain is detected, no event alert is generated.

Remarks: Remarks for the allowlist.

Creation time: The time when the allowlist was created.

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

Operation

Edit: Edit the allowed domain names and remarks.

Delete: Delete items from the allowlist.

Note:

The allowlist takes effect on all servers (Pro/Ultimate).

©2013-2022 Tencent Cloud. All rights reserved.

High-risk Commands

Last updated：2023-12-26 16:24:07

This document describes how to use the High-Risk Command Detection feature.

Overview

CWPP monitors the commands in the system in real time, and supports the configuration of rules to classify the commands in terms of risk level. If any high-risk command is detected, an alert will be sent to you in real time.

Limits

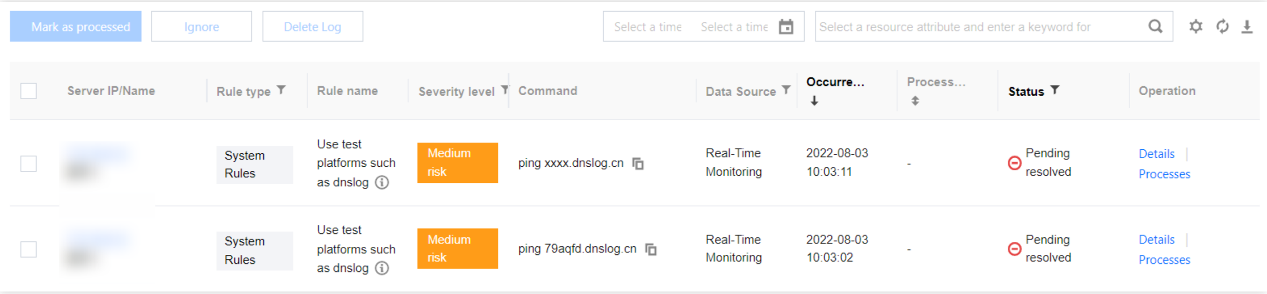
You have at least one server bound with a CWPP Pro/Ultimate license.

Operation Guide

1. Log in to the CWPP console.
2. Click **Intrusion Detection** > **High-risk commands** on the left side bar. The fields and operations related to the feature are described as follows:

Event List

In the **Event list**, you can view and handle the high-risk command risks detected by CWPP.



□	Server IP/Name	Rule type	Rule name	Severity level	Command	Data Source	Occurre...	Process...	Status	Operation
□	[redacted]	System Rules	Use test platforms such as dnslog ⓘ	Medium risk	ping xxxx.dnslog.cn	Real-Time Monitoring	2022-08-03 10:03:11	-	⊖ Pending resolved	Details | Processes
□	[redacted]	System Rules	Use test platforms such as dnslog ⓘ	Medium risk	ping 79aqfd.dnslog.cn	Real-Time Monitoring	2022-08-03 10:03:02	-	⊖ Pending resolved	Details | Processes

Field description:

Server IP/Mame: The server where a high-risk command was detected.

Rule type: **Preset rules** and **Custom rules**

Rule name: The name of the hit preset or custom rule.

Severity level: **High**, **Medium**, and **Low**.

Command: The content of the executed command.

Login user: The user logged in to the server when the command was executed.

PID: The unique ID of the process file.

Process: The running state of the program after execution.

Data source: Bash log and real-time monitoring.

Occurrence time: The time when the high-risk command occurred.

Processed time: The time when the high-risk command was handled on the CWPP console.

Status: **Pending processed**, **Added to allowlist**, **Processed** and **Ignored**

Operation

Details: You can view more information about high-risk commands, such as process information, command lines, and risk description.

Actions

Mark as processed: Please handle the risk manually by referring to **Fix Suggestion** in the event details, and then mark the event as **Processed**.

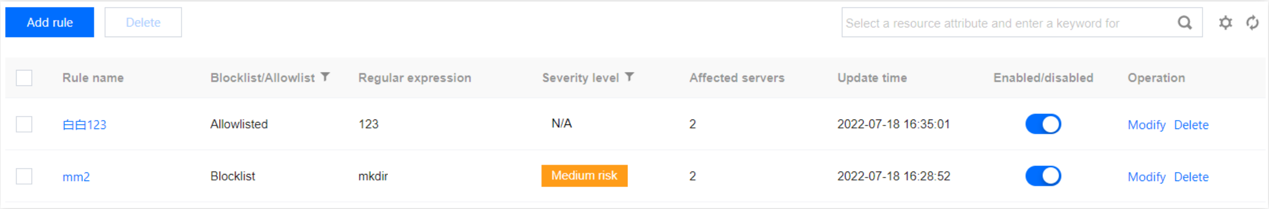
Add to Allowlist: Once an event is added to the allowlist, no alert will be sent if the same event occurs again.

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

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

Configuring Custom Rules

In **Custom Rules**, you can add/delete rules to/from the allowlist/blocklist of high-risk commands, and check and edit the allowlist/blocklist.



□	Rule name	Blocklist/Allowlist	Regular expression	Severity level	Affected servers	Update time	Enabled/disabled	Operation
□	白白123	Allowlisted	123	N/A	2	2022-07-18 16:35:01	●	Modify Delete
□	mm2	Blocklist	mkdir	Medium risk	2	2022-07-18 16:28:52	●	Modify Delete

Field description:

Rule name: The name of the rule for the blocklist/allowlist of high-risk commands.

Blocklist/Allowlist: When a command matches the regular expression of the blocklist, an alert for the security event is generated. When a command matches the regular expression of the allowlist, no alert is generated to avoid false positives.

Regular expression: A regular expression that determines whether a command matches the blocklist/allowlist.

Severity level: High, Medium, Low, None.

Affected servers: The range of servers on which a rule takes effect.

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

Enabled/disabled: Enable/Disable.

Operation

Edit: Edit the range of servers on which a rule takes effect.

Delete: Delete rules.

©2013-2022 Tencent Cloud. All rights reserved.

Local Privilege Escalation

Last updated：2023-12-26 16:24:14

This document describes how to use the Anti-Local Privilege Escalation feature.

Overview

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

Limits

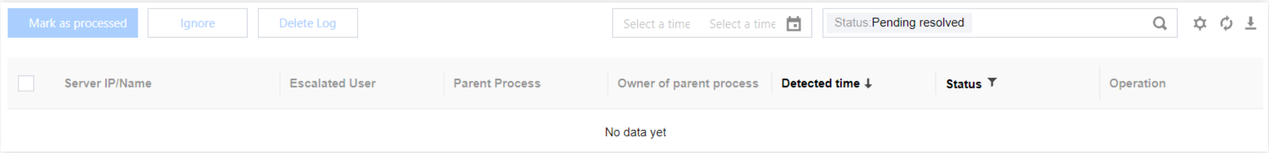
The Anti-Local Privilege Escalation feature is available only if you have at least one server bound to a (CWPP Pro/Ultimate) license.

Operation Guide

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

Event List

In the **Event List**, you can view and handle the local privilege escalation risks detected by CWPP.



□	Server IP/Name	Escalated User	Parent Process	Owner of parent process	Detected time ↓	Status	Operation

No data yet

Field description:

Server IP/Name: The server where local privilege escalation was detected.

Privilege Elevation User: The user with a low privilege who gains control of the server by obtaining a high privilege.

©2013-2022 Tencent Cloud. All rights reserved.

Parent Process: The parent process for privilege escalation.

Parent Process User: The user who can execute the parent process.

Detected At: The time when the local privilege escalation was detected.

Status: Pending, Allowlisted, Handled, or Ignored

Operation

Details: You can view more information about high-risk commands, such as process information, command lines, and risk description.

Actions

Mark as processed: Please handle the risk manually by referring to "Solutions" in the event details, and then mark the event as "Handled".

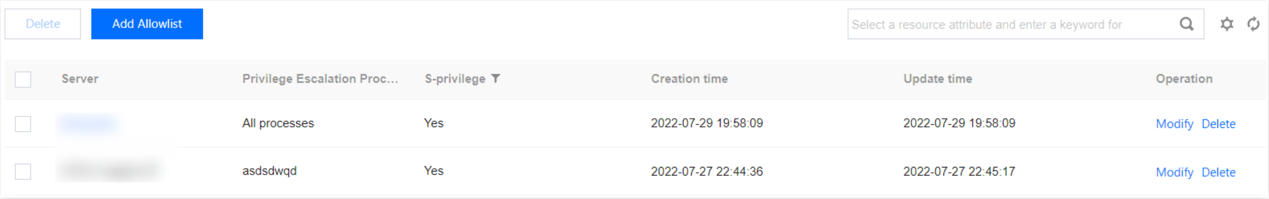
Add to Allowlist: Once an event is added to the allowlist, no alert will be sent if the same event occurs again.

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

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

Allowlist Management

In **Allowlist Management**, you can add/delete items to/from the allowlist, or edit and check the allowlist.



□	Server	Privilege Escalation Proc...	S-privilege	Creation time	Update time	Operation
□	[redacted]	All processes	Yes	2022-07-29 19:58:09	2022-07-29 19:58:09	Modify Delete
□	[redacted]	asdsdwqd	Yes	2022-07-27 22:44:36	2022-07-27 22:45:17	Modify Delete

Field description:

Servers: The range of servers on which the allowlist takes effect.

Privilege Escalation Process: The process for privilege escalation.

With S Permission: Whether the user executing a file has the ownership of the file (whether the user is the temporary owner of the file).

Creation time: The time when the allowlist was created.

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

Operation

Edit: Edit the conditions of privilege escalation.

Delete: Delete items from the allowlist.

©2013-2022 Tencent Cloud. All rights reserved.

Reverse Shell

Last updated：2023-12-26 16:24:22

This document describes how to use the reverse shell detection feature.

Overview

Reverse shell detection identifies and records reverse shell connections from.

Limits

You have at least one server bound to a CWPP Pro/Ultimate license.

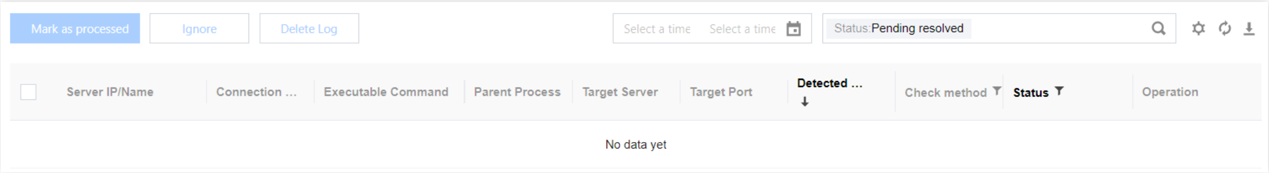
Alerts are only triggered for reverse shell connected to a server is detected in a public network.

Operation Guide

1. Log in to the CWPP console.
2. Click **Intrusion Detection** > **Reverse Shell** on the left side bar. The fields and operations related to the feature are described as follows.

Event List

In the **Event list**, you can view and handle the reverse shell risks detected by CWPP.



Status:Pending resolved

□	Server IP/Name	Connection ...	Executable Command	Parent Process	Target Server	Target Port	Detected ... ↓	Check method	Status	Operation

No data yet

Field description:

Server IP/Name: The server where a reverse shell was detected.

Connection Process: The process for the reverse connection.

Command: The command executed for the reverse shell.

Parent Process: The parent process for the connection process.

©2013-2022 Tencent Cloud. All rights reserved.

Target Server: The target server of the reverse shell.

Target Port: The target port of the reverse shell.

Detected Time: The time when the reverse shell action was first detected.

Check Method: Behavior analysis, command feature detection.

Status: **Pending processed**, **Added to allowlist**, **Processed** and **Ignored**

Operation

Details: You can view more information about reverse shells, such as process information, command lines, and risk description.

Actions

Mark as processed: Please handle the risk manually by referring to **Fix Suggestions** in the event details, and then mark the event as "Handled".

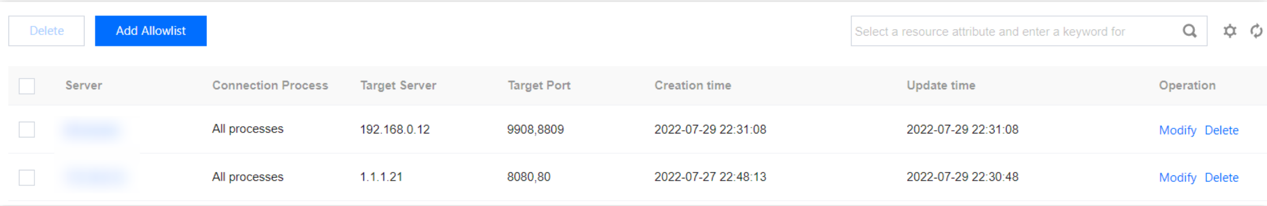
Add to Allowlist: Once an event is added to the allowlist, no alert will be sent if the same event occurs again.

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

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

Allowlist Management

In **Allowlist Management**, you can add/delete items to/from the allowlist, or edit and check the allowlist.



□	Server	Connection Process	Target Server	Target Port	Creation time	Update time	Operation
□	[redacted]	All processes	192.168.0.12	9908,8809	2022-07-29 22:31:08	2022-07-29 22:31:08	Modify Delete
□	[redacted]	All processes	1.1.1.21	8080,80	2022-07-27 22:48:13	2022-07-29 22:30:48	Modify Delete

Field description:

Servers: The range of servers on which the allowlist takes effect.

Connection Process: The connection process in the allowlist.

Target Server: The target server in the allowlist.

Target Port: The target port in the allowlist.

Creation time: The time when the allowlist was created.

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

Operation

Edit: Edit the conditions of reverse shells in the allowlist.

Delete: Delete items from the allowlist.

Vulnerability Management

Last updated：2023-12-26 16:24:44

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

Overview

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

Important Notes

The Vulnerability Management feature is available only if you have at least one server bound to a (**CWPP Pro**/**Ultimate**) license.

Vulnerabilities that can be detected: Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities.

Vulnerabilities that can be fixed automatically: Linux software vulnerabilities (some) and Web-CMS vulnerabilities (some).

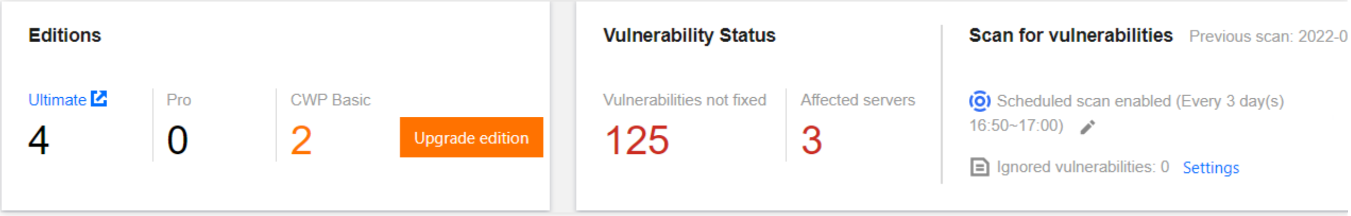
Operation Guide

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

Vulnerability Scan

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

©2013-2022 Tencent Cloud. All rights reserved.



Editions

Ultimate	Pro	CWP Basic
4	0	2

Upgrade edition

Vulnerability Status

Vulnerabilities not fixed	Affected servers
125	3

Scan for vulnerabilities Previous scan: 2022-0

Scheduled scan enabled (Every 3 day(s) 16:50~17:00)

Ignored vulnerabilities: 0 Settings

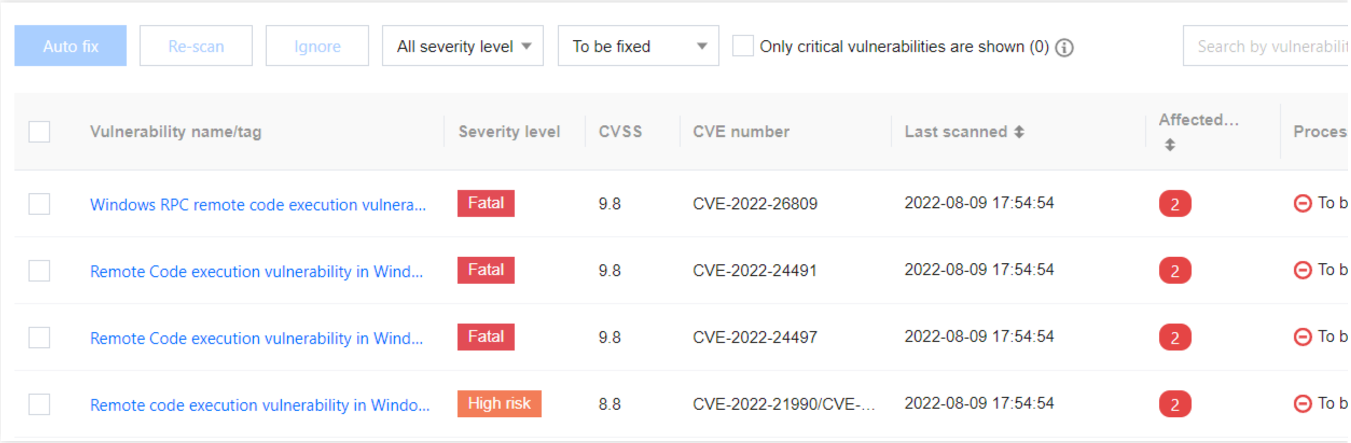
Click **Quick Scan** to open the **Quick Scan Settings** pop-up window. You can perform a scan immediately after setting the vulnerability category, vulnerability level, scan timeout threshold, and servers covered by the scan.

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

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

Vulnerability List

The vulnerabilities in the **Vulnerability List** are categorized as Urgent Vulnerabilities, Critical Vulnerabilities, and All Vulnerabilities. The three categories are not obviously different from each other in terms of functionality. The fields and operations related to Vulnerability List are described as follows using **All Vulnerabilities** as an example.



□	Vulnerability name/tag	Severity level	CVSS	CVE number	Last scanned	Affected...	Proces
□	Windows RPC remote code execution vulnera...	Fatal	9.8	CVE-2022-26809	2022-08-09 17:54:54	2	To b
□	Remote Code execution vulnerability in Wind...	Fatal	9.8	CVE-2022-24491	2022-08-09 17:54:54	2	To b
□	Remote Code execution vulnerability in Wind...	Fatal	9.8	CVE-2022-24497	2022-08-09 17:54:54	2	To b
□	Remote code execution vulnerability in Windo...	High risk	8.8	CVE-2022-21990/CVE-...	2022-08-09 17:54:54	2	To b

Field description:

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

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

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

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

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

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

©2013-2022 Tencent Cloud. All rights reserved.

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

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

Operation

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

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

Rescan: Perform a scan again for this vulnerability.

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

Baseline Management

Last updated：2023-12-26 16:24:54

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

Overview

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

Important Notes

The Baseline Management feature is available only if you have at least one server bound to a (**CWPP Pro**/**Ultimate**) license.

Supported baseline types for check

Baseline Type	Supported Baselines for Check
Unauthorized access	Unauthorized access to CouchDB Unauthorized access to Elasticsearch unauthorized access to MongoDB unauthorized access to Hadoop unauthorized access to Kubelet Redis baseline compliance check unauthorized access to ZooKeeper
Weak passwords	Linux system weak passwords MySQL weak passwords Windows system weak passwords Linux system weak passwords Rsync weak passwords Linux account with empty password Access to Rsync without a password Xampp default FTP password ActiveMQ baseline compliance check
Remote code execution	JavaRMI remote code execution

©2013-2022 Tencent Cloud. All rights reserved.

	Jenkins without authentication causes execution of arbitrary commands
Tencent Cloud security standards	MongoDB security baseline check Linux security baseline check Windows security baseline check FTP security baseline check Nginx security baseline check Information leakage baseline check
Other	NFS misconfiguration causes mounting of sensitive directories PHP-FPM misconfiguration Docker daemon port (2375) is open Detection of Tomcat example directories Memcached's UDP port exploited by DDoS amplification attacks IIS misconfiguration causes resolution vulnerability RPCBind misconfiguration CentOS baseline check

Operation Guide

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

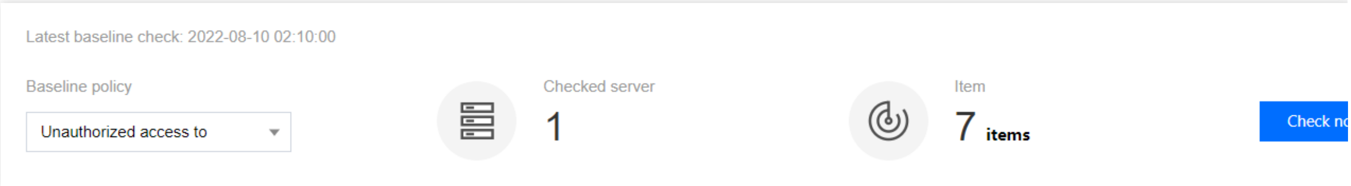
Baseline policies

A baseline policy is a collection of user-defined baseline check items, allowing you to track baseline pass rates and detected risks based on the dimensions included in the policy.

Tencent Cloud default baseline policies: Tencent Cloud CWPP provides default baseline policies based on mainstream network security baseline check items, including: weak password policy, CIS baseline policy, and Tencent Cloud best security practice policy. You can add check items and servers to be checked to a default baseline policy, under which the check is conducted once every 7 days by default (at 00:00 of the day).

Note:

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



Latest baseline check: 2022-08-10 02:10:00

Baseline policy: Unauthorized access to

Checked server: 1

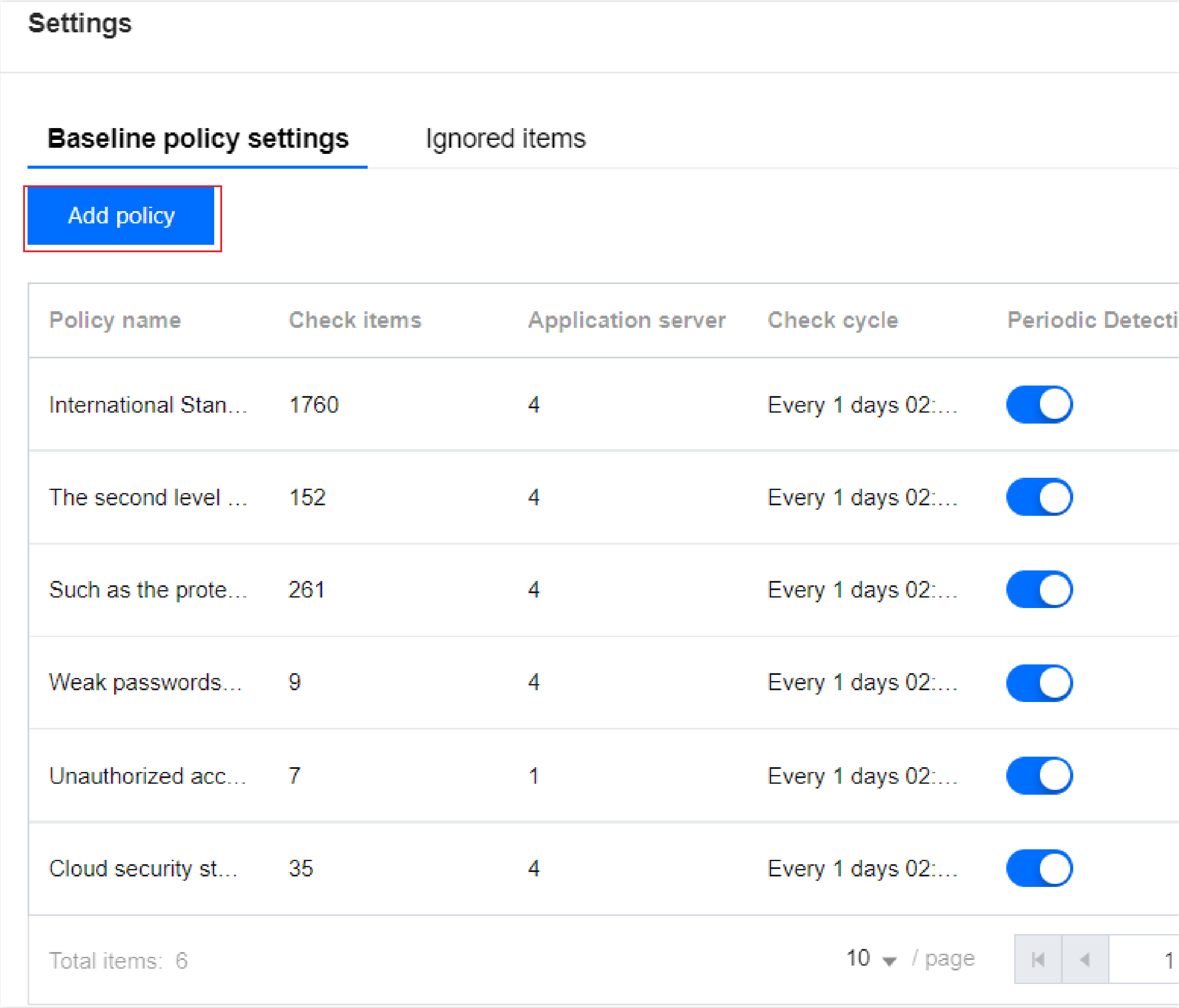
Item: 7 items

Add Baseline Policies

©2013-2022 Tencent Cloud. All rights reserved.

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

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



Settings

Policy name	Check items	Application server	Check cycle	Periodic Detecti
International Stan...	1760	4	Every 1 days 02:...	
The second level ...	152	4	Every 1 days 02:...	
Such as the prote...	261	4	Every 1 days 02:...	
Weak passwords...	9	4	Every 1 days 02:...	
Unauthorized acc...	7	1	Every 1 days 02:...	
Cloud security st...	35	4	Every 1 days 02:...	

Total items: 6 10 / page 1

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

Note:

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

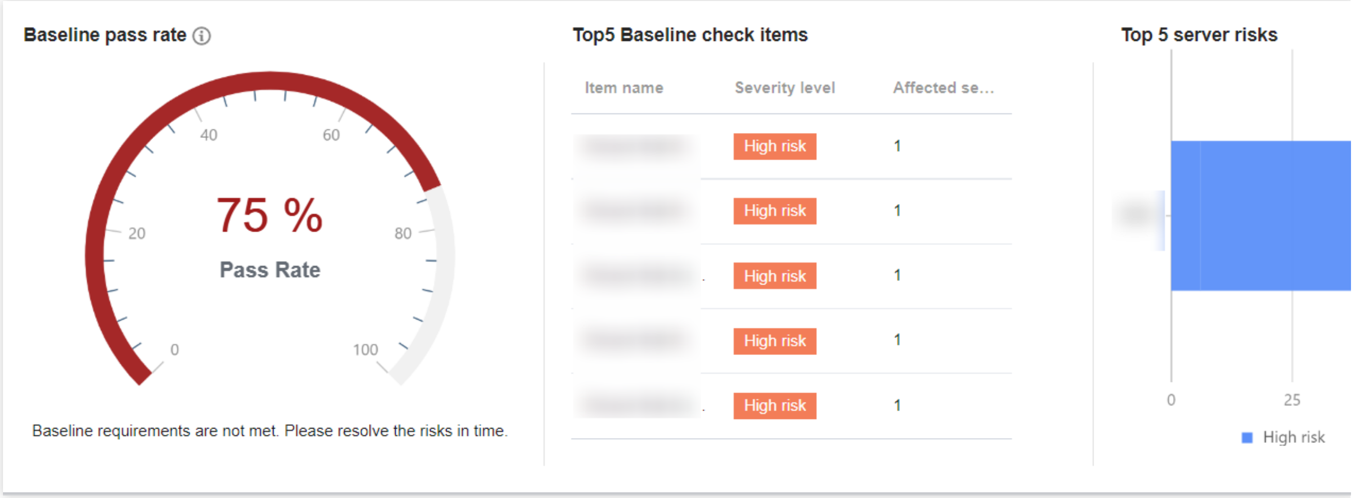
Quick Check

Select the baseline policies for your check, click **Quick Check** (The check generally takes 2-10 minutes).

Periodic Check

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

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



Baseline requirements are not met. Please resolve the risks in time.

Top5 Baseline check items

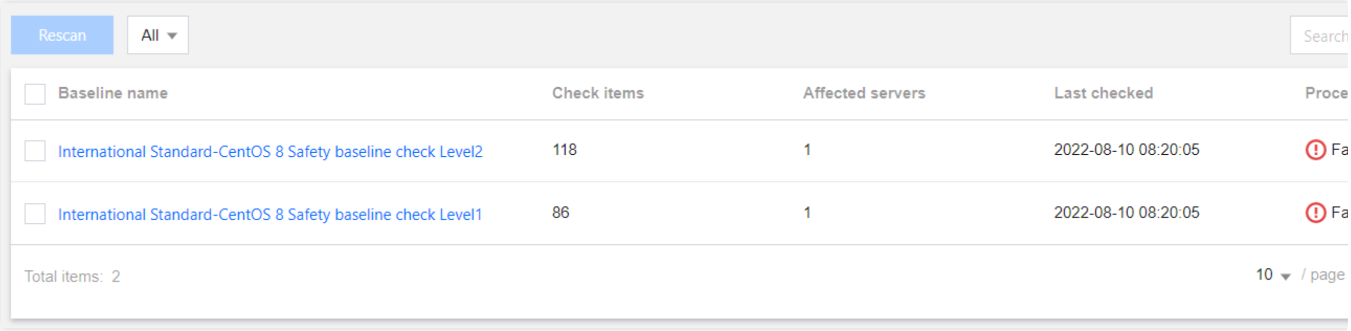
Item name	Severity level	Affected se...
[illegible]	High risk	1
[illegible]	High risk	1
[illegible]	High risk	1
[illegible]	High risk	1
[illegible]	High risk	1

Visualized baseline data

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

Baseline check result list

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



□ Baseline name	Check items	Affected servers	Last checked	Proce
□ International Standard-CentOS 8 Safety baseline check Level2	118	1	2022-08-10 08:20:05	Fa
□ International Standard-CentOS 8 Safety baseline check Level1	86	1	2022-08-10 08:20:05	Fa

Total items: 2

10 / page

Field description:

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

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

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

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

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

©2013-2022 Tencent Cloud. All rights reserved.

Status: Pass, Fail and In Progress.

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

Rescan:

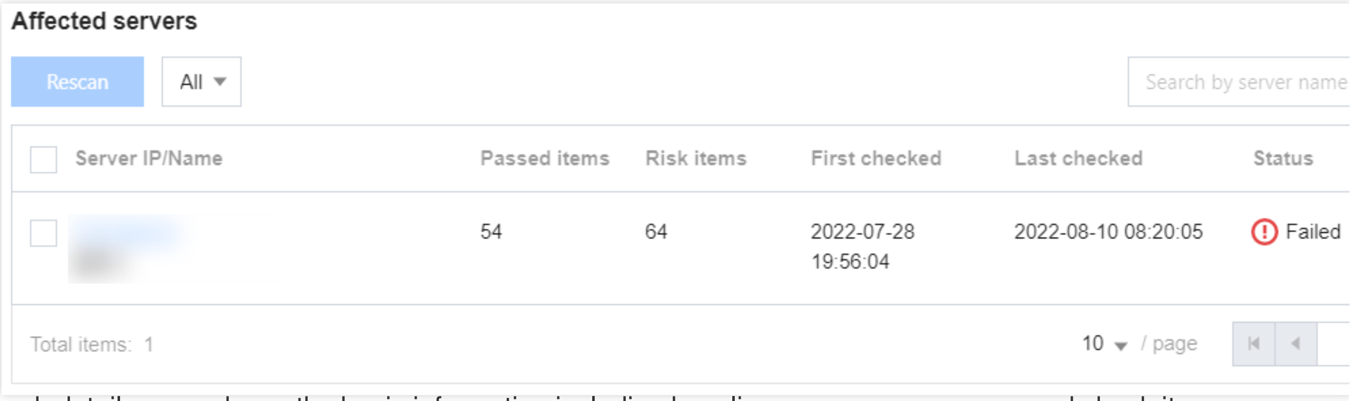
Option 1: Select the baselines for a recheck, and click **Recheck** in the upper left corner of the list to run a recheck for the selected baselines at one time.

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

View details:

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

The baseline details page shows the description and threat level of the baseline, as well as the list of affected servers.

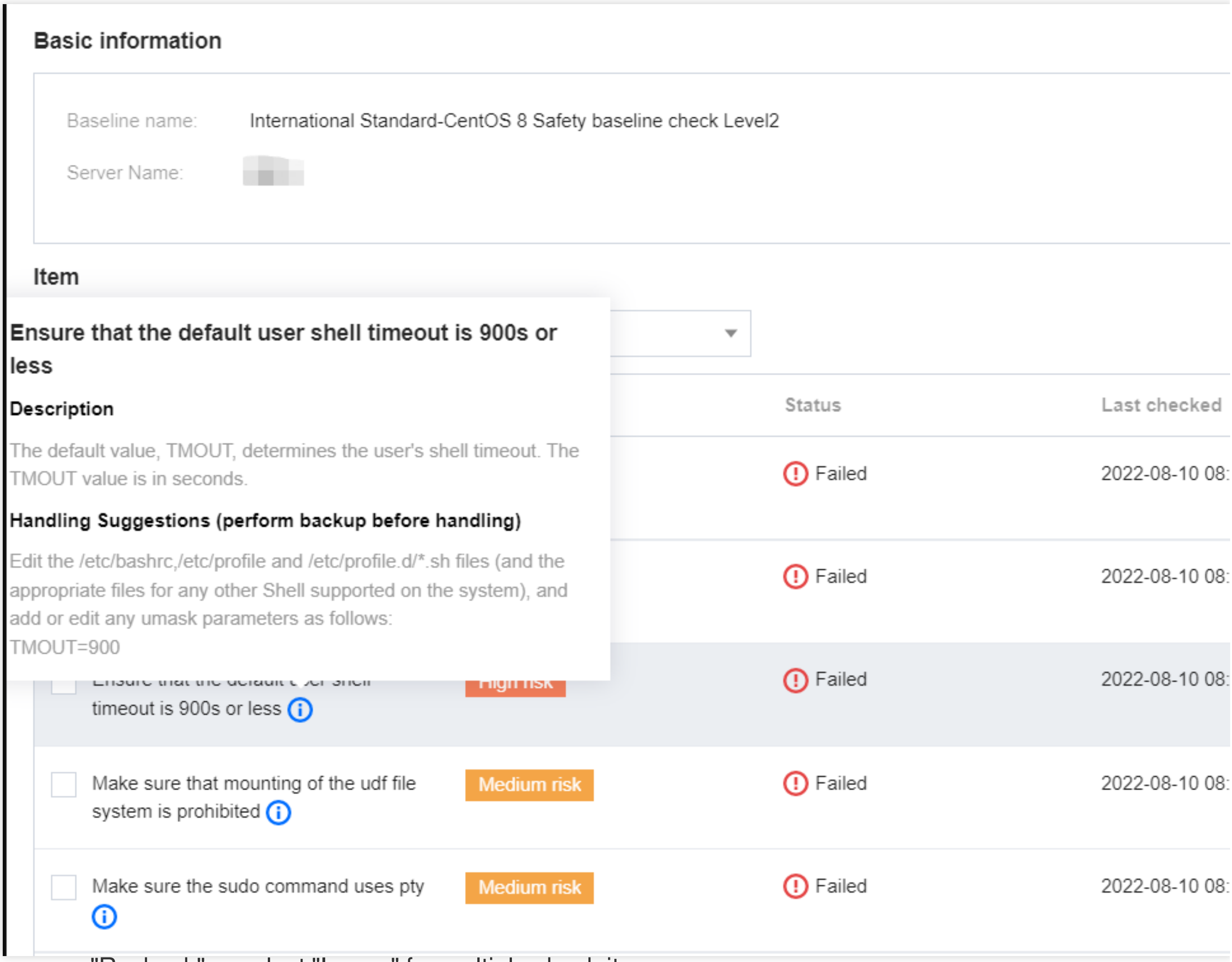


Affected servers

□	Server IP/Name	Passed items	Risk items	First checked	Last checked	Status
□	[redacted]	54	64	2022-07-28 19:56:04	2022-08-10 08:20:05	Failed

Total items: 1

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



Basic information

Baseline name: International Standard-CentOS 8 Safety baseline check Level2

Server Name: [redacted]

Item

Ensure that the default user shell timeout is 900s or less

Description

The default value, TMOUT, determines the user's shell timeout. The TMOUT value is in seconds.

Handling Suggestions (perform backup before handling)

Edit the /etc/bashrc,/etc/profile and /etc/profile.d/*.sh files (and the appropriate files for any other Shell supported on the system), and add or edit any umask parameters as follows:

TMOUT=900

			Status	Last checked
			Failed	2022-08-10 08:
			Failed	2022-08-10 08:
□	Ensure that the default user shell timeout is 900s or less ⓘ	High risk	Failed	2022-08-10 08:
□	Make sure that mounting of the udf file system is prohibited ⓘ	Medium risk	Failed	2022-08-10 08:
□	Make sure the sudo command uses pty ⓘ	Medium risk	Failed	2022-08-10 08:

You can run a "Recheck" or select "Ignore" for multiple check items.

You can filter check items by threat level or status.

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

©2013-2022 Tencent Cloud. All rights reserved.

Critical File Monitor

Last updated：2023-12-26 16:32:49

This document describes how to use the Critical File Monitor feature.

Overview

Based on Tencent Cloud's adaptive learning technology, this feature allows you to monitor critical files in real time based on system rules and custom rules. If suspicious access to a file is detected, the system will send you an alert in real time.

Limits

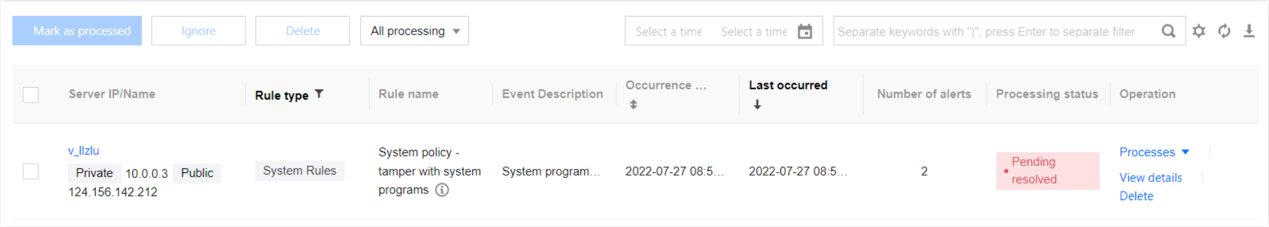
The Critical File Monitor feature is available only if you have at least one server bound to a (CWPP Pro/Ultimate) license.
Only Linux kernel 3.10 or above is supported.

Operation Guide

1. Log in to the CWPP console.
2. Click **Advanced Defense** > **Critical File Monitor** on the left sidebar. The fields and operations related to the feature are described as follows.

Event List

In the **Event List**, you can view and handle the risks related to core files (file is tampered with or files are added) that are detected by CWPP.



□	Server IP/Name	Rule type	Rule name	Event Description	Occurrence ...	Last occurred	Number of alerts	Processing status	Operation
□	v_llzlu Private 10.0.0.3 Public 124.156.142.212	System Rules	System policy - tamper with system programs ⓘ	System program...	2022-07-27 08:5...	2022-07-27 08:5...	2	• Pending resolved	Processes View details Delete

Field description:

Server IP/Name: The server where the core file risk was detected.

Rule Category: System rule or custom rule.

Matched Rule Name: The name of the matched system rule or custom rule.

Event Description: A description of the core file risk.

Occurrence time: The time when the core file risk event first occurred.

Last Occurred: The time when the core file risk was last detected.

Status: **Pending processed**, **Allowed**, **Processed manually** and **Ignored**

Operation

Details: You can view more information about core file risks, such as process information and risk description.

Actions

Mark as processed: Please handle the risk manually by referring to "Solutions" in the event details, and then mark the event as "Handled".

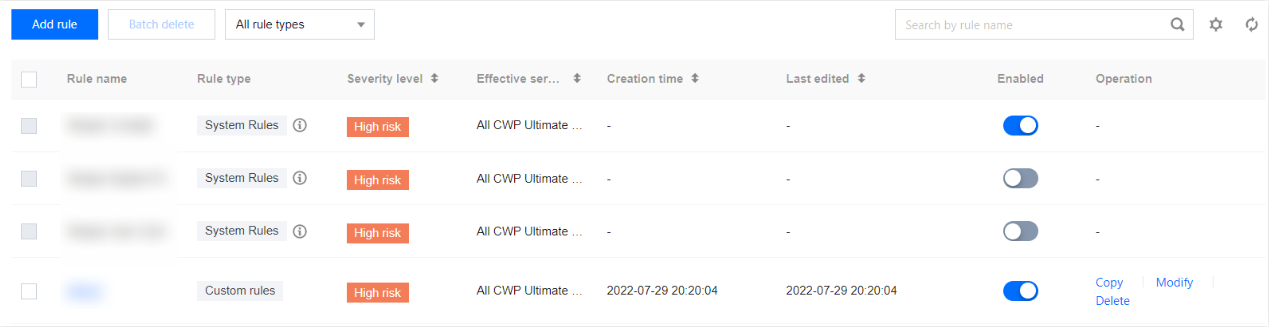
Add to Allowlist: Once an event is added to the allowlist, no alert will be sent if the same event occurs again.

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

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

Configure Monitoring Rules

In **Configure Monitoring Rules**, you can configure allow/alert rules for the core file access processes and add, delete, edit and check the rules.



□	Rule name	Rule type	Severity level	Effective ser...	Creation time	Last edited	Enabled	Operation
□	[redacted]	System Rules	High risk	All CWP Ultimate ...	-	-	●	-
□	[redacted]	System Rules	High risk	All CWP Ultimate ...	-	-	○	-
□	[redacted]	System Rules	High risk	All CWP Ultimate ...	-	-	○	-
□	[redacted]	Custom rules	High risk	All CWP Ultimate ...	2022-07-29 20:20:04	2022-07-29 20:20:04	●	Copy Modify Delete

Note:

System rules take effect on all servers on which CWPP Ultimate is installed. They can only be enabled or disabled, and cannot be edited or deleted.

Field description:

Rule Name: The name of the core file monitoring rule.

Rule Category

System Rule: System rules are configured by Tencent's CWPP operation experts and algorithm experts based on multiple models and apply to most scenarios for monitoring the tampering with users' settings.

Custom Rule: The rule configured by users.

Threat Level: High, Medium, Low, None.

Covered Servers: The range of servers on which a rule takes effect.

Creation time: The time when the rule was created.

Last Edited: The time when the rule was last edited.

Enabled: On/Off.

Operation

Copy: Copy an existing rule for editing.

Edit: Edit the range of servers on which a rule takes effect.

Delete: Delete rules.

©2013-2022 Tencent Cloud. All rights reserved.

Log Analysis

Last updated：2024-05-14 10:20:05

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

Restrictions

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

Log Category	Log Type	Log Description	Supported Versions
Alarm Log	Intrusion detection	Malicious file scan, unusual login, password cracking, malicious requests, high-risk commands, local privilege escalation, and reverse shell.	Professional edition and Flagship edition
	Vulnerability Management	Emergency vulnerabilities, Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities.	Professional edition and Flagship edition
	Baseline Management	Security baseline	Professional edition and Flagship edition
	Advanced Defense	Core file monitoring	Flagship edition
	Client-Related	Client offline and client uninstallation	Basic edition and later

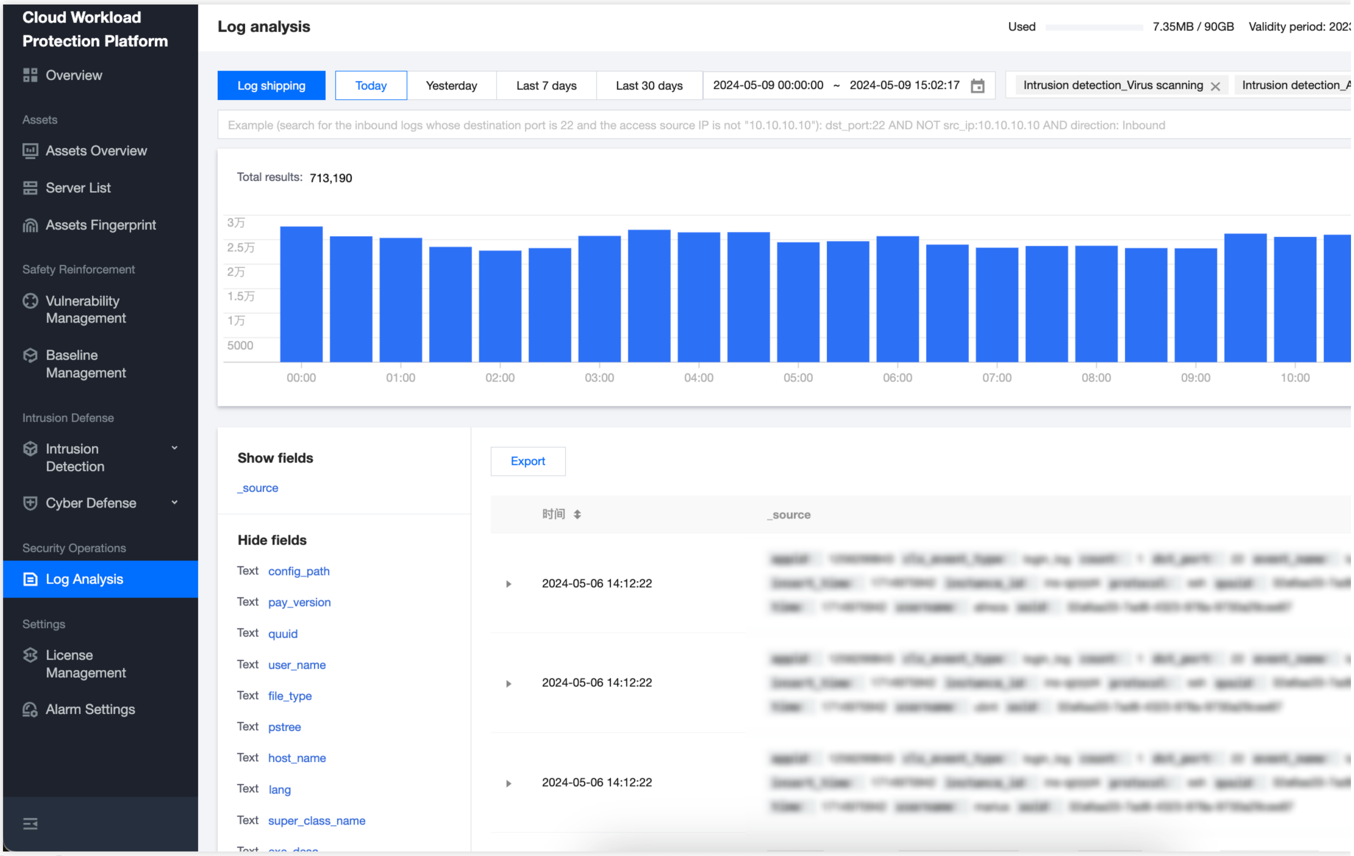
To use the log shipping feature, you must first purchase a TDMQ for CKafka instance, and select the appropriate CKafka instance specification based on the volume of logs to be shipped.

The log shipping feature only supports using a single TDMQ for CKafka account for shipping.

According to the Cybersecurity Law, the log storage duration must be at least 6 months. It is recommended that each server be configured with a storage capacity of 20 - 40 GB to collect and retain log data.

Operation Guide

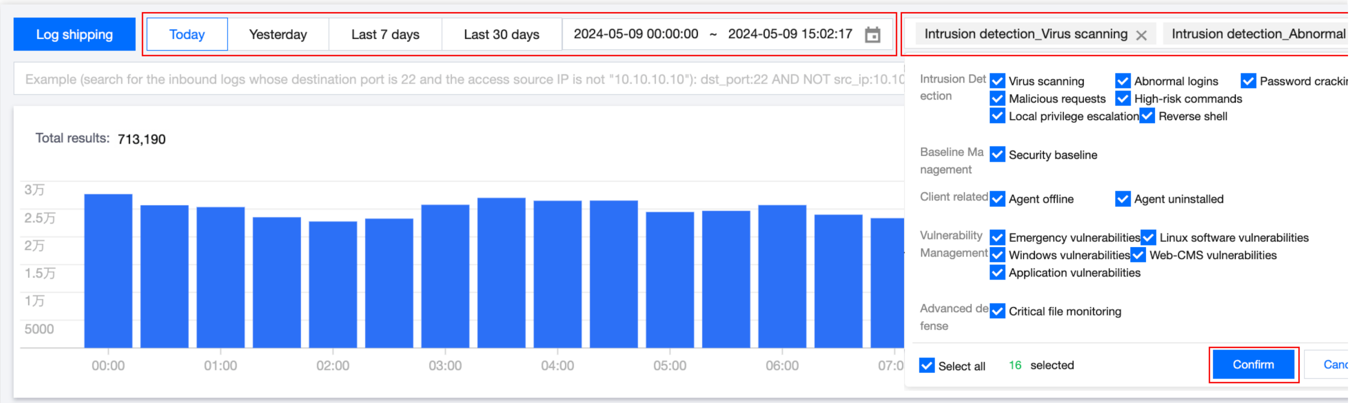
1. Log in to the Host Security console.
2. In the left sidebar, choose **Log Analysis** to perform operations such as log query and log shipping.



Viewing Log

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

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


Log shipping
Today
Yesterday
Last 7 days
Last 30 days
2024-05-09 00:00:00 ~ 2024-05-09 15:02:17
Intrusion detection_Virus scanning
Intrusion detection_Abnormal
Example (search for the inbound logs whose destination port is 22 and the access source IP is not "10.10.10.10"): dst_port:22 AND NOT src_ip:10.10
Total results: 713,190
3万
2.5万
2万
1.5万
1万
5000
00:00
01:00
02:00
03:00
04:00
05:00
06:00
07:0
Confirm
Canc

Intrusion Detection: ☑ Virus scanning ☑ Abnormal logins ☑ Password crackin ☑ Malicious requests ☑ High-risk commands ☑ Local privilege escalation ☑ Reverse shell

Baseline Management: ☑ Security baseline

Client related: ☑ Agent offline ☑ Agent uninstalled

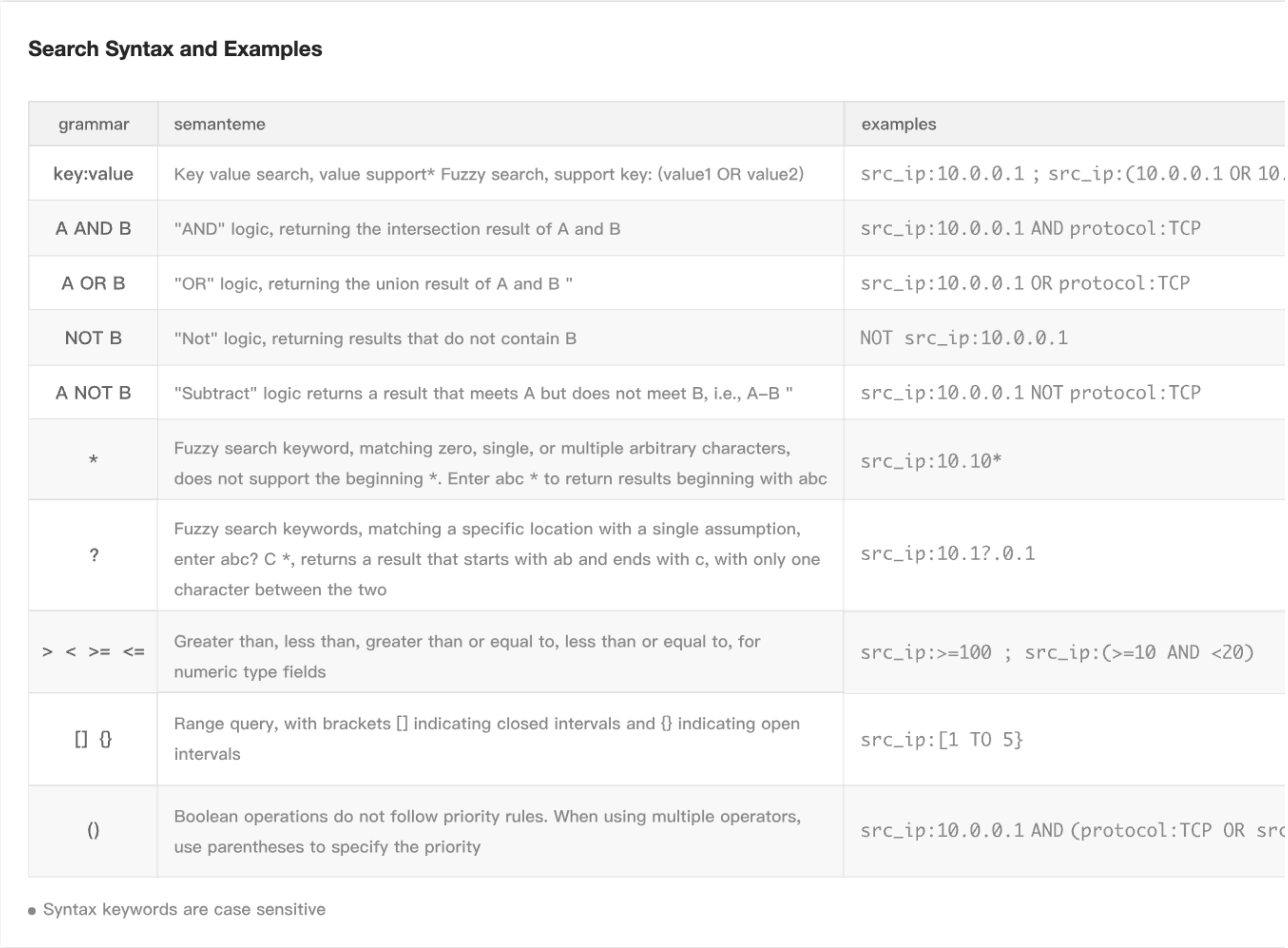
Vulnerability Management: ☑ Emergency vulnerabilities ☑ Linux software vulnerabilities ☑ Windows vulnerabilities ☑ Web-CMS vulnerabilities ☑ Application vulnerabilities

Advanced defense: ☑ Critical file monitoring

☑ Select all 16 selected

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

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

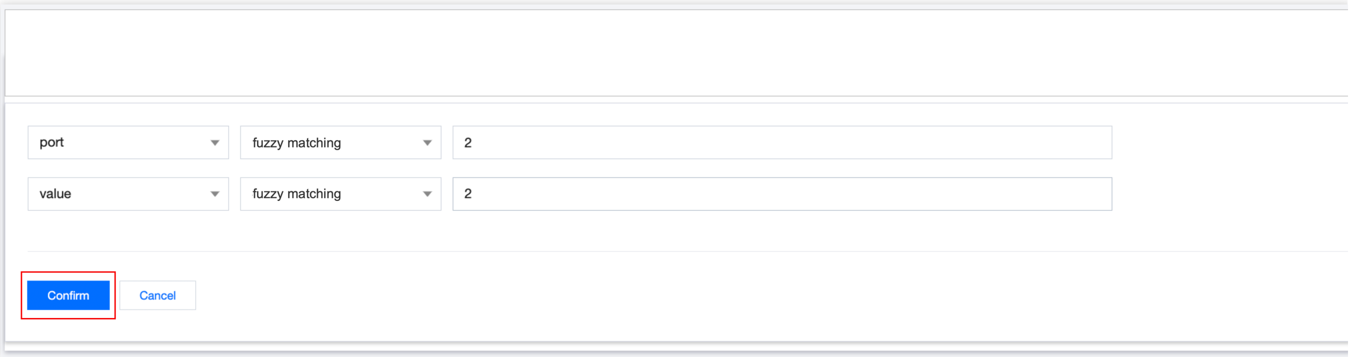


Search Syntax and Examples

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

- Syntax keywords are case sensitive

Choose Field Match Filter: Click 🔍. Choose the appropriate field and operator from the drop-down list. Enter the corresponding field value, and then click **Confirm** to filter.

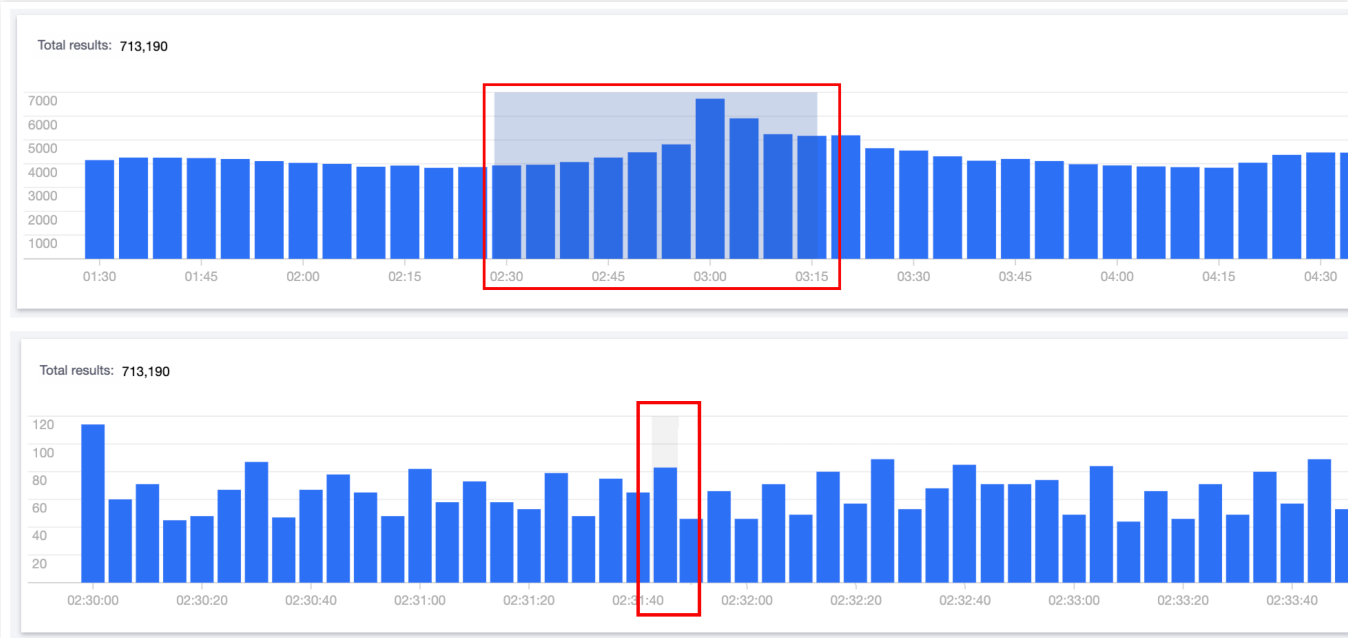


port	fuzzy matching	2
value	fuzzy matching	2

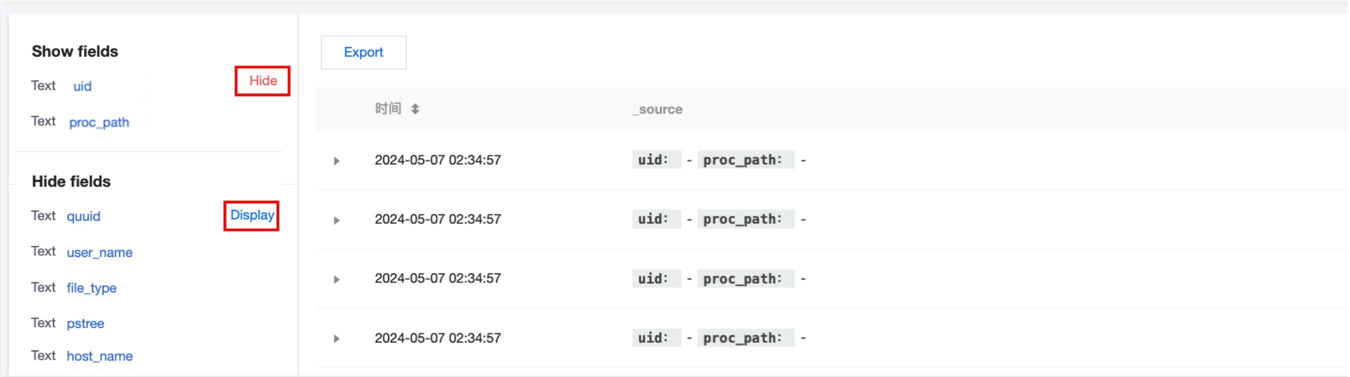
Note:

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

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



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



Show fields

- Text uid — Hide
- Text proc_path

Hide fields

- Text quuid — Display
- Text user_name
- Text file_type
- Text pstree
- Text host_name

时间 ⇕	_source
2024-05-07 02:34:57	uid: - proc_path: -
2024-05-07 02:34:57	uid: - proc_path: -
2024-05-07 02:34:57	uid: - proc_path: -
2024-05-07 02:34:57	uid: - proc_path: -

Click **Export** to export logs that meet the search criteria as a file. Download it through the browser to a local directory.

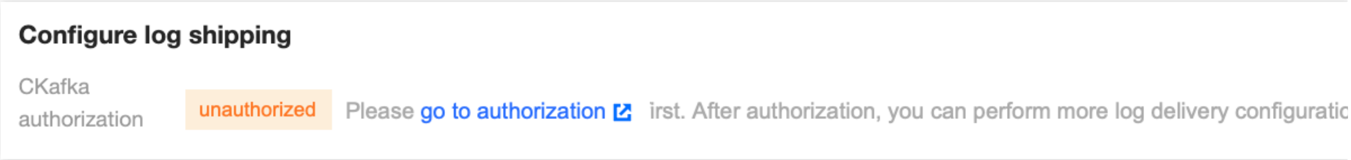
Note:

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

Log Shipping

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

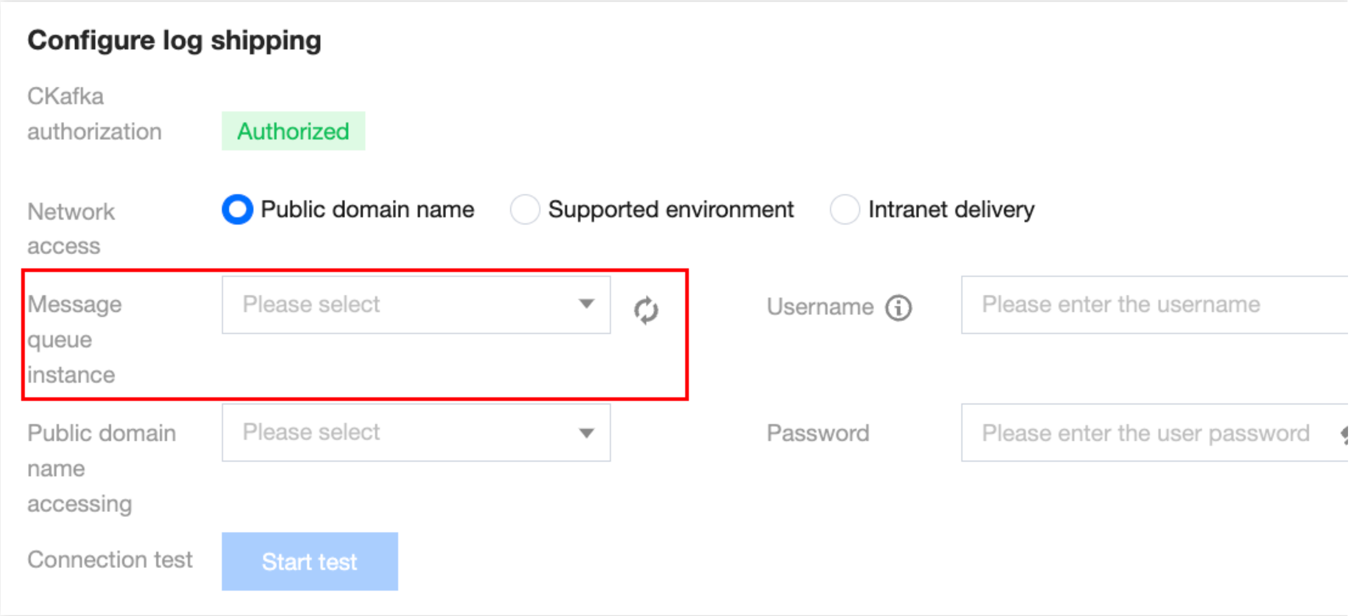
1. Click **Log Shipping** on the top left corner to open the log shipping configuration pop-up. If the CKafka service is not authorized for the first time, click **Go to Authorize** first. After agreeing to the service authorization, you may make more log shipping configurations.



Configure log shipping

CKafka authorization: unauthorized Please go to authorization irst. After authorization, you can perform more log delivery configuratic

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



Configure log shipping

CKafka authorization: Authorized

Network access: ● Public domain name ○ Supported environment ○ Intranet delivery

Message queue instance: Please select

Username: Please enter the username

Public domain name accessing: Please select

Password: Please enter the user password

Connection test: Start test

3. Choose the network access method.

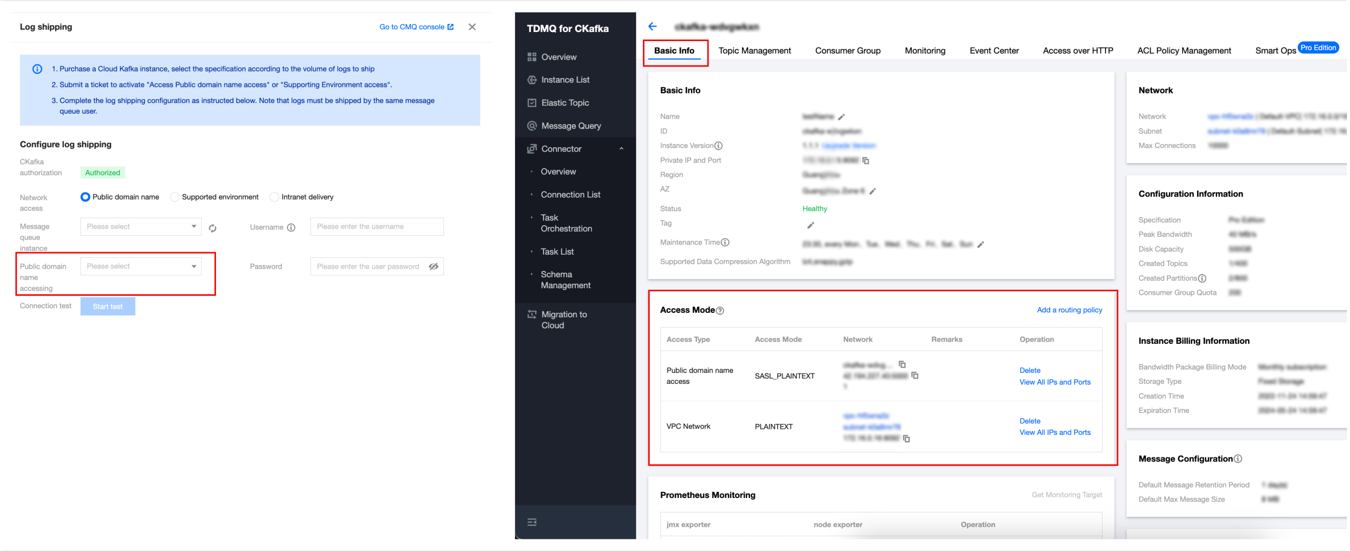
Network Access Method	Description	Optional Routing Instructions
Public domain name access.	Logs are shipped through the public network.	This is the designated access method for TDMQ for CKafka instances.
Supporting environment access.	Logs are shipped through Tencent Cloud's private network. It offers higher performance.	This is the designated access method for TDMQ for CKafka instances. But the PLAINTEXT access method is currently not supported.

©2013-2022 Tencent Cloud. All rights reserved.

Private network shipping.	Logs are shipped through Tencent Cloud's private network without the need for users to configure routing in CKafka. An invisible private network routing is automatically created to support the access.	-

Note:

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



Log shipping

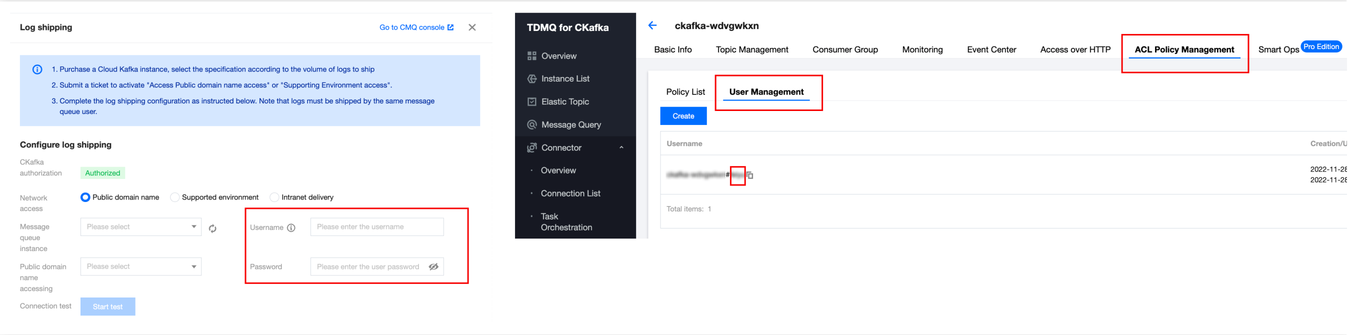
1. Purchase a Cloud Kafka instance, select the specification according to the volume of logs to ship
2. Submit a ticket to activate "Access Public domain name access" or "Supporting Environment access".
3. Complete the log shipping configuration as instructed below. Note that logs must be shipped by the same message queue user.

Configure log shipping

CKafka authorization: Authorized

Network access: ● Public domain name ○ Supported environment ○ Intranet delivery

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



Log shipping

1. Purchase a Cloud Kafka instance, select the specification according to the volume of logs to ship
2. Submit a ticket to activate "Access Public domain name access" or "Supporting Environment access".
3. Complete the log shipping configuration as instructed below. Note that logs must be shipped by the same message queue user.

Configure log shipping

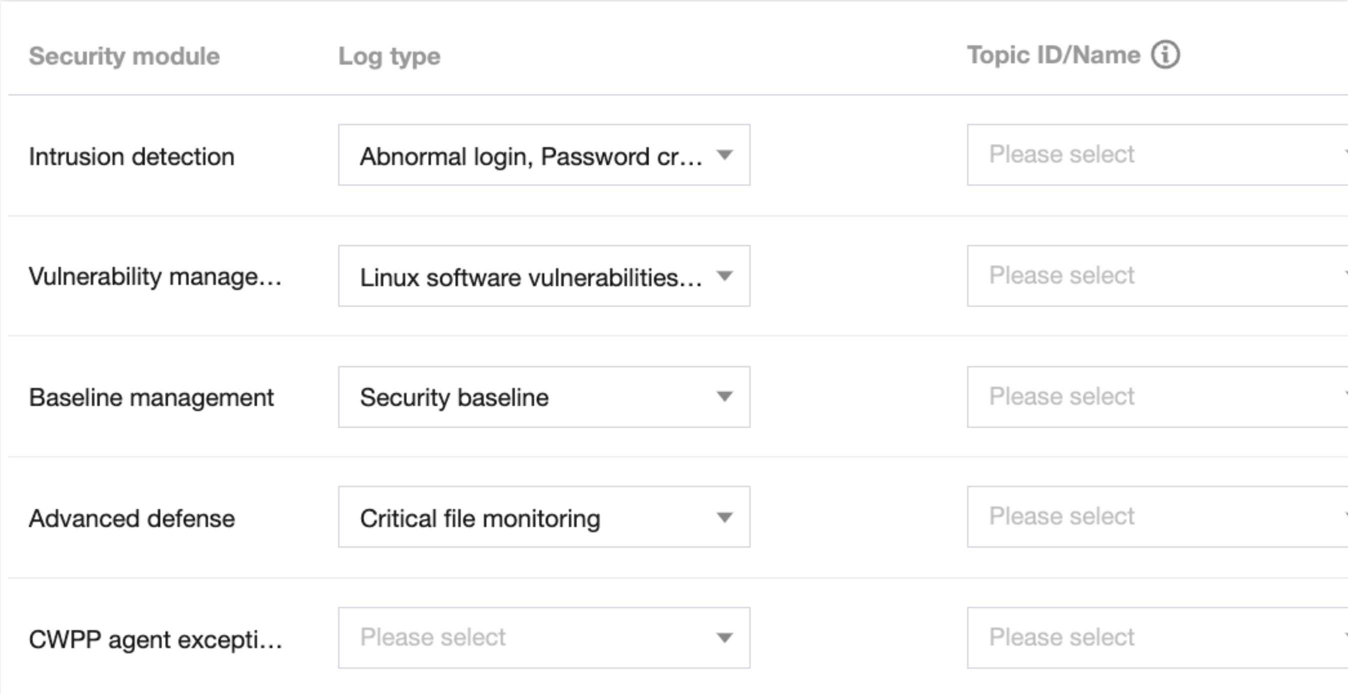
CKafka authorization: Authorized

Network access: ● Public domain name ○ Supported environment ○ Intranet delivery

ckafka-wdvgwkxn

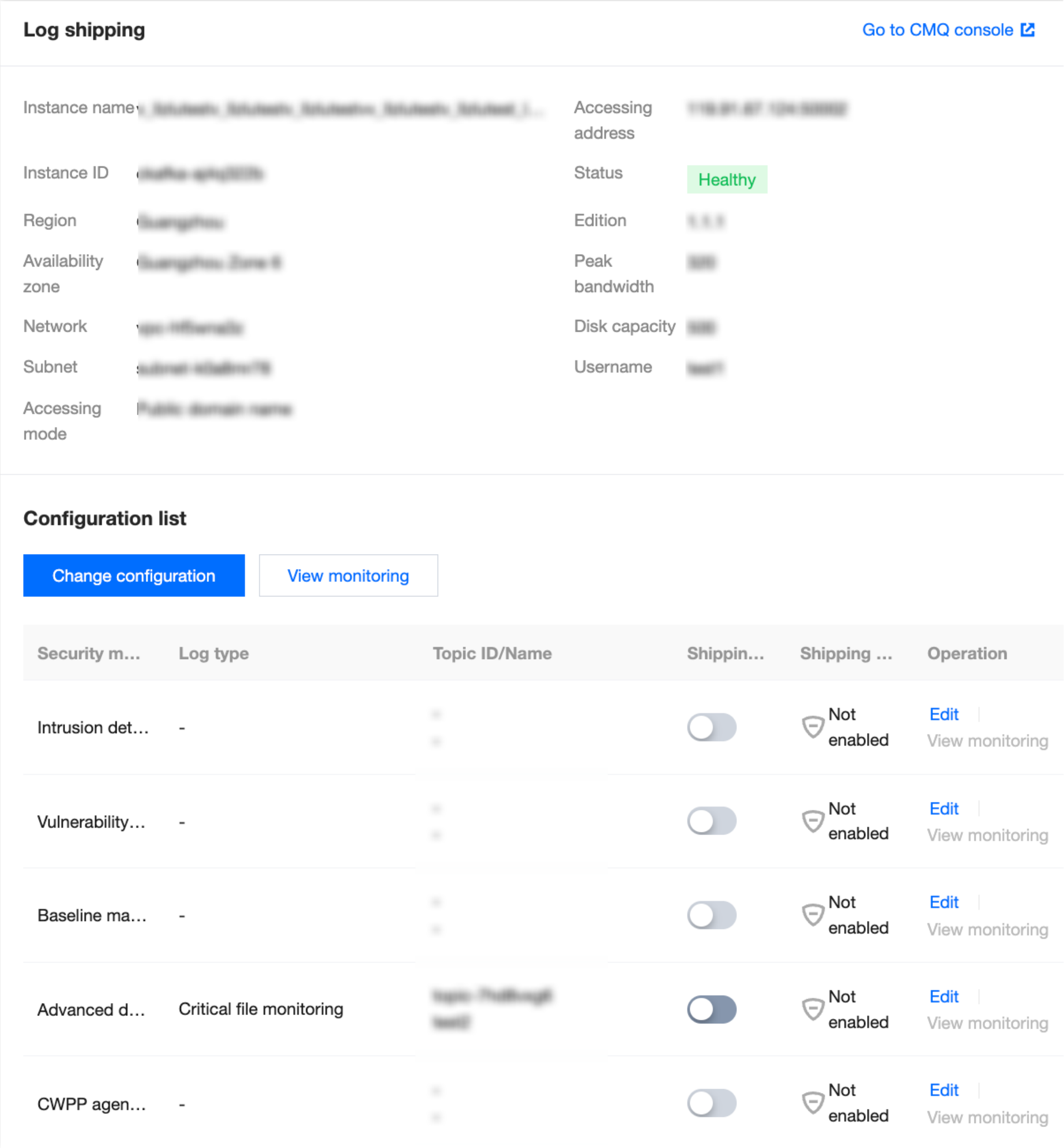
Total items: 1

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



Security module	Log type	Topic ID/Name
Intrusion detection	Abnormal login, Password cr…	Please select
Vulnerability manage…	Linux software vulnerabilities…	Please select
Baseline management	Security baseline	Please select
Advanced defense	Critical file monitoring	Please select
CWPP agent excepti…	Please select	Please select

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



Log shipping

Go to CMQ console

Instance name	[redacted]	Accessing address	[redacted]
Instance ID	[redacted]	Status	Healthy
Region	[redacted]	Edition	[redacted]
Availability zone	[redacted]	Peak bandwidth	[redacted]
Network	[redacted]	Disk capacity	[redacted]
Subnet	[redacted]	Username	[redacted]
Accessing mode	[redacted]		

Configuration list

Change configuration | View monitoring

Security m...	Log type	Topic ID/Name	Shippin...	Shipping ...	Operation
Intrusion det...	-	[redacted]	○	Not enabled	Edit | View monitoring
Vulnerability...	-	[redacted]	○	Not enabled	Edit | View monitoring
Baseline ma...	-	[redacted]	○	Not enabled	Edit | View monitoring
Advanced d...	Critical file monitoring	[redacted]	○	Not enabled	Edit | View monitoring
CWPP agen...	-	[redacted]	○	Not enabled	Edit | View monitoring

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

Note:

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

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

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

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

©2013-2022 Tencent Cloud. All rights reserved.

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

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

Note:

Reconfiguration will interrupt the current shipping process.

©2013-2022 Tencent Cloud. All rights reserved.

Cloud Access Management

Last updated：2023-12-26 16:33:19

Background

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

Your key is shared by multiple users, posing huge risks of data breaches.

Your users might introduce security risks from misoperations due to the lack of user access control.

In this case, you can create multiple users in CAM to take charge of different services, and give them permissions on different consoles by associating policies. This document provides samples to guide you on how to use the CWPP access policies.

Samples

Full access policy

To grant your users full access to all CWPP APIs, you need to associate the policy QcloudCWPPFullAccess with them.

See Authorization Management to grant users full access with the preset policy QcloudCWPPFullAccess.

Read-only policy

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

See Authorization Management to grant users read-only access with the preset policy QcloudCWPPReadOnlyAccess.

Custom policies

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

Note:

New users will not be associated with any CWPP policies by default, indicating they do not have any permissions. For more information, see Overview.

©2013-2022 Tencent Cloud. All rights reserved.