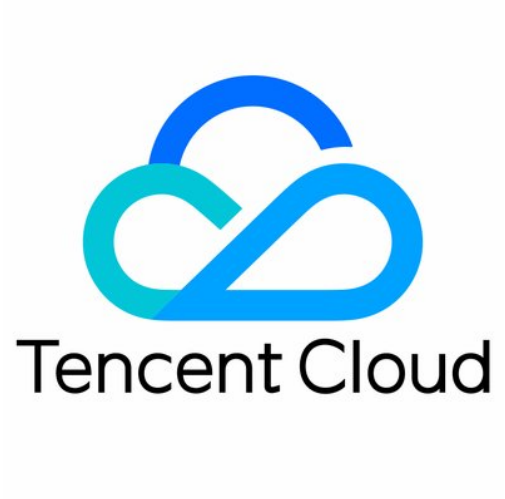
Cloud Workload Protection

Operation Guide

Product Documentation



Contents

Operation Guide
Security Overview

Last updated : 2020-05-14 10:31:28

Prerequisites

The new version of the security overview feature is currently in beta test and can be used only by accounts randomly chosen by the beta test system.

Overview

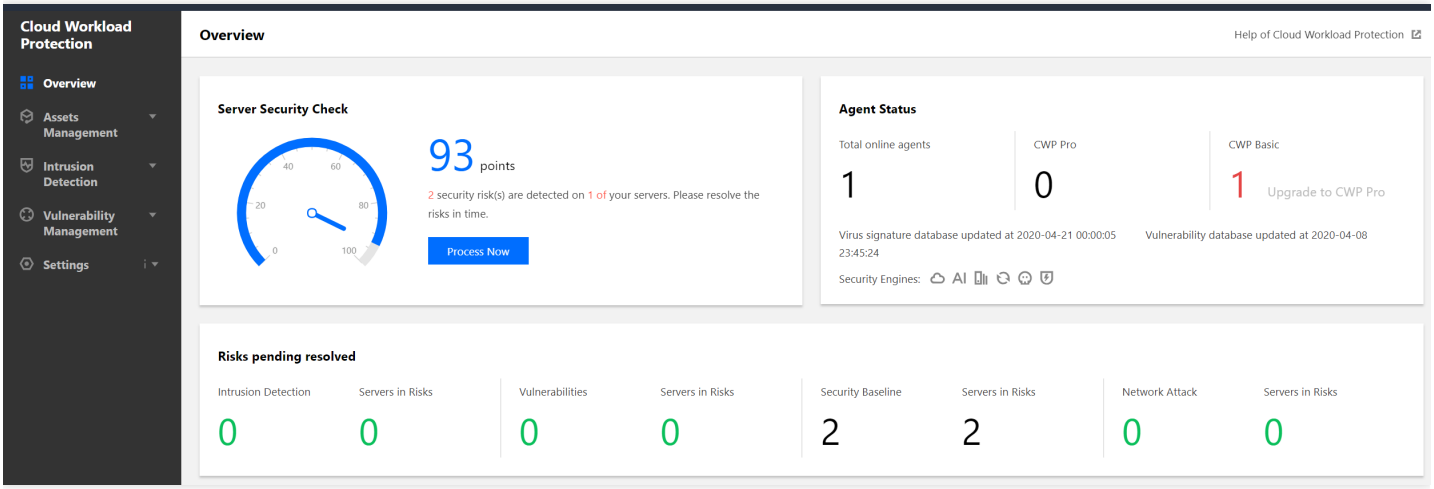
As the server security information display and processing center, the Security Overview page of CWP can display the server health check score, protection status, risks to be processed, risk trend, and overall server security status in real time. In addition, it provides CWP help documentation and suggestions on CWP upgrade service, helping you defend against intrusions and attack threats to protect your workload security.

Feature Overview

Log in to the CWP Console and click **Security Overview** on the left sidebar to enter the security overview page which provides security overview information and relevant operations. The features of its modules are as described below:

Server security health check

The server security health check feature can score your servers through security health checks and provide the numbers of servers and security risks. Click **Process Now** to enter the risk processing page where you can directly process detected intrusions and network defense risks and manage vulnerabilities.



The server security status has the following three levels:

Risk Level	Health Check Score	Font Color	Description
Low	90–100	Green	Your asset security status is excellent. Please maintain the status and perform routine inspection.
Medium	60–89	Orange	Your asset has many security risks. You are recommended to solve them promptly.
High	20–59	Red	Your asset has severe security risks. Please solve them as soon as possible.

> The lowest health check score for server security is 20.

The score penalties are calculated by security event category. The security event levels and penalty rules are as follows:

Level	Security Event (Counted by Event Quantity)	Penalty Per Event	Maximum Total Penalty
Severe	Trojan, virus, and successful intrusion.	-50	-80
High	High-risk vulnerability, high-risk baseline risk, and unusual login location.	-10	-60
Medium	Medium-risk vulnerability and baseline risk.	-3	-30

Level	Security Event (Counted by Event Quantity)	Penalty Per Event	Maximum Total Penalty
Low	Low-risk vulnerability and baseline risk.	-2	-20
Other	CWP Basic (unprotected status).	-1	-10

Protection status

The protection status section displays the total number of currently online severs, number of CWP Pro-protected online servers, and number of CWP Basic-protected servers as well as virus library date, vulnerability library date, and security engine protection information.

- In the detection module of CWP Basic, click **Upgrade to Pro** to enter the CWP upgrade page. You can make a payment to upgrade from CWP Basic to CWP Pro for those servers for more powerful risk and threat defense capabilities.
- Security engine protection will display 6 engine icons, which represent engines of cloud-based antivirus, AI, virtual machine detection, exception analysis, threat intelligence, and attack protection, respectively. If you have not activated CWP Pro, these icons are grayed out, and after you activate CWP Pro, they will be available.

Pending risks

The pending risks section displays the number of server risks to be processed and the number of affected servers. You can click a risk event or its occurrence quantity to enter the corresponding risk processing page.
The data of pending risks is synced in real time and can be divided into the following 4 categories:

- **Intrusions**: this module provides detection and auditing for 7 types of intrusions, namely, trojans, unauthorized logins, brute force attacks, malicious requests, reverse shells, local privilege escalation, and high-risk commands. It also displays the numbers of risks and affected servers.
- **Vulnerabilities**: this module detects vulnerabilities in web applications and system components and display the numbers of vulnerabilities and affected servers.
- **Security baseline**: this module only displays the numbers of baseline risks and affected servers.
- **Network attacks**: this module displays the numbers of attacks and affected servers.

Risk trend

The risk trend section displays a line chart of the trend in security risks and threats in the last 7, 14, or 30 days and allows you to view the trend by time period. You can hover your mouse on the trend chart to view the numbers of risks and threats such as trojans, viruses, brute force attacks, suspicious logins, vulnerabilities, and baseline risks on the corresponding date.

Real-Time updates

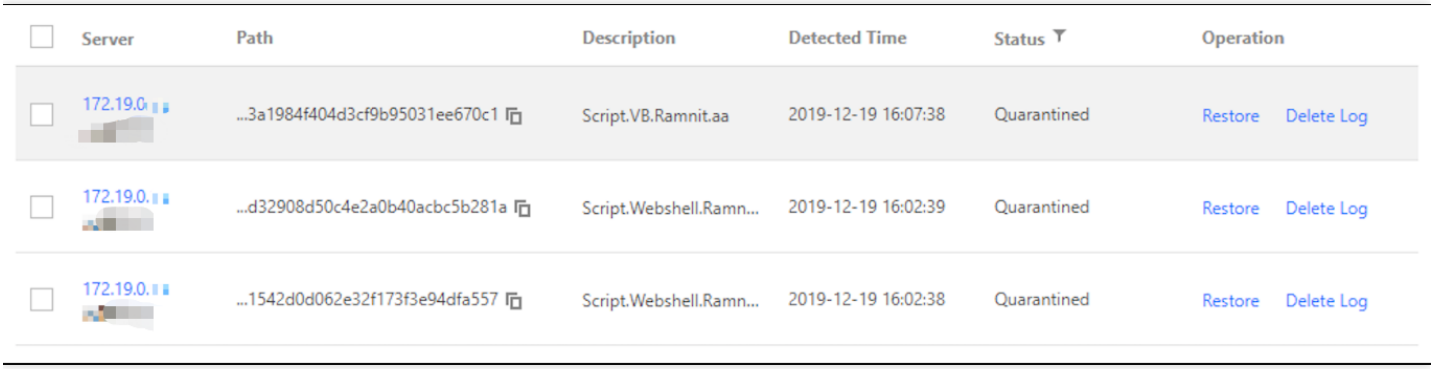
The real-time updates section displays real-time server risks and threat events in reverse chronological order.

- Click **Server IP** to enter the corresponding tab on the "Server Details" page.
- Hover your mouse on an update and click **Process Now** on the right to enter the corresponding event processing page.

Trojan Operation and Handling

Last updated : 2020-03-02 19:27:31

Log in to the CWP Console and select **Intrusion Detection** > **Trojans** to view the trojan detection records, as shown below:



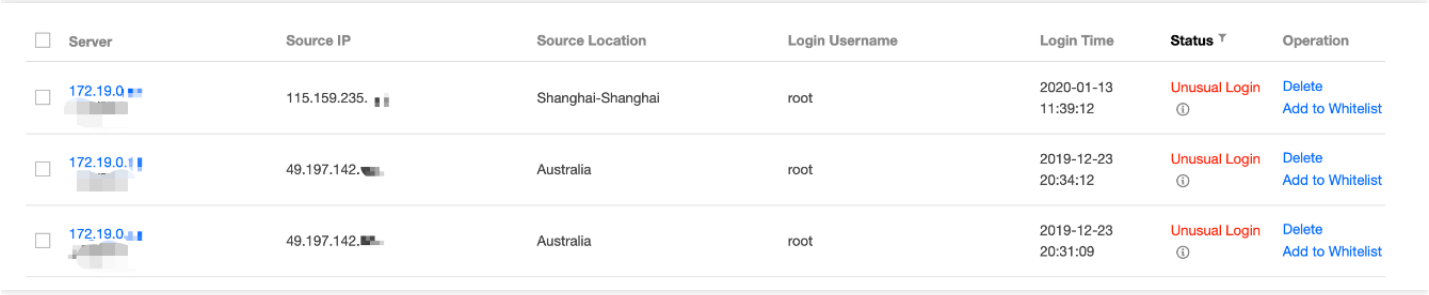
Dealing with suspicious files

- **Quarantine**
  After malicious files are confirmed, you can quarantine a single file or multiple files in batches. After successful quarantine, the original malicious files will be encrypted and quarantined. You can filter **quarantined** files to recover them in the future if necessary.
- **Trust**
  If a file is not malicious, you can trust it. After the file is added to the trust list, CWP will not inspect it again. You can filter the **trusted files** to manage them.
- **Delete Log**
  After a record is deleted, you cannot view related information. You are recommended to **quarantine** or **trust** a file before deleting it. You can also go to the file path to manually delete it.

Login Audit Operation

Last updated : 2020-07-30 12:04:09

CWP collects RDP and SSH login logs on the host and features login audit, which displays all login transactions on the host and marks suspicious login behaviors.



Server	Source IP	Source Location	Login Username	Login Time	Status	Operation
172.19.0.	115.159.235.	Shanghai-Shanghai	root	2020-01-13 11:39:12	Unusual Login	Delete Add to Whitelist
172.19.0.	49.197.142.	Australia	root	2019-12-23 20:34:12	Unusual Login	Delete Add to Whitelist
172.19.0.	49.197.142.	Australia	root	2019-12-23 20:31:09	Unusual Login	Delete Add to Whitelist

The included fields are described as follows:

- Server: the server currently logged in to.
- Source IP Address: IP address of the login source. Generally, it is an egress IP address of a network or a network proxy IP address.
- Source Location: the location where the source IP address locates.
- Login Username: the username used by the user who successfully logged in to the server.
- Login Time: the time at which login was successfully made (server's time with time zone information)
- Status:
  - Normal: CWP detects that the login request is from a common login location and marks it as a normal login.
  - Unusual login location: CWP detects that the login is performed at an unusual location. It may be caused by password leakage or an intended login by an admin at an unusual location.
- Operation:
  - Allowlist: if you think that a logged login is normal, you can click **Allowlist** to add it to the custom login allowlist and set it to normal login.
  - Delete: delete the log. A deleted log will not be displayed again.