

Cloud Workload Protection Platform

FAQs

Product Documentation



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



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.

FAQs

Last updated : 2023-12-26 16:40:40

This topic lists FAQs about CWPP.

Purchase

How can I purchase CWPP Pro and CWPP Ultimate?

See [Purchasing Protection Licenses](#).

Does CWPP conflict with other security products?

CWPP does not conflict with other security products. It protects servers by providing security capabilities in different dimensions than other products.

How do I disable CWPP Pro or CWPP Ultimate?

Log in to the [CWPP Console](#) and select **License Management** in the left navigation pane. Search for the servers for which you want to disable CWPP Pro or CWPP Ultimate, and then click **Unbind** in the operation column to disable the service. See [License Management](#).

How do I uninstall CWPP Agent?

Log in to the [CWPP Console](#) and select **Server List** in the left navigation pane. Search for the servers from which you want to uninstall CWPP Agent, and then click **Unbind** in the operation column to uninstall CWPP Agent (the latest status will be synced in about 10 minutes.)

Features

How often are the virus and vulnerability libraries updated?

Virus library: updated at 00:00 every day.

Vulnerability library: updated from time to time.

Why may the detection results be different between multiple scans of the vulnerabilities of Jar packages?

The detection of Jar package vulnerabilities, for example, Struts2 vulnerability highly dependent on whether the Jar package is loaded. The vulnerability cannot be detected when the package is not loaded. When the service is running, the Webserver loads the Jar package in two modes — dynamic loading and static loading. In the dynamic loading

mode, the Struts2 vulnerability can only be detected when the Jar package is running, so the check results are different between periods. It is recommended to scan for high-risk Jar package vulnerabilities multiple times to improve the accuracy of the check results.

What is the scanning frequency of files in the malicious file scan?

You can set the scanning frequency of files. For more information, see [Malicious File Scan](#).

How does the security scoring mechanism work?



See [Security Score Overview](#).

How long does it take for security baselines to take effect once they are configured in the product?

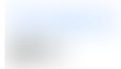

The security baselines take effect immediately after their configuration.

What should be done if the result of a security baseline check item is "Failed"?

1. Go to [Baseline Management](#), filter out the check items with a result of "Failed", and click **View Details** to open the details pop-up window.

<input type="checkbox"/> Baseline name	Check items	Affected servers	Last checked	Proc
<input type="checkbox"/> International Standard-CentOS 8 Safety baseline check Level1	86	1	2022-08-10 08:20:05	 f
<input type="checkbox"/> International Standard-CentOS 8 Safety baseline check Level2	118	1	2022-08-10 08:20:05	 f

2. In the check item details pop-up window, you can see the affected servers. Click **Details** in the operation column of a server to open the check result pop-up window.

<input type="checkbox"/> Server IP/Name	Passed items	Risk items	First checked	Last checked	Status
<input type="checkbox"/> 	51	35	2022-07-28 19:56:04	2022-08-10 08:20:05	 Fai

Total items: 1

10 / page

3. In the check result pop-up window, you can view the suggestions on how to fix the failed baseline items.

Basic information

Baseline name: International Standard-CentOS 8 Safety baseline check Level1

Server Name: 国际4

Item

Ensure that locks with failed password attempts have been configured

Description

Lock out the user after n consecutive failed login attempts.

Handling Suggestions (perform backup before handling)

Create or edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files to contain the following:

Auth required pam_faillock.so preauth silent deny=5 unlock_time=900

Auth required pam_faillock.so authfail deny=5 unlock_time=900

Status	Last checked
Failed	2022-08-10 08:00
Failed	2022-08-10 08:00
Failed	2022-08-10 08:00

Will I be notified if CWPP detects attacks such as vulnerabilities and Trojans?

Yes. You will get alarms if CWPP detects attacks such as Trojans and critical vulnerabilities, and will be notified via Message Center, SMS, email, or WeCom. You can set your notification channel in [Alarm Settings](#).