Cloud Workload Protection Platform

Quick Start

Product Documentation

Copyright Notice

Trademark Notice

Tencent Cloud

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.

Quick Start

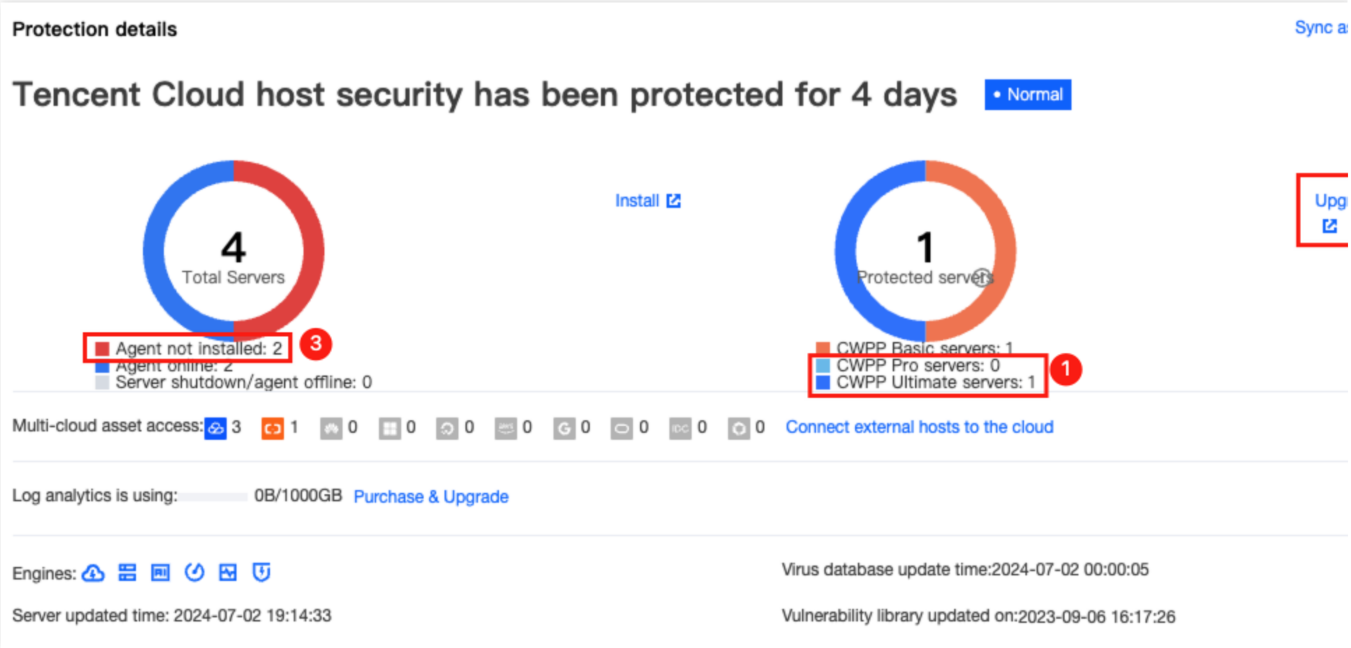
Last updated：2024-08-13 15:56:40

Step 1: Installing CWPP

Log in to the CWPP Console, and go to the Overview page to check if CWPP is installed on CVM.

Note

When purchasing Tencent CVM or CPM 1.0, you can select **Security Reinforcement** to install the CWPP client automatically.



Protection details

Tencent Cloud host security has been protected for 4 days • Normal

Agent not installed: 2

Agent online: 2

Server shutdown/agent offline: 0

CWPP Basic servers: 1

CWPP Pro servers: 0

CWPP Ultimate servers: 1

Multi-cloud asset access: 3 1 0 0 0 0 0 0 0 0 Connect external hosts to the cloud

Log analytics is using: 0B/1000GB Purchase & Upgrade

Engines:

Virus database update time:2024-07-02 00:00:05

Server updated time: 2024-07-02 19:14:33

Vulnerability library updated on:2023-09-06 16:17:26

a. CVM with CWPP installed and Pro or Ultimate edition enabled enjoys comprehensive, multi-dimensional system security protection provided by CWPP.

b. CVM with Basic edition of CWPP installed can upgrade the service to Pro or Ultimate edition by clicking **Upgrade** on the right side.

c. CVM without CWPP can click **Install** on the right side and following the instructions below:

Windows CVM environment

Linux CVM environment

Windows CVM Environment

Supported Versions

The following versions are supported for now:

Windows server 2008, 2012, 2016, 2019, and 2022 (32-bit or 64-bit).

Windows 10 and 11 (64-bit).

CWPP Installation

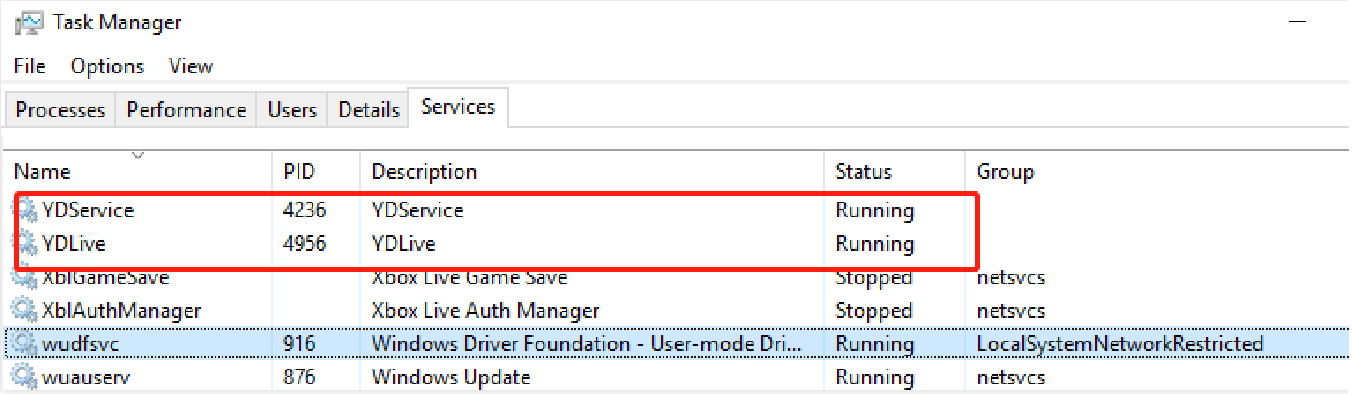
Server Type	Server Products	Server Architecture	Network	Client Download and Installation
Tencent Cloud	CVMs, Lighthouses, CPMs, and Edge Computing Machines	x86	VPC network	Open the cmd command line window, and paste and rur

				 `powershell -executionpolicy bypass -c`
Tencent Cloud	CVMs	x86	Basic network	Open the cmd command line window, and paste and rur

				`powershell -executionpolicy bypass -c`
Non-Tencent Cloud	/	x86	Public network and DC	Due to the restriction of the command validity period, ple

Installation Notes

Verification of successful Windows installation: Open Task Manager and check whether the YDService and YDLive processes are called. If yes, the installation is successful.



Name	PID	Description	Status	Group
YDService	4236	YDService	Running	
YDLive	4956	YDLive	Running	
XblGameSave		Xbox Live Game Save	Stopped	netsvcs
XblAuthManager		Xbox Live Auth Manager	Stopped	netsvcs
wudfsvc	916	Windows Driver Foundation - User-mode Dri...	Running	LocalSystemNetworkRestricted
wuauserv	876	Windows Update	Running	netsvcs

Linux CVM Environment

Supported Versions

The following versions (64-bit) are supported for now:

TencentOS Server

Tencent tlinux

CentOS 6 or later versions

Ubuntu 9.10 or later versions

Debian 6 or later versions

RHEL 6 or later versions

OpenCloudOS

AlmaLinux

openSUSE

Rocky Linux

Red Hat 6 or later versions

Alibaba Cloud Linux

Amazon Linux

CWPP Installation

Server Type	Server Products	Server Architecture	Network	Client Download and Installation
Tencent Cloud	CVMs, Lighthouses, CPMs, and Edge Computing Machines	x86	VPC network	

				`wget http://u.yd.tencentyun.com/ydeyes_`
Tencent Cloud	CVMs	x86	Basic network	

L

```
wget http://u.yd.qcloud.com/ydeyes_lin
```

Tencent Cloud	CVMs, Lighthouses, CPMs, and Edge Computing Machines	ARM	VPC network	

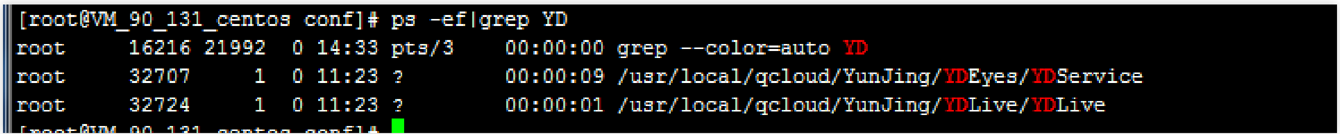
				`wget http://u.yd.tencentyun.com/ydeyes`
Tencent Cloud	CVMs	ARM	Basic network	

				 `wget http://u.yd.qcloud.com/ydeyes_lin`
Non-Tencent Cloud	/	x86, ARM	Public network, DC	Due to the restriction of the command validity period, ple

Installation Notes

Run the command to check whether the YDService and YDLive processes are running. If yes, the installation is successful.

```
ps -ef | grep YD
```



```
[root@VM_90_131_centos conf]# ps -ef|grep YD
root     16216 21992  0 14:33 pts/3    00:00:00 grep --color=auto YD
root     32707     1  0 11:23 ?        00:00:09 /usr/local/qcloud/YunJing/YDEyes/YDService
root     32724     1  0 11:23 ?        00:00:01 /usr/local/qcloud/YunJing/YDLive/YDLive
[root@VM_90_131_centos conf]#
```

Note: If the processes are not running, the program can be started by running the following command via a root user:

```
/usr/local/qcloud/YunJing/startYD.sh
```

Step 2: Operating CWPP

CWPP can process and display the security information of a server in real time. It supports detecting and isolating Trojan files, detecting vulnerabilities, identifying suspicious log-in behaviors and adding them to allowlist, blocking password-cracking attempts, and setting alarms. For details, see Operation Guide.

Step 3: Troubleshooting

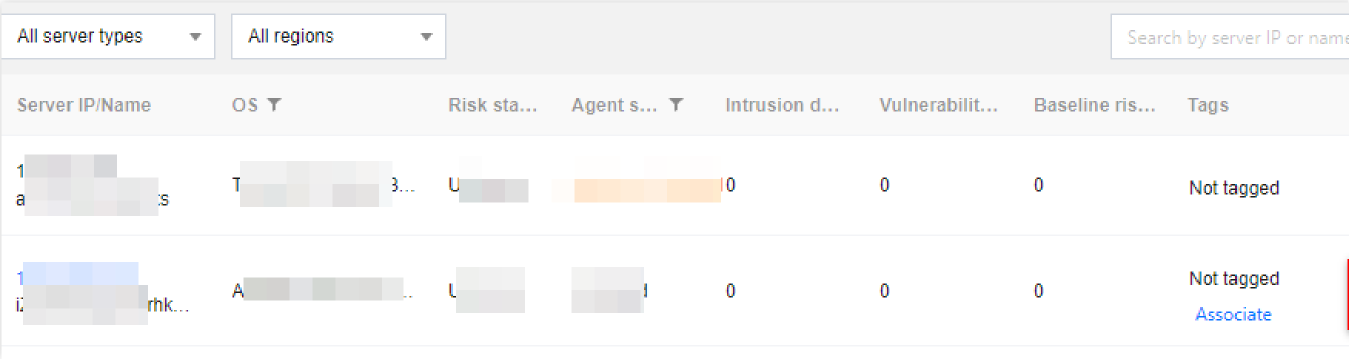
If the host is hacked, you can follow the intrusion troubleshooting guide to troubleshoot the problem and restore the normal running of the website or system. For details, see Intrusions on Linux or Intrusions on Windows.

Step 4: Uninstalling CWPP

If you no longer need CWPP protection, you can uninstall it. There are two ways to uninstall CWPP: via the console and via the system. Here is a detailed introduction:

Uninstalling via the Console

1. Log in to the CWPP Console. Select **Assets** > **Server List** in the left sidebar to check if CWPP is installed on your CVM.
2. In the Server List, select the server where you need to uninstall CWPP. Click **Uninstall agent** in the action bar on the right side.



Server IP/Name	OS	Risk sta...	Agent s...	Intrusion d...	Vulnerabilit...	Baseline ris...	Tags
[redacted]	[redacted]	[redacted]	[redacted]	0	0	0	Not tagged
[redacted]	[redacted]	[redacted]	[redacted]	0	0	0	Not tagged Associate

Uninstalling via the System

Windows System: Follow the path `C:\\Program Files\\QCloud\\YunJing\\uninst.exe` to locate the `uninst.exe` file and double-click to uninstall.

Linux System: Enter the command `if [ -w '/usr' ]; then /usr/local/qcloud/YunJing/uninst.sh ; else /var/lib/qcloud/YunJing/uninst.sh ; fi` to uninstall.

FAQs

How to Handle Firewall Interception During Installation?

It is recommended to allow access to the CWPP backend server addresses in firewall policies:

VPC Domain Names: `s.yd.tencentyun.com, l.yd.tencentyun.com, u.yd.tencentyun.com`

VPC Network IP: `169.254.0.55`

Basic Network Domain Names: `s.yd.qcloud.com, u.yd.qcloud.com, l.yd.qcloud.com`

Basic Network IPs: `10.148.188.202, 10.148.188.201, 11.177.125.116, 11.177.124.86, 11.149.252.57, 11.149.252.62, 11.149.252.51`

Non-Tencent Cloud Public Network Domain Names: `sp.yd.qcloud.com, up.yd.qcloud.com, lp.yd.qcloud.com`

Non-Tencent Cloud Public Network IPs: `120.232.65.223, 157.148.45.20, 183.2.143.163`

Ports: `5574, 8080, 80, 9080 (Public network also needs to allow port 443)`

How to Configure if Not Using Default DNS?

If you are not using the default DNS, you need to forward all resolutions of the root domains `tencentyun.com` and `yd.qcloud.com` to the default DNS.