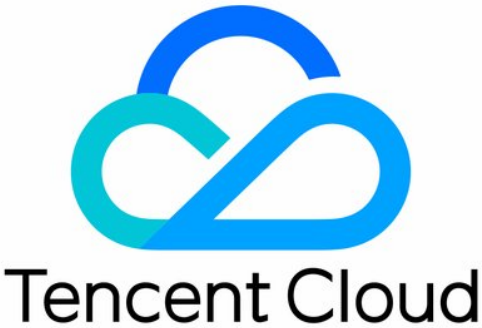
Cloud Workload Protection Platform

Cloud Workload Protection Description

Product Documentation



©2013-2022 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2023 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

Cloud Workload Protection Description
- Feature Description
- Agent Process Description
- Agent Installation Guide
- Security Score Overview

©2013-2022 Tencent Cloud. All rights reserved.

Cloud Workload Protection Description
Feature Description

Last updated：2023-12-26 16:39:11

Web shell detection

Web shells are common in hackers' attacks. The CWPP agent will scan newly created web program files on the server for suspicious risks. For a small number of files that are suspected to be web shells, CWPP reports them to Tencent Cloud, which then conducts further detection through the machine learning detection engine. After detection, the sample files will be deleted in real time. CWPP runs a full scan every day by default. No private data will be extracted in this process.

Abnormal login reminder

The abnormal login reminder allows you to identify abnormal admin logins. The source IP, time, login user name and login status data in the login log need to be collected for computing risks. The login log data is retained on cloud for one month.

Password cracking reminder

Detect password cracking attacks against your server and show you the log and result of the attacks. It collects and analyzes information in the logs, including source IP address, attack time, login username, and login status. The login logs will be retained in the cloud for one month.

Malicious Trojans and virus detection

Malicious Trojans and virus programs usually steal user data or launches attacks, which will consume a large amount of system resources and make your business unable to provide services normally. The CWPP agent will collect the hash values of suspicious programs to the cloud, and the cloud-based scanning and blocking module will inspect the values. If a value is not found in the cloud-based hash value library, the corresponding executable file will be reported to the cloud and inspected by the cloud-based anti-virus engine. After inspection, the sample file will be deleted in real time. CWPP runs a full scan every day by default. No private data will be extracted in this process.

Vulnerability alert

The current CWPP supports detecting Linux and Windows vulnerabilities and security baselines complying with Tencent Cloud requirements.
The vulnerability management feature presents the vulnerability risks on the current server and provides a repair solution to you for reference. This module downloads vulnerability policy library from the cloud to perform detection locally, and reports the name, version number, path, and discovery time of application for a server with vulnerability risk. No data related to user privacy is fetched during the process.

©2013-2022 Tencent Cloud. All rights reserved.

Upgrade and maintenance

The upgrade and maintenance feature mainly informs you of agent upgrades, so that you can obtain the latest security protection services in time. The agent needs to collect the CWPP version number, OS configuration information, security rule version number to the cloud for further judgment and prompt. No private data will be extracted in this process.

©2013-2022 Tencent Cloud. All rights reserved.

Agent Process Description

Last updated：2023-12-26 16:39:23

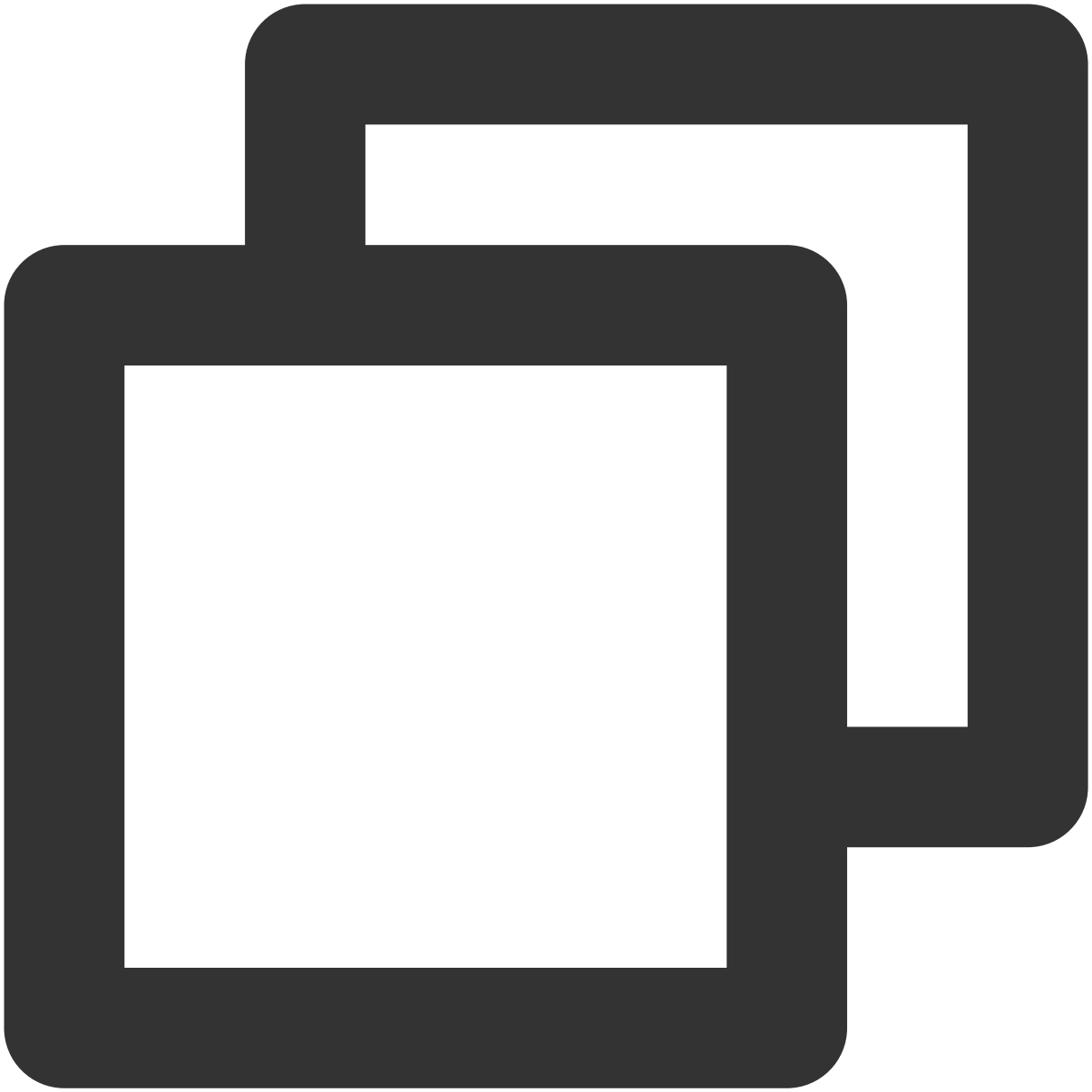
Item	Windows System	Linux System
Program installation directory	C:\\program files\\qcloud\\yunjing\\ydeyes C:\\program files\\qcloud\\yunjing\\ydlive	/usr/local/qcloud/YunJing/
Process name	YDService CWPP main service process YDLive daemon YDPython vulnerability & baseline scan plugin YDQuaraV2 Trojan isolation plugin qtflame assets collection plugin	YDService CWPP main service process YDLive daemon YDPython vulnerability & baseline scan plugin YDUtils process scan plugin YDQuaraV2 Trojan isolation plugin qtflame assets collection plugin tcss-agent container baseline scan plugin tcss-scan container image scan plugin
Registered service	YDService YDLive YDEdr	-

The port used by the agent program is randomly returned by the system, and there is no fixed port range. If the used port conflicts with the port for business, restart the agent program.

Agent restart commands (Linux)

1.1 Stop the agent program:

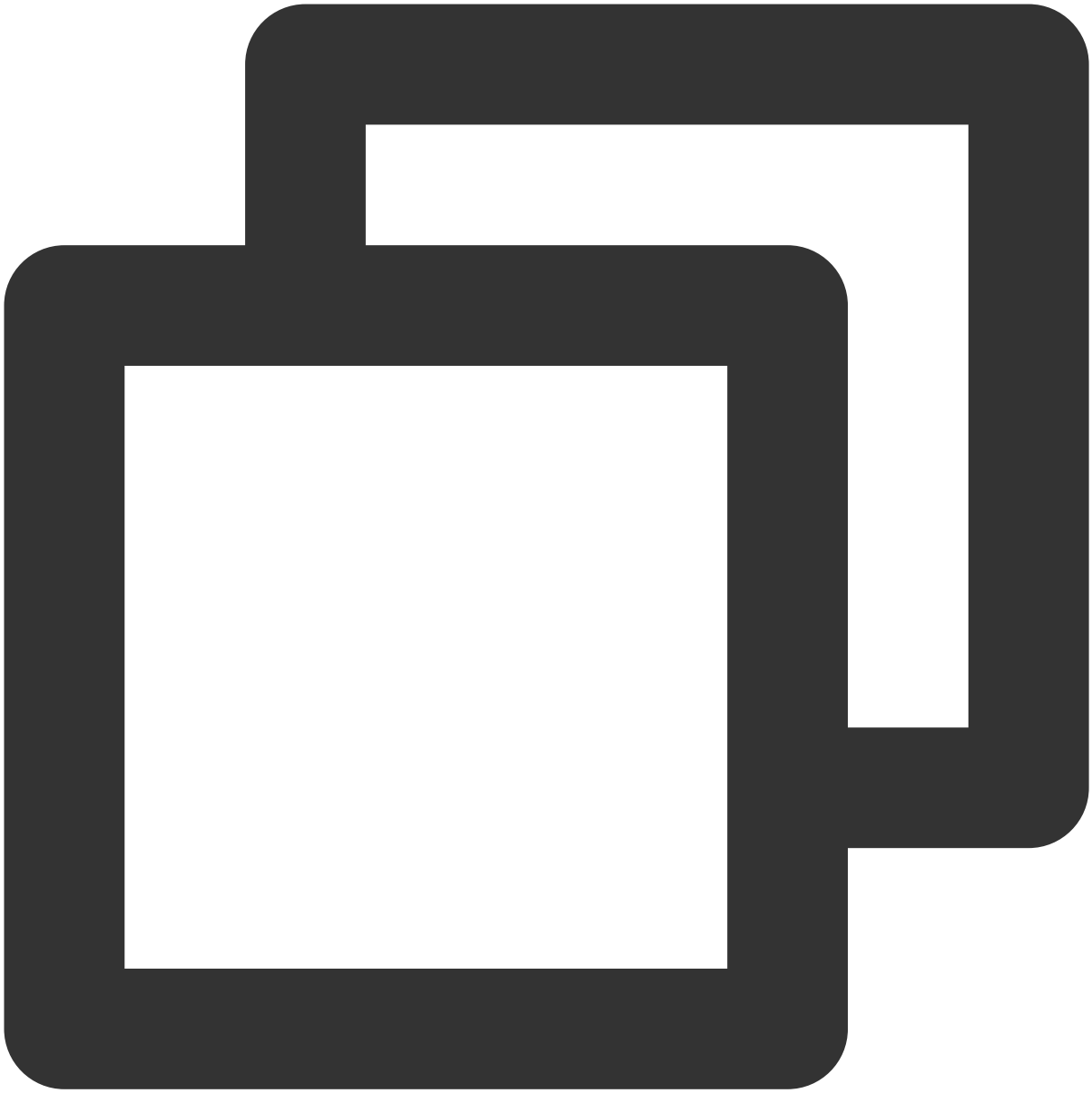
©2013-2022 Tencent Cloud. All rights reserved.



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

1.2 Restart the agent:

©2013-2022 Tencent Cloud. All rights reserved.



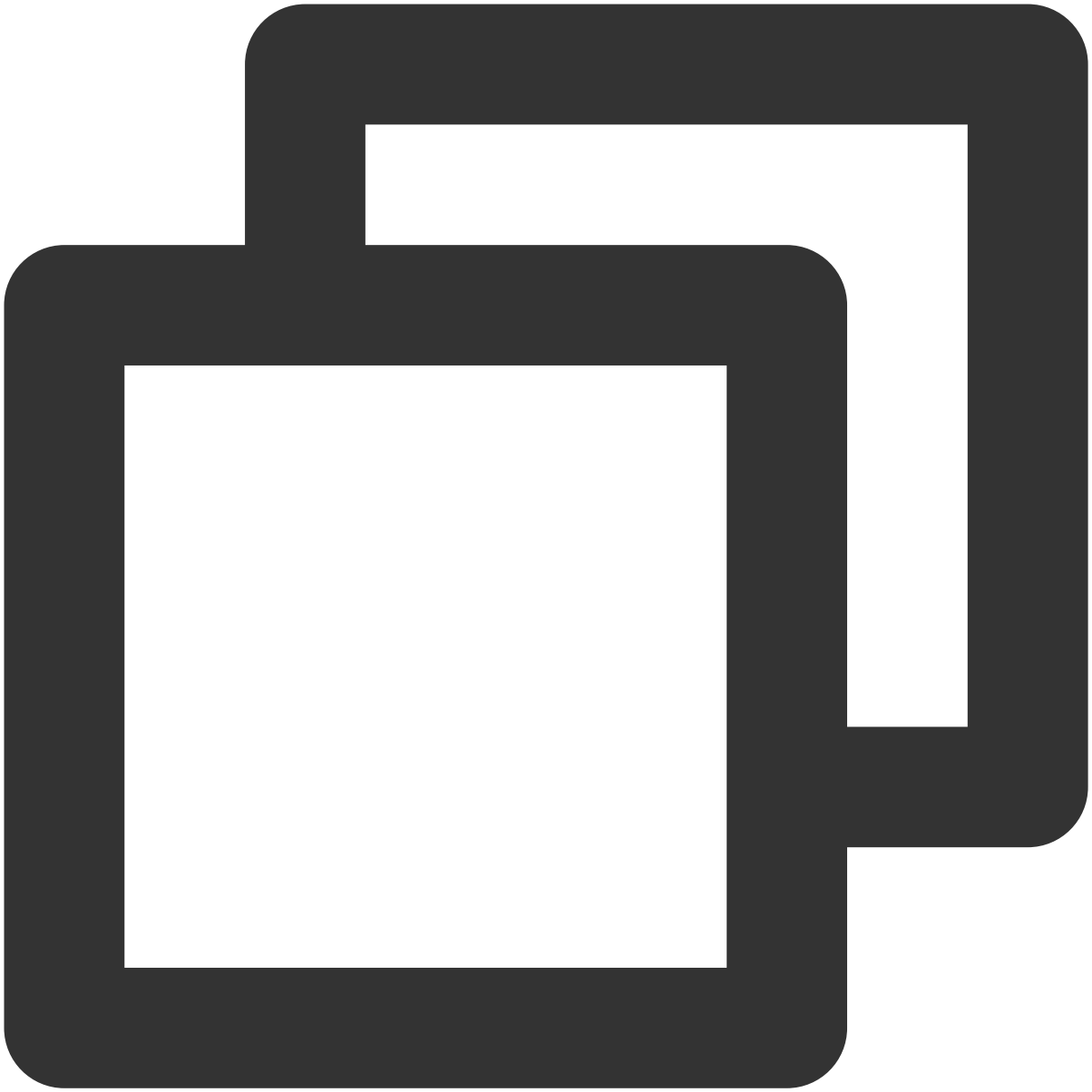
```
/usr/local/qcloud/YunJing/startYD.sh
```

Agent restart commands (Windows)

Enter the following commands or open Task Manager, locate YDService, and right-click to restart the agent.

1.1 Stop the agent program:

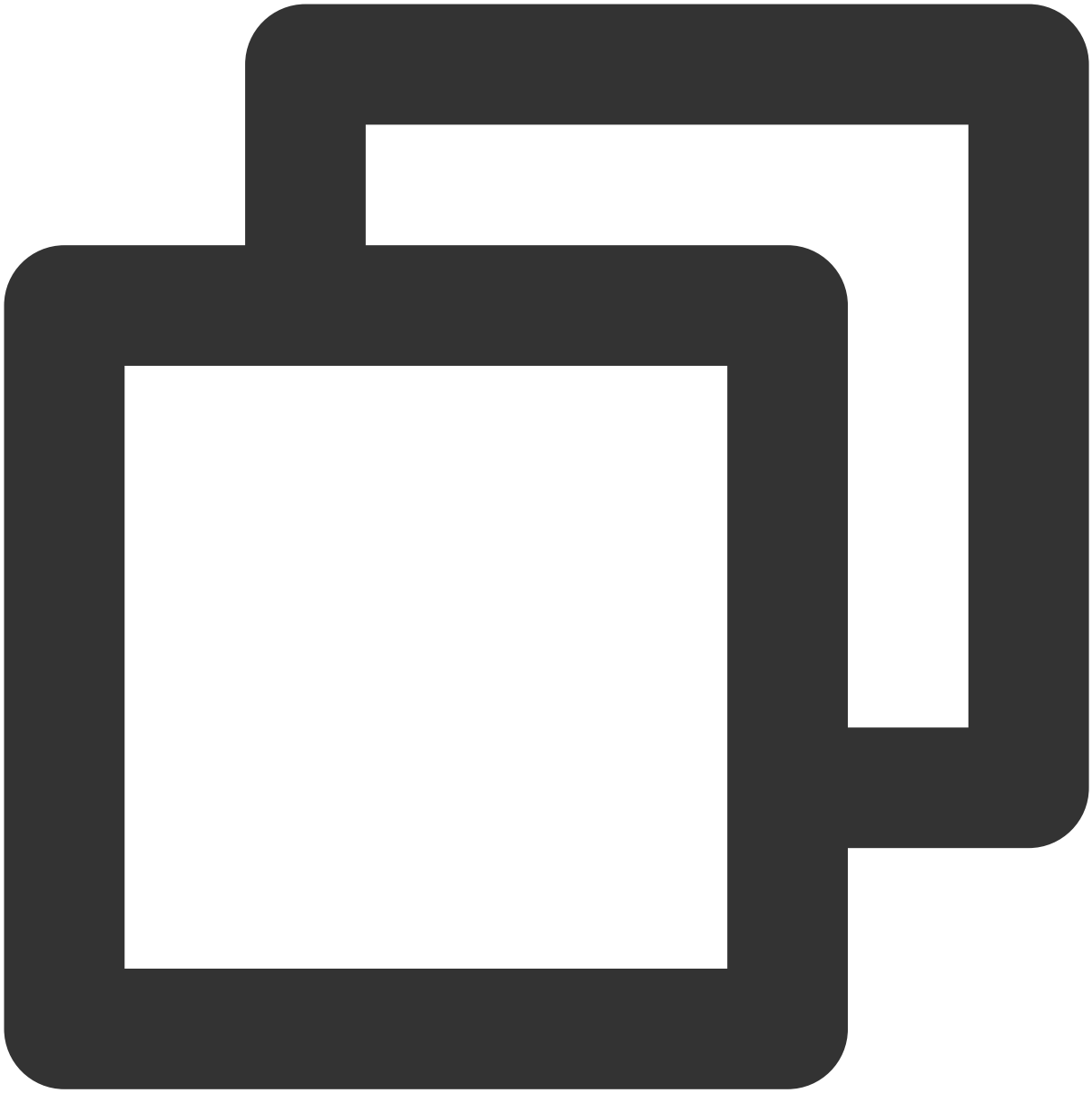
©2013-2022 Tencent Cloud. All rights reserved.



```
net stop YDService
```

1.2 Restart the agent:

©2013-2022 Tencent Cloud. All rights reserved.



```
net  start YDService
```

©2013-2022 Tencent Cloud. All rights reserved.

Agent Installation Guide

Last updated：2023-12-26 16:39:31

This topic describes how to install CWPP Agent.

Limitations

CWPP Agent can only be installed and used on the servers that meet the following two conditions.

Conditions	Description
Server type	CWPP supports servers running in a hybrid cloud. Tencent Cloud: CVM, Lighthouse, and ECM Non-Tencent Cloud servers: third-party cloud vendor servers and IDC servers
Server OS	Linux CentOS: 6, 7, 8 (64-bit) Ubuntu: 9.10 - 20.10 (64 bit) Debian: 6, 7, 8, 9, 10, 11 (64 bit) RHEL: 6, 7 (64 bit) Windows Windows server 2012, 2016, 2019 Windows server 2008 R2 Windows server 2003 (limited support)

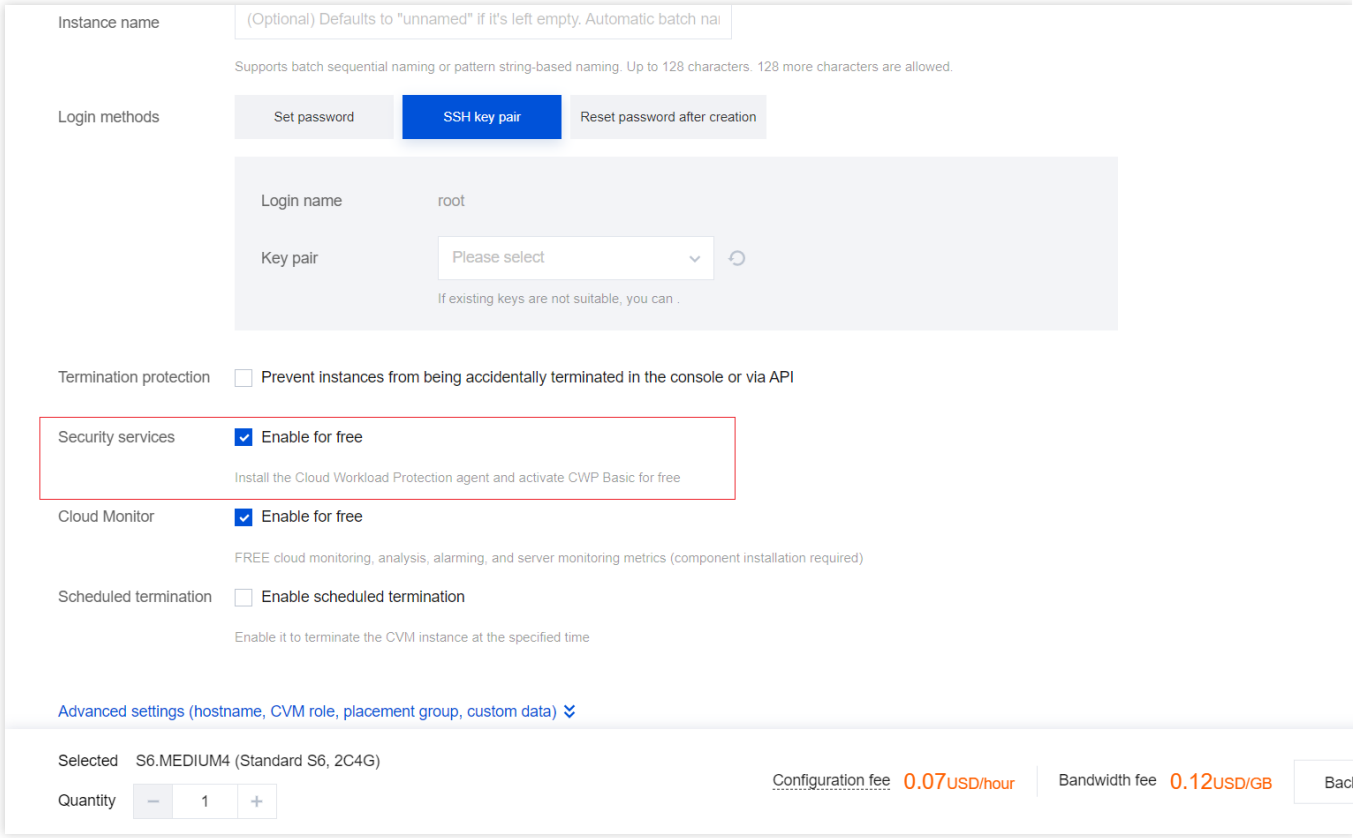
Installation

Option 1: Install directly upon purchase

Applicable to: CVM, Lighthouse, and ECM

When purchasing the above servers, select **Security Reinforcement** to automatically install the CWPP Agent.

©2013-2022 Tencent Cloud. All rights reserved.

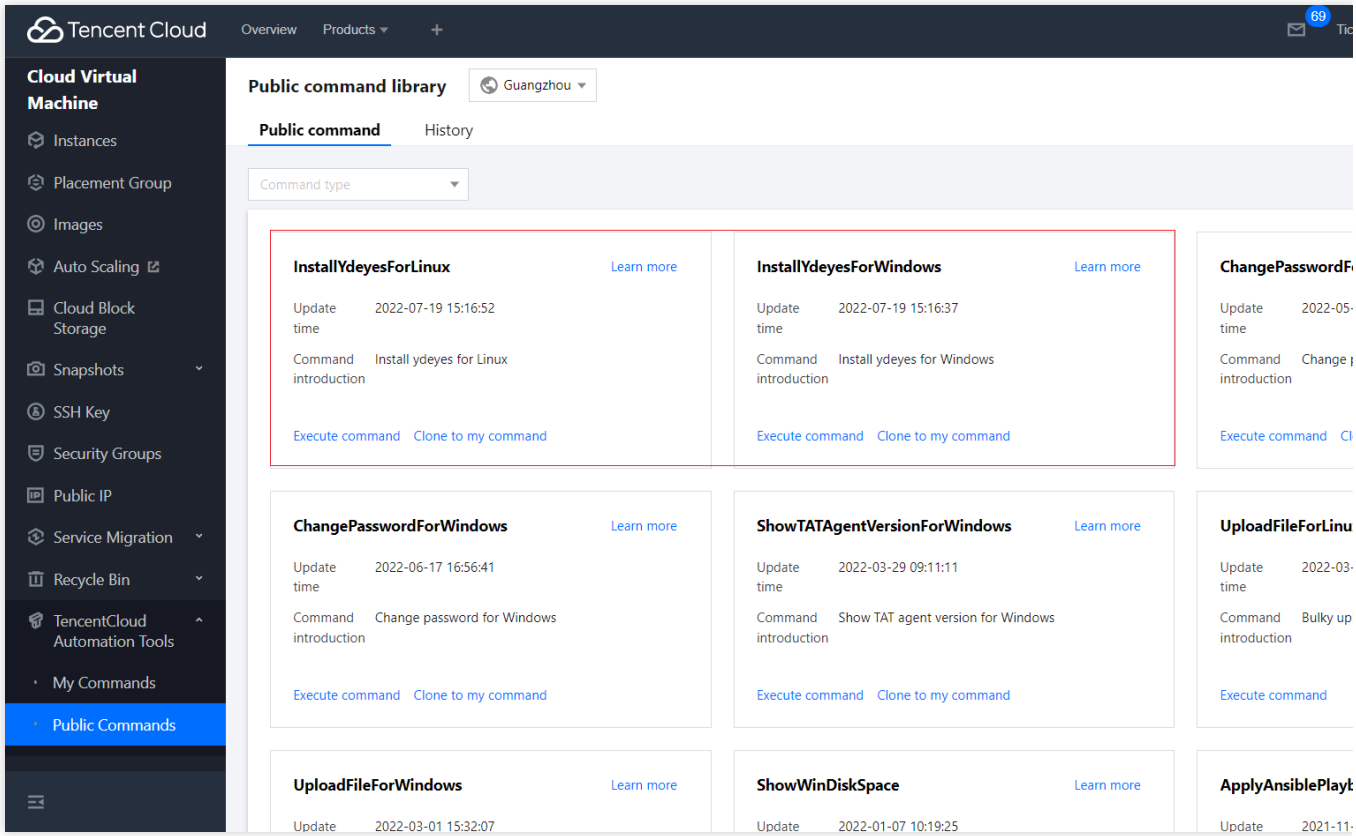


Option 2: Install automatically using Tencent Cloud Automation Tools (TAT)

Applicable to: CVM and Lighthouse

Go to **TAT**>**Public Command Library** of your CVM or Lighthouse server, locate the installation command of the CWPP Agent, click **Execute Command**, and select the server to install the agent.

©2013-2022 Tencent Cloud. All rights reserved.



Option 3: Install by following the installation guide

1. Log in to the CWPP Console.
2. Click **Server List** in the left navigation pane, click **Install CWPP Agent** to open the installation guide pop-up window, and select an installation method based on your server.

©2013-2022 Tencent Cloud. All rights reserved.

Install Cloud Workload Protection agent

Select a proper installation method

Server type	Tencent Cloud	Non-Tencent Cloud
Server System	Linux	Windows
Server Products	CVMs	
Server architecture	x86	arm
Network	VPC	Classic network

Copy and execute the command

```
wget http://uo.yd.tencentyun.com/ydeyes_linux64.tar.gz -O ydeyes_linux64.tar.gz && tar -zxvf ydeyes_linux6
```

Determines whether the installation is successful

Execute the command ps -ef | grep YD to view whether YDService and YDLive are running. If yes, the installa

```
[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/Y
root     32724     1  0 11:23 ?        00:00:01 /usr/local/qcloud/YunJing/YDLive/Y
[root@VM_90_131_centos conf]# ps -ef|grep YD
```

Note: If the process does not start, you can execute the command manually as a root user to start the prograr
/usr/local/qcloud/YunJing/YDEyes/YDService

©2013-2022 Tencent Cloud. All rights reserved.

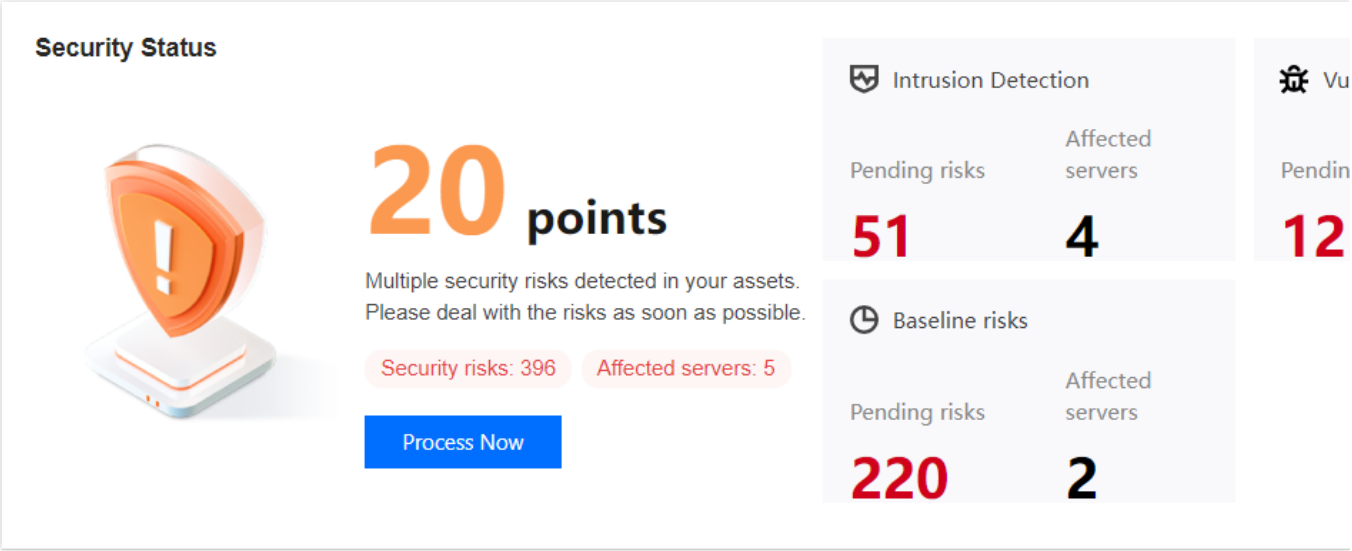
Security Score Overview

Last updated：2023-12-26 16:39:39

This topic describes how to calculate the security score for your assets.

Security Score

The highest security score is 100, and the lowest score is 20. The security level of a server is based on its security score, which is calculated by subtracting the points scored by the types, number, and threat level of security incidents from the total score of 100.



Scoring rules

Level	Security Incidents (by incident count)	Penalty per incident	Maximum total penalty
Critical	Trojan files, brute force attacks, and malicious requests	-40	-50
High	Critical vulnerabilities, high-risk vulnerabilities, critical baseline items, high-risk baseline items, unusual logins (high risk), local privilege escalation, and reverse shell	-10	-20
Medium	Medium-risk vulnerabilities and baseline items	-3	-10
Low	Low-risk vulnerabilities and baseline items	-2	-5

©2013-2022 Tencent Cloud. All rights reserved.

Other	Only CWPP Basic is implemented, or CWPP Agent is not installed	-1	-5

Security level

Level	Health check score	Text color	Description
Good	90-100	Green	The assets have a good security status. Regular inspection is recommended to maintain the good status.
Medium	60-89	Orange	Many security risks exist in the assets. It is recommended to handle the security incidents in a timely manner.
Bad	20-59	Red	Critical security risks exist in the assets. It is recommended to handle the security incidents as soon as possible.

©2013-2022 Tencent Cloud. All rights reserved.