主机安全

软件相关说明

产品文档

腾讯云

文档目录

软件相关说明
功能行为描述

最近更新时间：2023-12-26 15:26:49

Webshell 检测

Webshell 是黑客入侵过程中常用工具，主机安全客户端会对服务器上新创建的 Web 程序文件进行可疑风险判断，对于少量疑似 Webshell 文件，需要上报到云端，通过云端的机器学习检测引擎模块做进一步检测，检测完成后会实时删除该样本文件。主机安全默认提供每天全盘扫描服务，检测过程不会提取任何涉及用户隐私的数据。

登录异常提醒

登录异常提醒功能可以帮助用户识别异常的管理员登录行为，需要采集登录日志中的来源 IP、时间、登录用户名、登录状态数据到云端进行风险计算，登录日志数据需在云端保存一个月。

密码破解提醒

密码破解提醒功能可以告诉用户当前遭受的密码破解事件和破解结果，需要采集登录日志中的来源 IP、时间、登录用户名、登录状态数据到云端进行风险计算，登录日志数据需在云端保存一个月。

恶意木马和病毒检测

恶意木马和病毒程序通常会窃取用户数据或者对外攻击，消耗大量系统资源导致业务不能正常提供服务。客户端会采集可疑恶意程序的 哈希指纹 到云端，通过云查杀模块对哈希指纹进行检测，若云端哈希库无该文件记录，需要上报可执行文件到云端，通过云端杀毒引擎进行检测，检测完后会实时删除该样本文件。主机安全默认提供每天全盘扫描服务，检测过程中不会提取任何涉及用户隐私的数据。

漏洞提醒

目前主机安全支持检测影响面较大的 Linux 和 Windows 双平台的漏洞，以及符合腾讯云安全要求的基线检测。
漏洞管理功能会显示当前主机上的漏洞风险情况，同时提供修复方案供用户参考。该模块执行时会从云端下载漏洞策略库在本地执行检测，对于存在漏洞风险的主机，会上报应用软件的名称、版本号、路径、发现时间。主机安全默认提供每天漏洞扫描服务，这个过程不会提取任何涉及用户隐私的数据。

升级维护

升级维护功能主要提醒用户对客户端进行升级，以获得最新的安全防护服务，客户端软件需要采集主机安全版本号、操作系统配置信息、安全规则版本号到云端进行判断和提醒，该过程不会提取任何涉及用户隐私的数据。

客户端进程说明

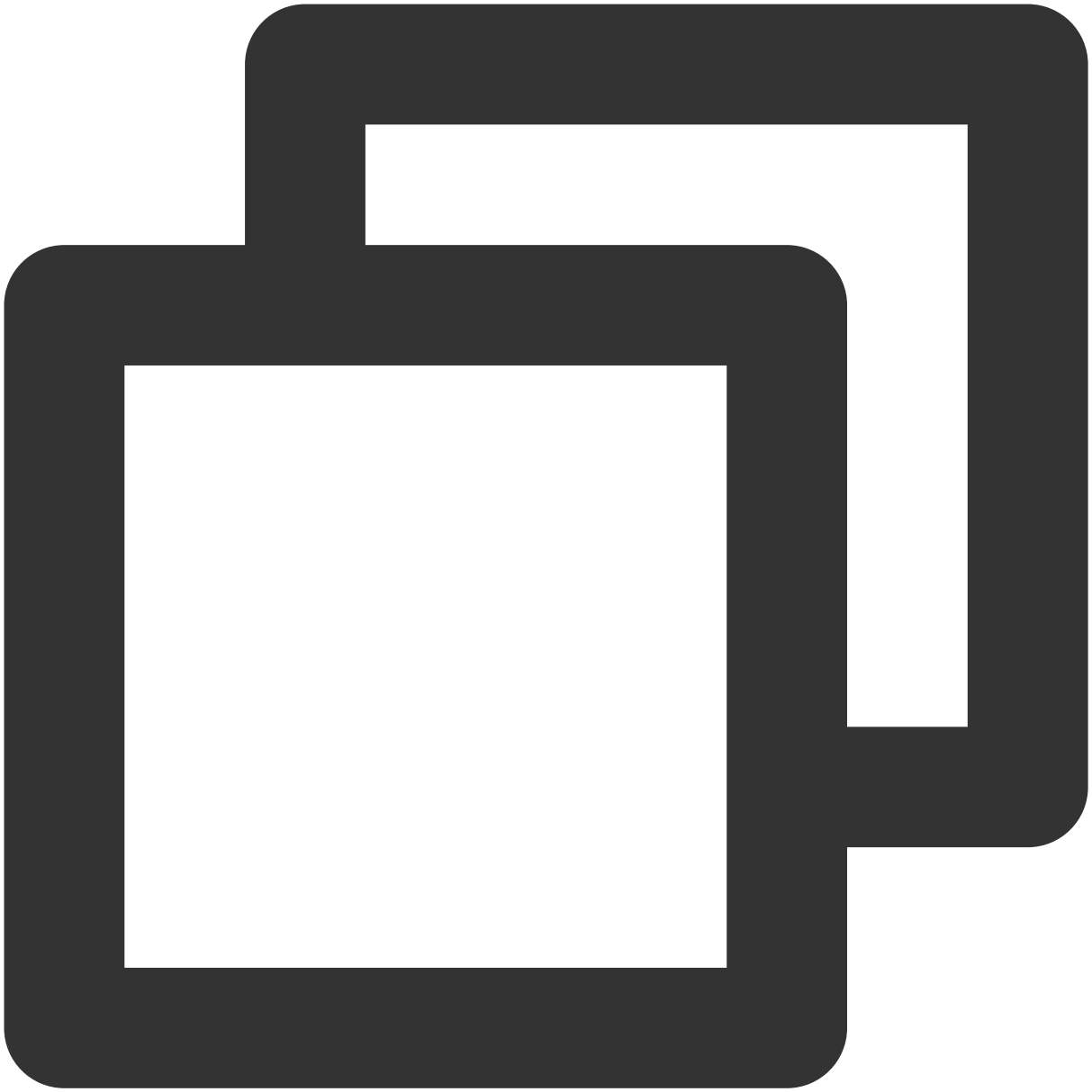
最近更新时间：2023-12-26 15:26:58

名称	Windows 系统	Linux 系统
程序安装目录	C:\\program files\\qcloud\\yunjing\\ydeyes C:\\program files\\qcloud\\yunjing\\ydlive	/usr/local/qcloud/YunJing/
进程名称	YDService 云镜主服务进程 YDLive 守护进程 YDPython 漏洞&基线扫描插件 YDQuaraV2 木马隔离插件 qtflame 资产采集插件	YDService 云镜主服务进程 YDLive 守护进程 YDPython 漏洞&基线扫描插件 YDUtils 进程扫描插件 YDQuaraV2 木马隔离插件 qtflame 资产采集插件 tcss-agent 容器基线扫描插件 tcss-scan 容器镜像扫描插件
注册服务名称	YDService YDLive YDEdr	-

客户端程序所占用端口是系统随机返回的，无固定端口范围，若占用端口与用户业务端口冲突，重启客户端程序即可。

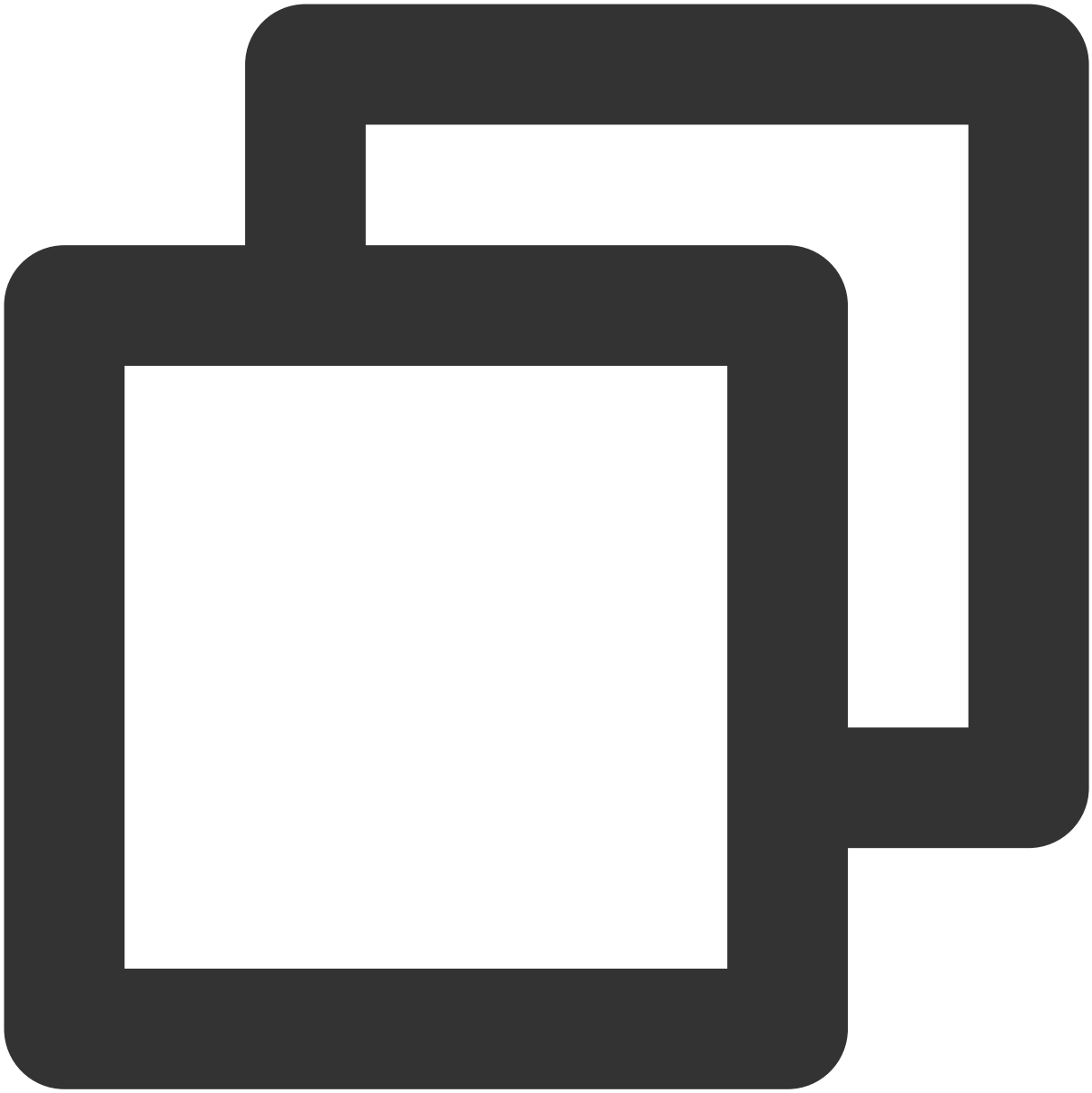
客户端重启命令（Linux系统）

1.1 暂停客户端程序服务



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

1.2 重新启动客户端

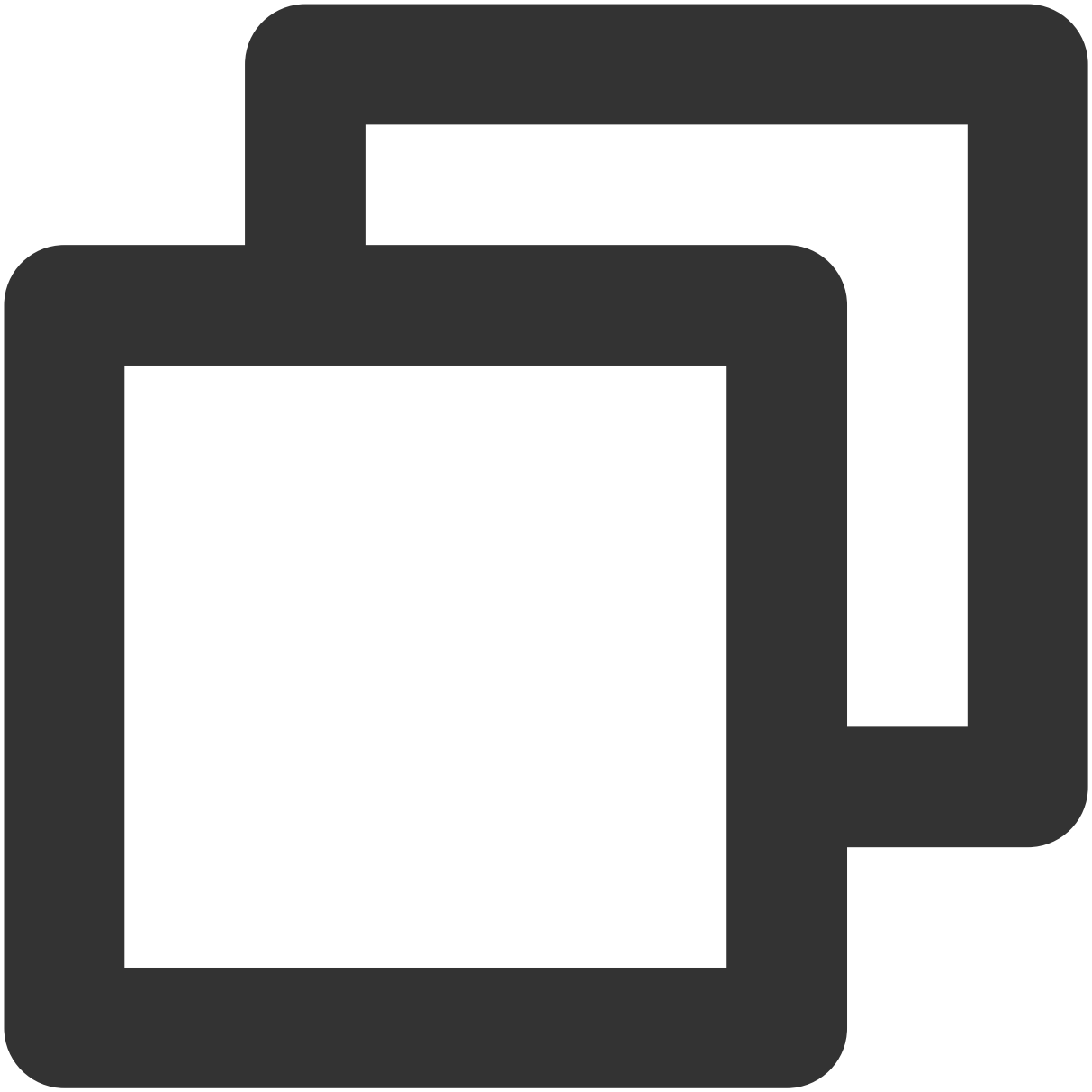


```
/usr/local/qcloud/YunJing/startYD.sh
```

客户端重启命令（Windows系统）

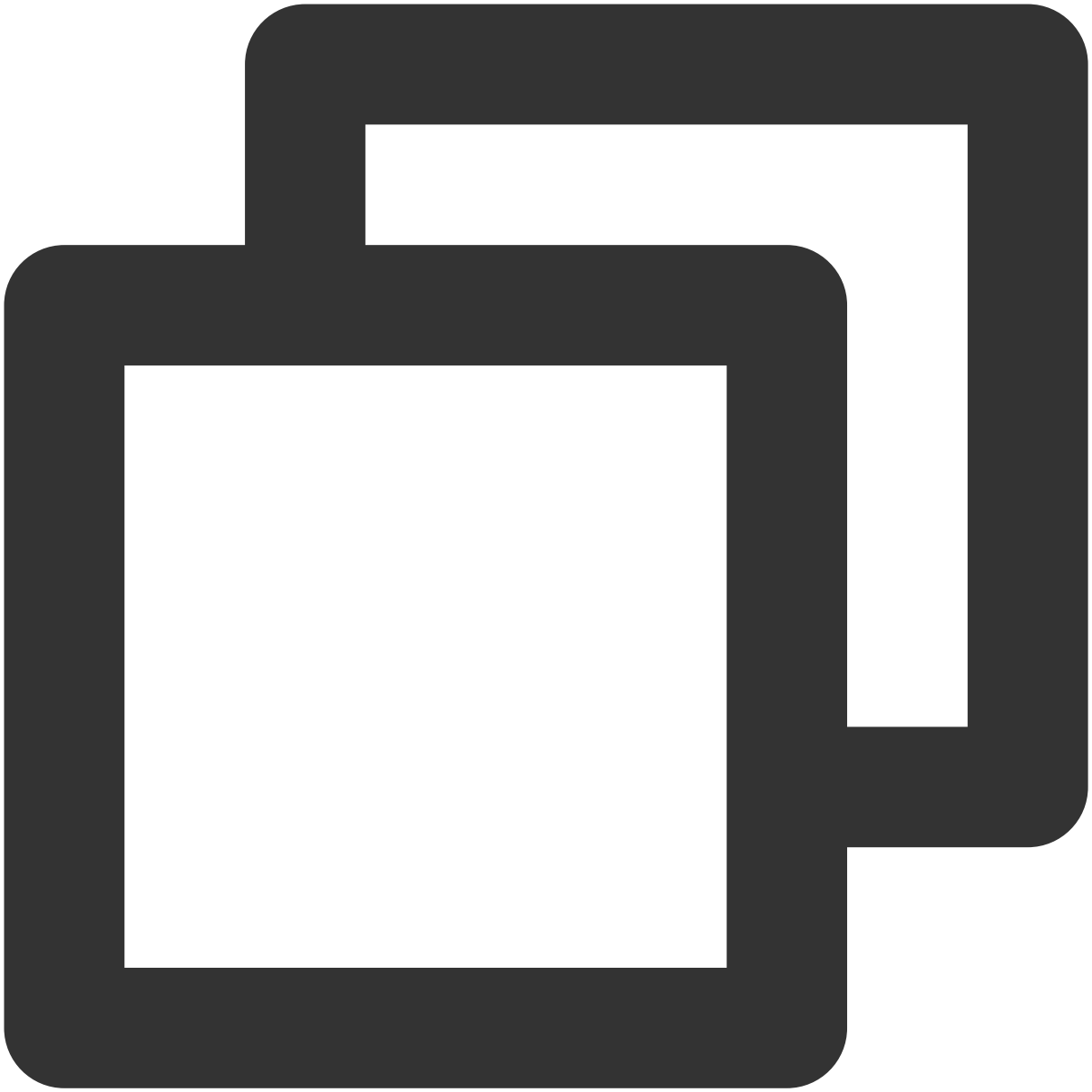
输入以下命令，或打开任务管理器的服务，找到 YDService 服务，右键重启。

1.1 暂停客户端程序服务



```
net stop YDService
```

1.2 重新启动客户端



```
net  start YDService
```

客户端安装指引

最近更新时间：2023-12-26 15:27:07

本文将为您介绍如何安装主机安全客户端。

限制说明

服务器须满足以下两个条件，才可正常安装和使用主机安全客户端。

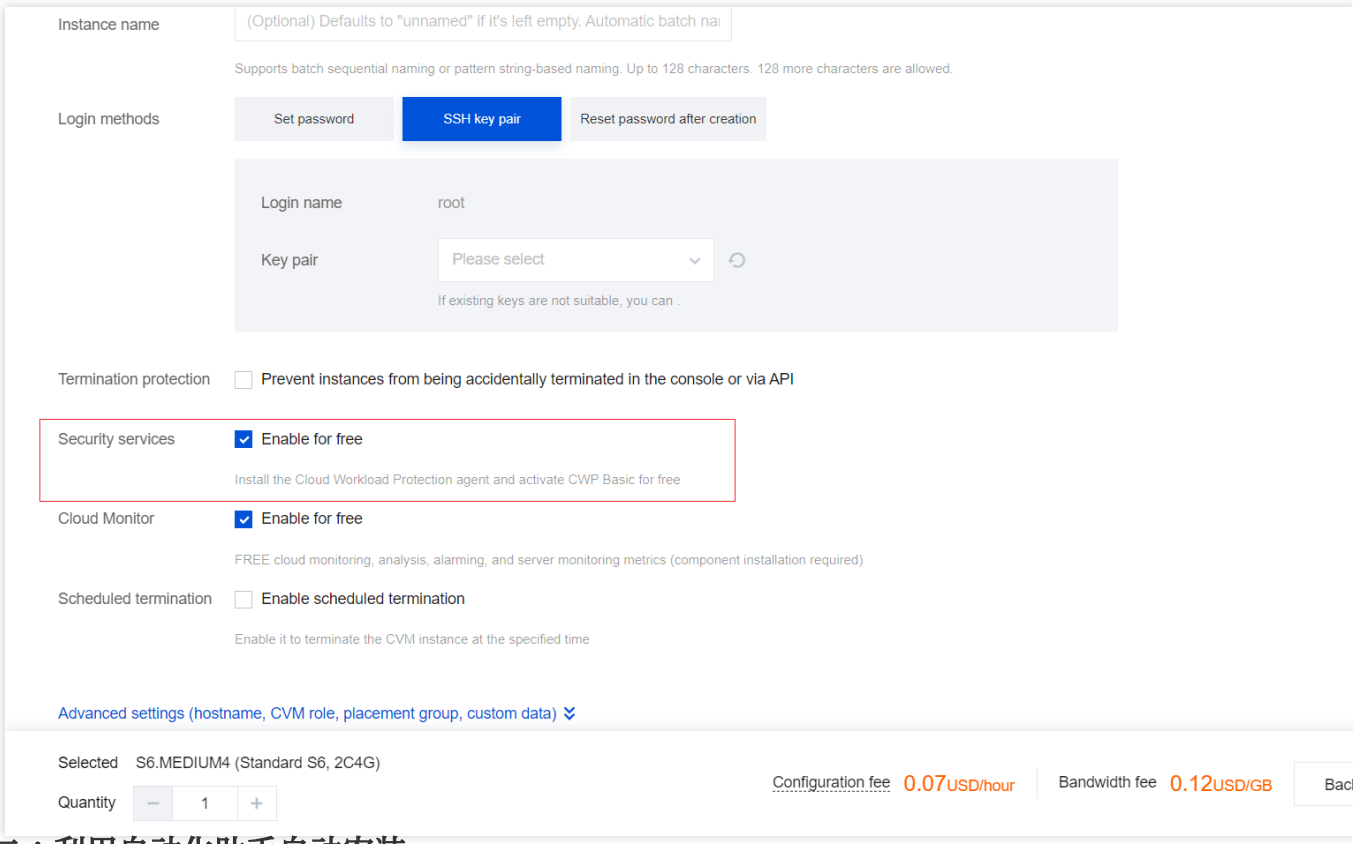
条件	说明
服务器类型	主机安全已支持混合云主机接入。 腾讯云：云服务器（CVM）、轻量应用服务器（Lighthouse）、边缘计算机器（ECM） 非腾讯云：第三方云厂商服务器、IDC服务器
服务器系统	Linux系统 CentOS: 6, 7, 8(64 bit) Ubuntu: 9.10 - 20.10(64 bit) Debian: 6, 7, 8, 9, 10, 11(64 bit) RHEL: 6, 7(64 bit) Windows系统 Windows server 2012, 2016, 2019 Windows server 2008 R2 Windows server 2003 (limited support)

安装方式

方式一：购买服务器时直接安装

适用于：云服务器（CVM）、轻量应用服务器（Lighthouse）、边缘计算机器（ECM）

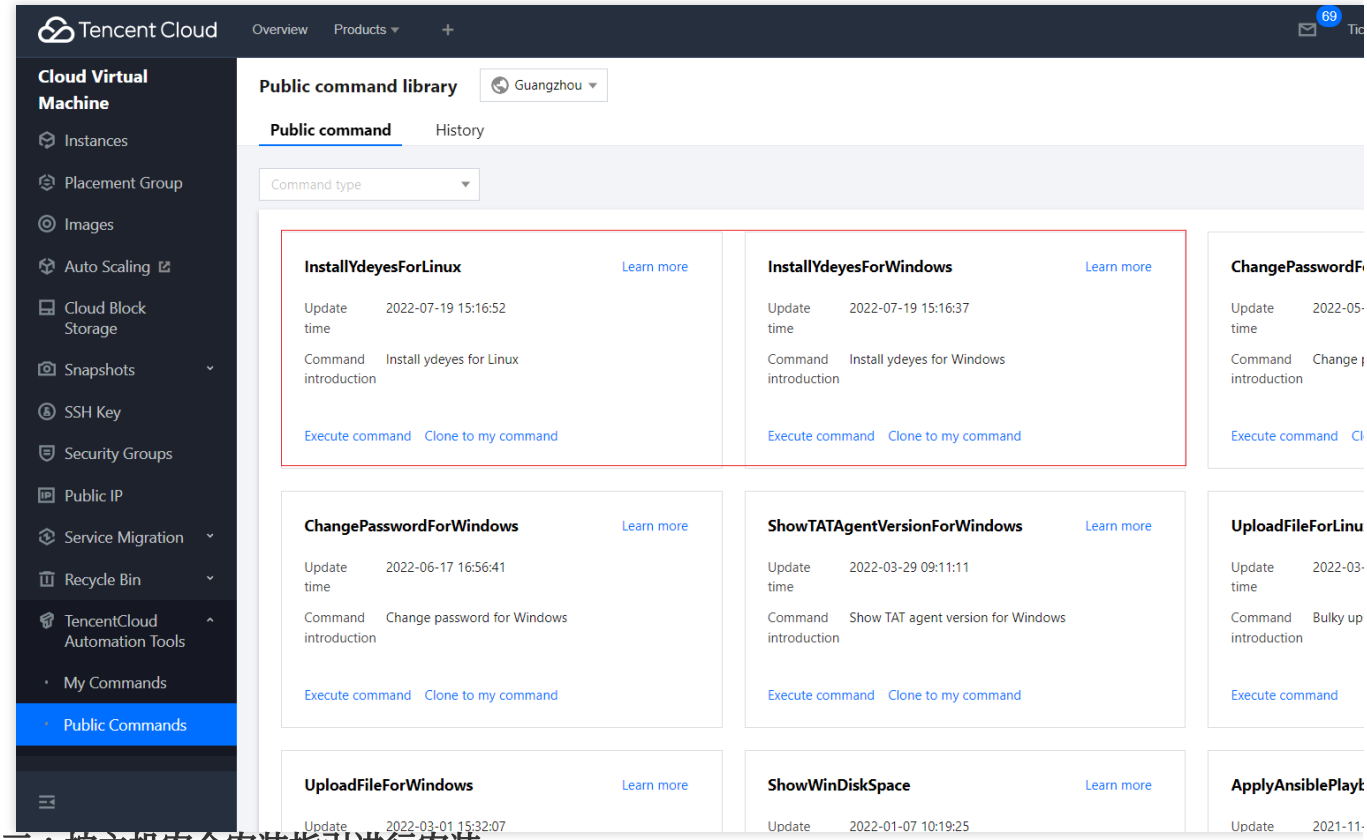
在选购上述服务器时，勾选**安全加固**项即自动安装主机安全客户端。



方式二：利用自动化助手自动安装

适用于：云服务器（CVM）、轻量应用服务器（Lighthouse）

在云服务器或轻量应用服务器的**自动化助手>公共命令库**中，找到主机安全客户端的安装命令，点击**执行命令**，选择服务器进行安装即可。



方式三：按主机安全安装指引进行安装

1. 登录主机安全控制台。
2. 单击左侧导航中的**主机列表**，点击**安装主机安全客户端**按钮，打开安装指引弹窗，根据服务器不同特性，选择合适的安装方式进行安装。

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

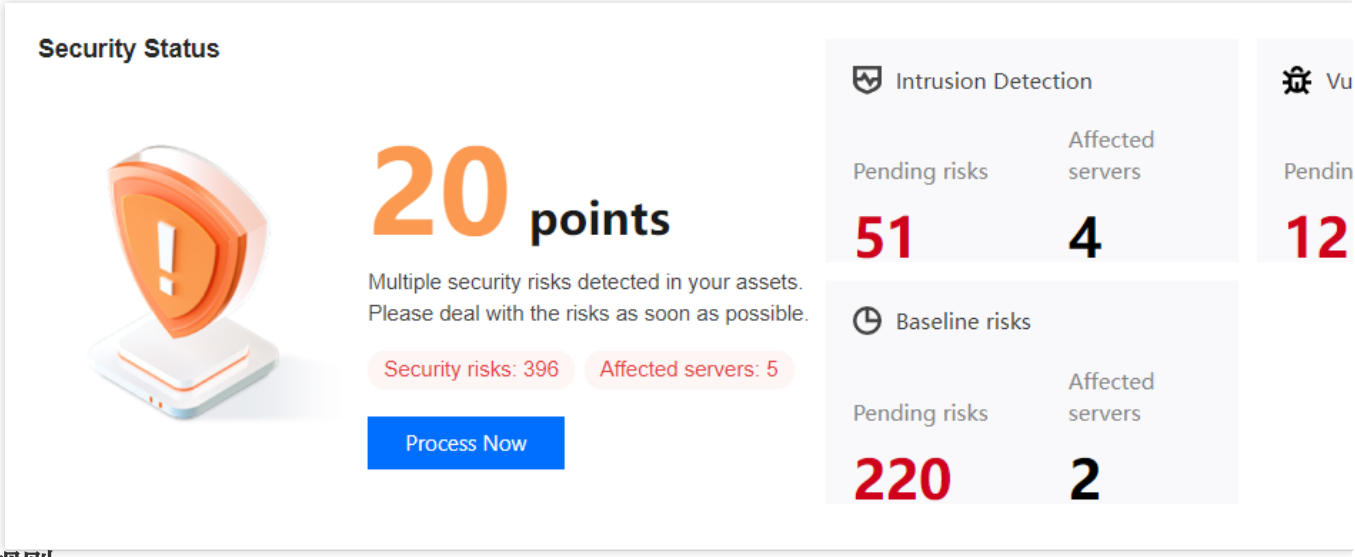
安全评分说明

最近更新时间：2023-12-26 15:27:17

本文将为您介绍安全评分细则。

安全评分

安全评分满分100，底分20。依据安全事件类型、安全事件数量、事件威胁等级进行扣分，以最终分数来划分安全等级。



扣分规则

等级	安全事件（按事件数计算）	扣分/个	叠加最大扣分
严重	木马文件、暴破成功、恶意请求	-40分	-50分
高危	严重漏洞、高危漏洞、严重基线、高危基线、异常登录（高危）、本地提权、反弹Shell	-10分	-20分
中危	中危漏洞、中危基线	-3分	-10分
低危	低危漏洞、低危基线	-2分	-5分
其他	基础版防护、未安装主机安全客户端	-1分	-5分

安全等级

等级	体检评分	字体颜色	状态说明
优	90分 - 100分	绿色	资产安全状态较好，需继续保持，定期巡检。
中危	60分 - 89分	橙色	资产存在较多安全风险，建议您及时处理安全事件。
高危	20分 - 59分	红色	资产存在严重安全风险，请您尽快处理安全事件。