

# 主机安全 快速入门 产品文档



腾讯云

**【版权声明】**

©2013-2020 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

**【商标声明】**

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

**【服务声明】**

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

**【联系我们】**

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

# 快速入门

最近更新时间：2020-09-10 15:01:31

## 入门准备

主机安全可在腾讯云服务器（黑石物理服务器 CPM）安装时一同安装，或单独进行安装。

登录 [主机安全控制台](#)，在左侧导航栏中，选择【资产管理】>【主机列表】，查看云服务器是否已安装主机安全，如下图所示：



| 服务器                                     | 操作系统                    | 防护状态              | 漏洞数量 | 防护级别                | 操作          |
|---|-------------------------|-------------------|------|---------------------|-------------|
| 10.1.1.1<br>ccs_ubuntu16.04.1 LTSx86_64 | ubuntu16.04.1 LTSx86_64 | 防护中               | 0    | 专业防护 <span>✔</span> | 卸载 关闭专业防护   |
| 10.1.1.2<br>ccs_ubuntu16.04.1 LTSx86_64 | ubuntu16.04.1 LTSx86_64 | 防护中               | 0    | 基础防护                | 卸载 开通专业防护   |
| 10.1.1.3<br>ccs_centos7.3x86_64         | centos7.3x86_64         | 离线 <span>ⓘ</span> | 0    | 基础防护                | 重新安装 开通专业防护 |

- 红色框中的服务器安装了主机安全的专业防护版本，享有主机安全带来的全面多维度的系统安全保障。
- 蓝色框中的服务器安装了主机安全的基础防护版本，可在右侧单击【开通专业防护】，升级为专业防护版本。
- 黄色框中的服务器没有安装主机安全产品。可根据如下指引及进行安装：
  - [Windows 云服务器环境](#)
  - [Linux 云服务器环境](#)

## 主机安全安装

### Windows 云服务器环境

#### 适配版本

目前支持的版本：

- Windows server 2012
- Windows server 2008 R2
- Windows server 2003 (limited support)
- Windows server 2016

#### 系统配置

### 硬盘 IO :

- IO : < 500KB/s , 瞬时达到 1 MB 为正常情况。
- IOPS : < 30次/s , 一般为个位数。

### 详细的性能指标 :

| 机器类型 | 安全事件   | CPU  | 内存占用  |
|------|--|--|---|
| 小型机器 | 安全事件生成速率较慢 : 每秒 < 50 个安全事件。                  | 维持在2%以内, 可能偶有瞬时抖动到10%, 极少到35%, 连续一小段时间超过35%, 就会自动重启客户端。  | <ul style="list-style-type: none"> <li>• 系统1G内存, 客户端占用 10MB - 30MB。</li> <li>• 系统1G - 2G内存, 客户端占用10MB - 40MB。</li> <li>• 系统2G - 4G内存, 客户端占用10MB - 60MB。</li> </ul>  |
| 小型机器 | 安全事件生成速率极快 : 每秒 50个 - 200个安全事件, 数量极大, 且持续如此。 | 维持在5%以内, 可能偶有瞬时抖动到20%, 极少到35%, 连续一小段时间超过35%, 就会自动重启客户端。  | <ul style="list-style-type: none"> <li>• 系统1G内存, 客户端占用 10MB - 40MB。</li> <li>• 系统1G - 2G内存, 客户端占用10MB - 60MB。</li> <li>• 系统2G - 4G内存, 客户端占用10MB - 120MB。</li> </ul> |
| 大型机器 | 如果安全事件量极少, 资源消耗标准等同于小型机 ( 4G内存 )。            | 维持在10%以内, 可能偶有瞬时抖动到20%, 极少到35%, 连续一小段时间超过35%, 就会自动重启客户端。 | 客户端占用60MB - 360MB   |

### 下载地址

- 外网下载地址 :

[https://imgcache.qq.com/qcloud/csec/yunjing/static/ydeyes\\_win32.exe](https://imgcache.qq.com/qcloud/csec/yunjing/static/ydeyes_win32.exe)

- 基础网络下载地址 ( 非 VPC 服务器 ) :

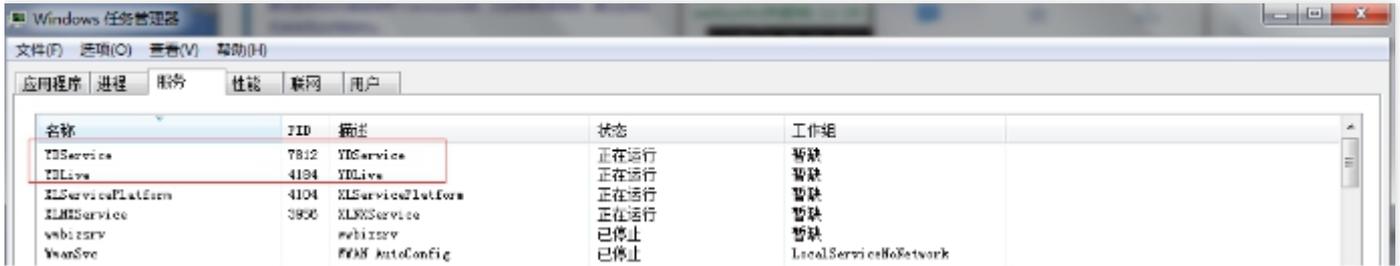
[http://u.yd.qcloud.com/ydeyes\\_win32.exe](http://u.yd.qcloud.com/ydeyes_win32.exe)

- VPC & 黑石服务器下载 :

[http://u.yd.tencentyun.com/ydeyes\\_win32.exe](http://u.yd.tencentyun.com/ydeyes_win32.exe)

### 安装说明

Windows 安装成功状态验证：打开任务管理器，查看 YDService，YDLive 进程是否有调用，有调用则安装成功。



## 常见问题

- 防火墙拦截

建议防火墙策略放通主机安全后台服务器访问地址：

域名：`s.yd.qqcloud.com`; `l.yd.qqcloud.com`; `u.yd.qqcloud.com`

端口：`5574`、`8080`、`80`、`9080`

- DNS 说明

若您不需要使用默认 DNS，则需要将 `tencentyun.com` 和 `yd.qqcloud.com` 根域的所有解析转发至默认 DNS。

## Linux 云服务器环境

### 适配版本

目前支持的版本：

- RHEL : Versions 6 and 7 ( 64 bit )
- CentOS : Versions 6 and 7 ( 64 bit )
- Ubuntu : 9.10 - 18.04 ( 64 bit )
- Debian : 6, 7, 8, 9 ( 64 bit )

### 下载地址

- 外网下载地址：

```
wget --no-check-certificate https://imgcache.qq.com/qcloud/csec/yunjing/static/yunjinginstall.sh && sh ./yunjinginstall.sh
```

- 基础网络下载地址（非 VPC 服务器）：

```
wget http://u.yd.qqcloud.com/ydeyesinst_linux64.tar.gz && tar -zxvf ydeyesinst_linux64.tar.gz && sh self_cloud_install_linux64.sh
```

- VPC & 黑石服务器下载

```
wget http://u.yd.tencentyun.com/ydeyesinst_linux64.tar.gz && tar -zxvf ydeyesinst_linux64.tar.gz &
& sh self_cloud_install_linux64.sh
```

## 安装说明

执行完安装命令后查看 YDService, YDLive 进程是否有调用, 有调用则安装成功。命令为:

```
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
```

如果进程没有起来, 可以使用 root 用户手动执行命令, 启动程序。命令为:

```
/usr/local/qcloud/YunJing/YDEyes/YDService
```

## 卸载说明

主机安全共有控制台卸载与系统卸载两种方式, 下面将为您详细介绍:

### • 控制台中卸载

- i. 登录 [主机安全](#) 控制台, 查看自己的云服务器是否已安装主机安全。
- ii. 在服务器列表中, 选择需要卸载主机安全的服务器进行卸载。



### • 进入系统卸载

#### i. Windows 系统

依照路径找到 `uninst.exe` 文件, 双击即可卸载。

路径: `C:\Program Files\QCloud\YunJing\uninst.exe`。

#### ii. Linux 系统

输入命令: `/usr/local/qcloud/YunJing/uninst.sh` 即可卸载。

## 常见问题

- 防火墙拦截

建议防火墙策略放通主机安全后台服务器访问地址：

域名：`s.yd.qcloud.com`; `l.yd.qcloud.com`; `u.yd.qcloud.com`

端口：`5574`、`8080`、`80`、`9080`

- DNS 说明

若您需要不使用默认 DNS，则需要将 `tencentyun.com` 和 `yd.qcloud.com` 根域的所有解析转发至默认 DNS。

## 开通专业防护

用户可以通过以下两种渠道进行开通：

- **方式1**：在腾讯云官网，[主机安全产品介绍页面](#) 中单击【立即选购】，随即跳转腾讯云控制台登录界面，登录后可以为需要的云服务器开通专业防护。
- **方式2**：登录 [主机安全控制台](#)，在左侧导航栏中，单击【安全概览】，进入安全概览页面，在上方公告栏中，单击【升级专业版】，即可为需要的云服务器开通专业防护。

## 入侵检测

安装主机安全后，可以享有主机安全带来的木马文件查杀、登录行为审计、密码破解检测等功能，这些功能随主机安全安装后自动启用，现有两种方式查看服务器入侵检测详情：

- **方式1**：登录 [主机安全控制台](#)，在左侧导航栏中，选择【资产管理】>【主机列表】，服务器列表中找到需要查看的服务器，单击服务器 IP 地址，然后单击【入侵检测】即可查看该服务器入侵检测详情。
- **方式2**：登录 [主机安全控制台](#)，在左侧导航栏中，单击【入侵检测】，然后单击所需查看的功能，即可查阅所有开通主机安全的服务器入侵检测详情。

更多功能操作请参见：

- [木马文件操作处理](#)
- [登录审计操作](#)

## 漏洞检测

安装主机安全并开通专业防护后，可以享有主机安全带来的系统组件漏洞检测、Web 组件漏洞检测、安全基线检测功能。

登录 [主机安全控制台](#)，在左侧导航栏中，单击【漏洞管理】，然后单击所需查看的功能，即可查阅所有开通主机安全专业防护的服务器漏洞检测详情，并可以按照提示进行修复。

## 相关文档

- [安全概览](#)
- [木马文件操作处理](#)
- [登录审计](#)
- [密码破解](#)