

云安全中心 客户端说明



腾讯云

【 版权声明 】

©2013–2026 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或 95716。

文档目录

客户端说明

客户端进程说明

内核级 Hook 能力说明

客户端说明

客户端进程说明

最近更新时间：2026-10-21 14:46:04

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/
组件（类型）	- YDService（主服务进程） - YDLive（守护进程） - YDPython（漏洞/基线扫描组件） - YDQuaraV2（木马隔离组件） - YDFlame（资产采集组件） - YDGuard（客户端防卸载组件，开启客户端自保护-防卸载后生效）	- YDService（主服务进程） - YDLive（守护进程） - YDPython（漏洞/基线扫描组件） - YDUtills（进程扫描组件） - YDQuaraV2（木马隔离组件） - YDFlame（资产采集组件） - tcss-agent（容器基线扫描组件） - tcss-scan（容器镜像扫描组件）
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
```

内核级 Hook 能力说明

最近更新时间：2026-10-21 14:46:05

云安全中心 Linux 客户端使用 eBPF，在内核中采集主机网络行为。采集在内核态完成，不修改业务进程。本文说明这组采集的前提，以及已经验证可以完整采集的内核版本。

采集内容

客户端通过 eBPF 的 kprobe 与 tracepoint 采集以下五项网络行为。下文内核版本，均指这五项都可以采集。

网络行为	识别目标
发起网络连接	主动外联
TCP 连接状态变化	连接建立与断开
端口绑定	主机监听的端口
UDP 发送（含 DNS 查询）	DNS 访问
Unix 域套接字连接	本机进程之间的连接

已验证内核版本

操作系统	内核版本
CentOS 8	4.18.0-305.3.1.el8.x86_64 4.18.0-348.7.1.el8_5.x86_64
al8 内核	5.10.134-16.3.al8.x86_64
TencentOS Server 3.1 (TK4)	5.4.119-19.0009.65 5.4.119-19.0009.67.3
TencentOS Server 4	6.6.92-34.1.oc9.x86_64 6.6.92-34.1.tl4.x86_64 6.6.119-47.8.oc9.x86_64
OpenCloudOS Server 9	6.6.34-9.oc9.x86_64 6.6.47-12.oc9.x86_64 6.6.117-45.1.oc9.x86_64 6.6.119-49.23.oc9.x86_64

Ubuntu	• 6.8.12-060812-generic • 6.14.11-061411-generic
--------	--

i 说明：

- 结论只适用于表中的完整内核版本，不能按5.4、6.6 这类主版本号类推到其他构建。
- 只能采集部分网络行为的内核，不列入上表。
- 内核版本补充验证后，以更新后的本文和主机实际结果为准。

采集前提

确认内核有提供 BTF，BTF 是内核自带的类型信息，客户端靠它加载 eBPF 程序（如 CentOS 7 默认的 3.10 内核没有 BTF，可安装客户端，但不会启用上述网络行为采集），确认步骤如下：

1. 在 Linux 主机上执行：

```
ls /sys/kernel/btf/vmlinux
```

2. 若该文件存在，表示内核提供 BTF。

i 说明：

有 BTF 只说明具备加载条件，请按下文核对内核版本是否已验证五项网络行为采集。

核对内核

核对当前主机的内核版本，是否已验证可以完整采集上述五项网络行为，核对步骤如下：

1. 在 Linux 主机上执行：

```
uname -r
```

2. 将输出的完整内核版本与上文 [已验证内核版本](#) 对照，查找完全相同的内核版本。

- **可查到：**说明上述五项网络行为内容均可采集。
- **查不到：**说明该版本仍在验证中，尚未收录至本文，五项网络行为的采集情况，以该主机实际结果为准。