# H3C SecPath D2000-G[AK][V]系列数据库审计系统

## 流量探针安装指导

# 目 录

# 1 流量探针的安装指导

## 1.1 流量探针安装包的获取

打开浏览器，访问数据库审计设备的登录页面，鼠标移至登录页面的右上角，在展开的下拉项中，选择“流量探针客户端”，即可下载流量探针安装包。

图1-1 下载流量探针客户端界面

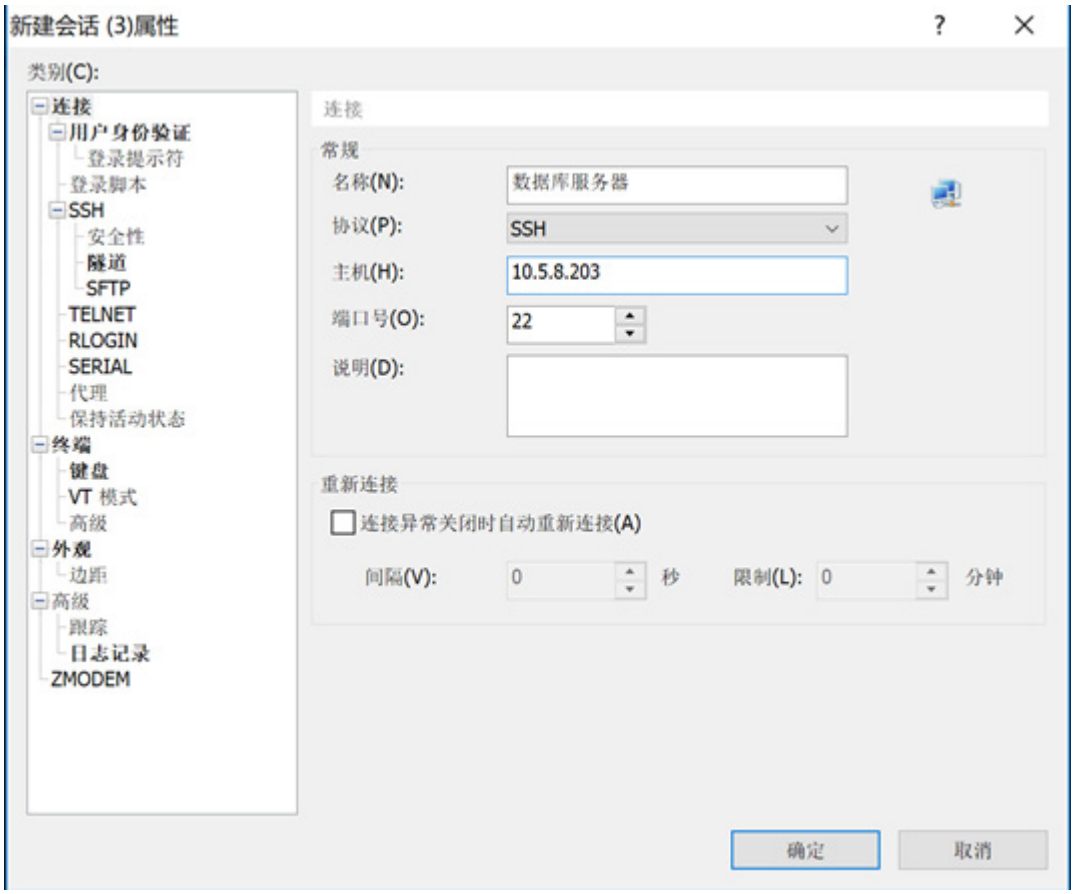

## 1.2 Linux版本安装与配置

Linux 版安装包分为 64 位和 32 位两种，64 位安装包理论上支持 Linux 2.6.32 及以上内核版本的 Linux 系统，例如 Centos6 X64；32 位安装包理论上支持 Linux 2.6.24 及以上内核版本的 Linux 系统，例如 ubuntu 14.04 X86。

### 1. 流量探针客户端安装

使用远程工具，如 Xshell 工具，设置连接参数，输入用户名、密码，连接用户数据库服务器。

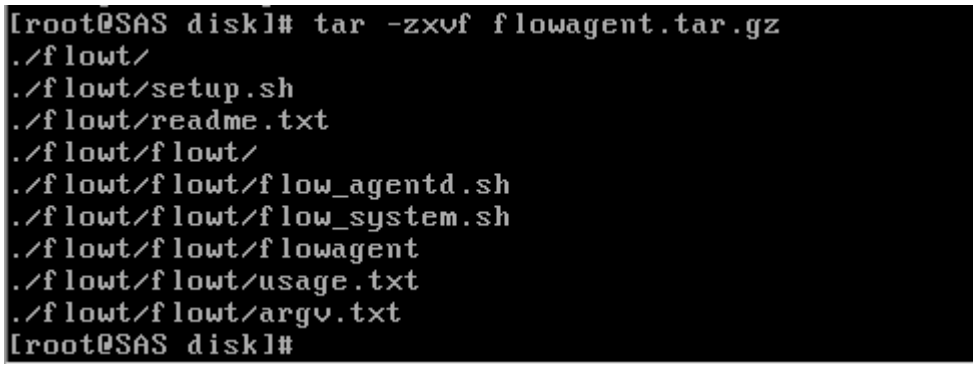
图1-2 连接 linux 服务器




连接上数据库服务器后，将下载好的流量探针 flowagent.tar.gz （如果系统版本为 32 位，则使用 flowagent_32.tar.gz）文件通过文件传输工具 Xftp 上传到用户许可的文件夹。例如，上传到根目录下的 mnt/disk 文件夹，使用命令（cd /路径名，如“cd /mnt/disk”）进入该文件夹后，接着使用解压命令“tar -zxvf flowagent.tar.gz”，解压 flowagent.tar.gz 文件。

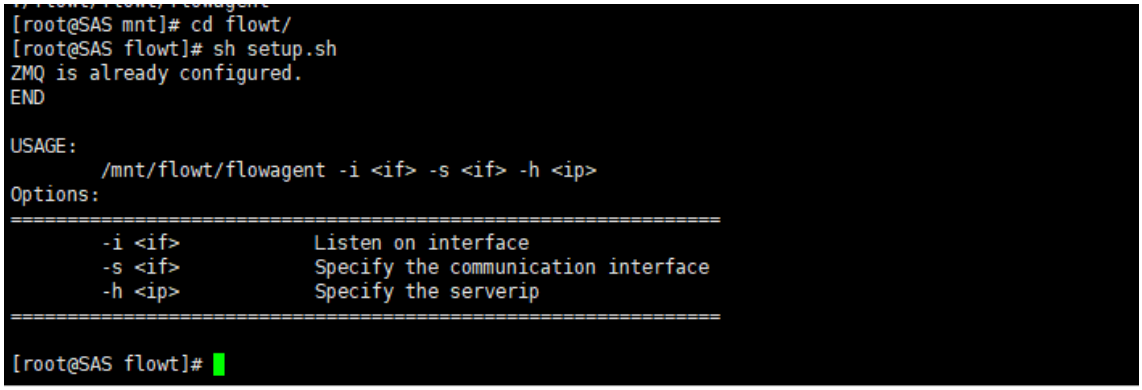
备注：可使用“getconf LONG_BIT”命令查看 Linux 系统是 64 位还是 32 位。

图1-3 解压安装包




进入解压后的 flowt 文件夹，输入安装命令“sh setup.sh”，回车后完成安装。

图1-4 完成安装界面




## 2. 流量探针客户端卸载

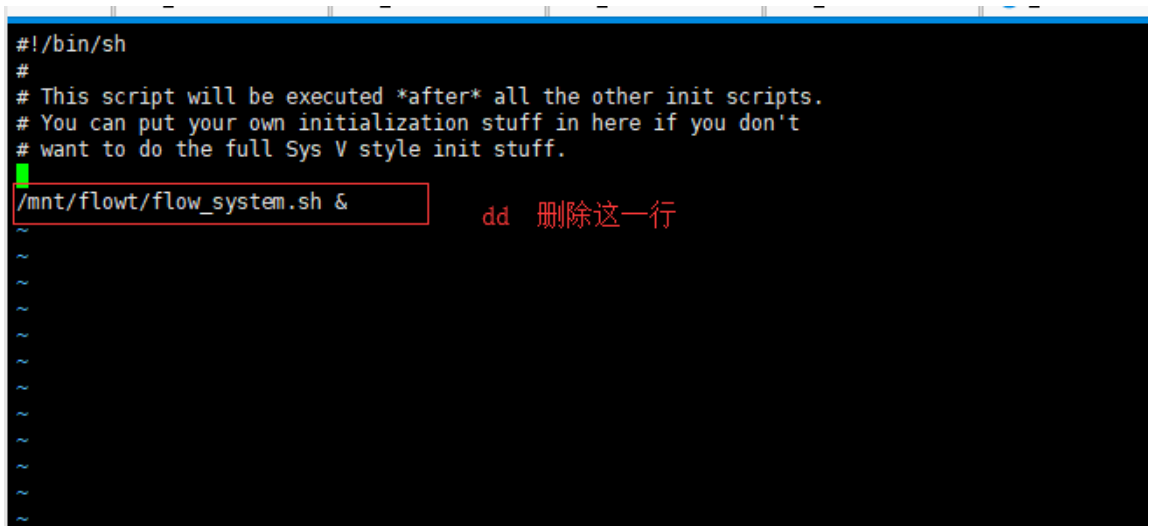
(1) 卸载流量探针客户端，需先停止流量转发服务，输入命令：“/mnt/flowt/flow_agentd.sh stop”，停止流量转发服务；

(2) 删除 etc 目录下的 rc.local 文件中的“/mnt/flowt/flow_system.sh &”，并保存退出。具体步骤如下：

a. 输入“vi /etc/rc.local”命令，打开 rc.local 文件；

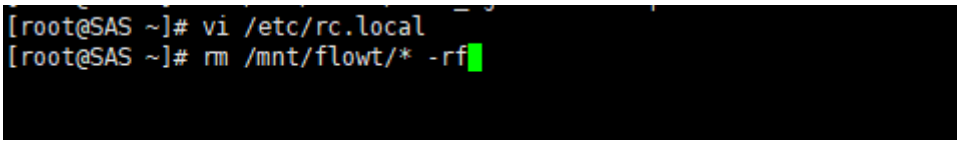
b. 移动光标到“/mnt/flowt/flow_system.sh &”这行，输入“dd”，删除这行；

图1-5 删除行界面




c. 输入“:wq”，回车，保存退出；

图1-6 保存退出后界面



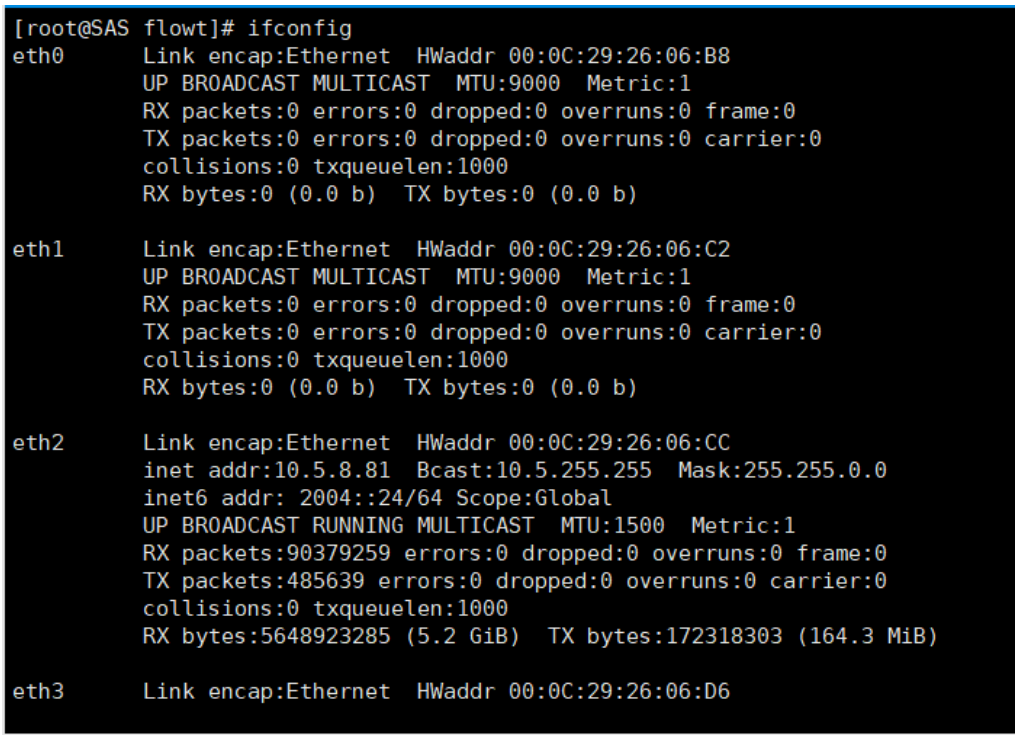

注：如误删其它行，请输入“:q!”，回车，不保存修改退出，重新操作即可。

删除运行文件目录，输入命令“rm /mnt/flowt -rf”，完成流量探针客户端卸载。

### 3. 流量探针客户端运行

(1) 安装完成后，通过“ifconfig”命令查看数据库服务器的网卡信息，获取需要进行转发流量的网卡名称。

图1-7 查看网卡信息界面




(2) 测试运行流量探针客户端，输入测试命令。

“cd /mnt/flowt”，回车，继续输入命令“./flowagent -i eth0,eth1 -s eth2 -h 10.5.8.202”

注：

eth0、eth1、eth2、10.5.8.202 根据实际环境填写。

eth0：数据库服务器上流量需被转发的网卡名。

eth1：数据库服务器上流量需被转发的网卡名。

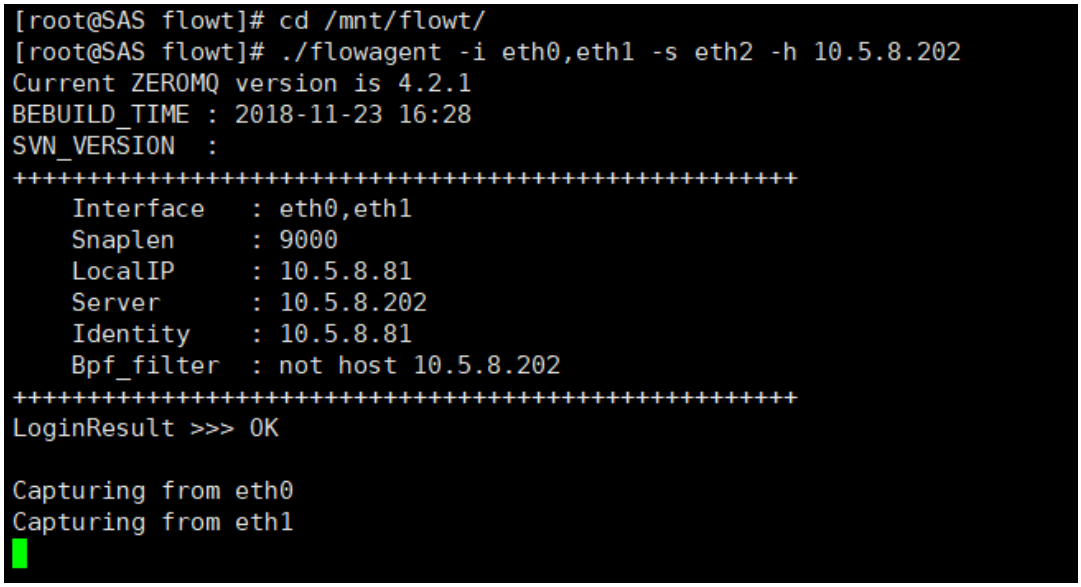
eth2：数据库服务器上通信 IP 所在的网卡名。

10.5.8.202：数据库审计设备上接收转发流量的网卡 IP。

(3) 运行测试命令后，确认流量探针是否正常运行，如果打印。

“LoginResult >>> OK”则配置并运行成功，如下图：

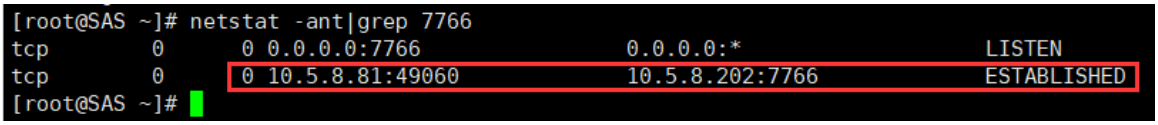
图1-8 运行命令执行成功后界面




(4) 使用组合键“Ctrl+C”退出，流量探针客户端将按照已通过的参数运行。此时，该测试参数只是临时保存，需进入参数配置文件配置参数，输入命令“vi /mnt/flowt/argv.txt”，回车后，打开参数配置文件，修改默认参数为之前测试通过的参数，即“-i eth0,eth1 -s eth2 -h 10.5.8.202 –D”，修改后保存退出，流量探针客户端会自动重新启动。

(5) 执行命令“netstat -ant|grep 7766”，如出现如下图以 tcp 开头的内容，表示流量探针已正常工作。

图1-9 探针正常运行界面




## 4. 修改流量转发网卡配置

(1) 修改流量转发网卡配置，需先停止流量转发服务，输入命令：“/mnt/flowt/flow_agentd.sh stop”，停止流量转发服务。

(2) 根据实际情况，可修改流量探针转发配置，通过输入命令“vi /mnt/flowt/argv.txt”，回车后，打开参数配置文件，修改运行参数，修改后保存退出。

(3) 修改完成后，输入命令“/mnt/flowt/flow_agentd.sh start”，启动流量转发服务。

## 5. 流量探针运行参数

系统默认内置的参数如下：

-i eth0 -s eth0 -h 10.5.6.221 –D

-i 指定需监听的网卡（网卡名可通过 ifconfig 命令查看）。在-i 后添加网卡名，可同时添加多个网卡，多个网卡间使用英文逗号“,”分割，如-i eth0,eth1;

-s 指定安装流量探针服务器上的通信网卡，在-s 后添加网卡名，不可同时添加多个网卡，如-s eth0；

-h 指定接收流量探针转发流量的审计设备的通信网卡 IP，在-h 后添加 IP，如-h 10.5.6.221。

### 6. 详细示例

假设流量探针安装在 MySQL 服务器 10.5.8.81 上，转发 MySQL 服务器网卡名为 eth0，eth1 的网卡流量，MySQL 服务器的通信网卡名为 eth2，数据库审计设备管理接收转发流量的网卡 IP 为 10.5.8.202。

(1) 停止流量探针命令

输入命令“/mnt/flowt/flow_agentd.sh stop”；

(2) 修改流量探针命令

输入命令“vi /mnt/flowt/argv.txt”，回车后，进入参数配置页，修改运行参数为

“-i eth0,eth1 –s eth2 –h 10.5.8.202 -D”，保存，退出；

(3) 修改完成后，输入命令“/mnt/flowt/flow_agentd.sh start”，启动流量转发服务。

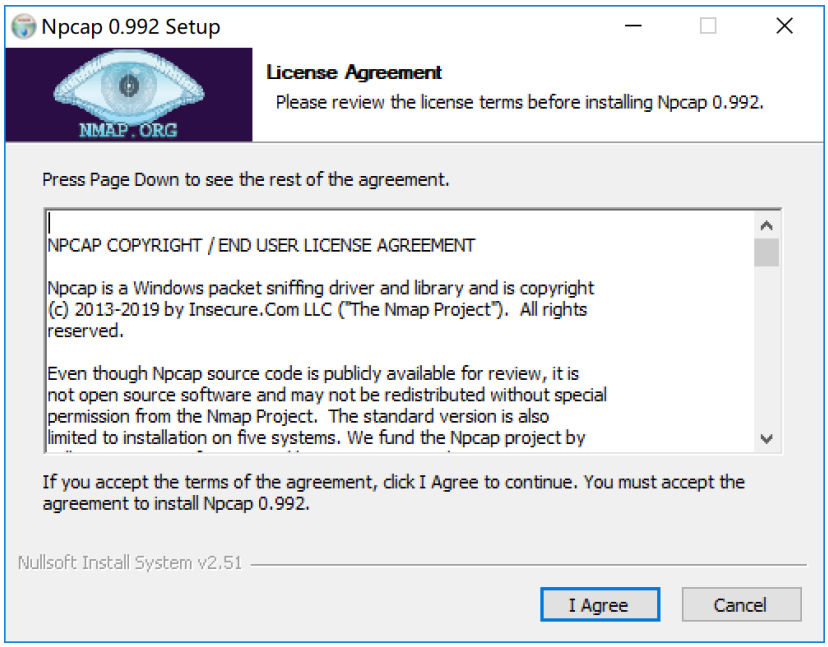
## 1.3 Windows版本安装与配置

Windows 版安装包兼容 32 位与 64 位系统，理论上 Windows 用户版支持 Windows 7 及以上操作系统，Windows 服务器版支持 Windows Server 2008 及以上操作系统。

### 1. 流量探针客户端安装

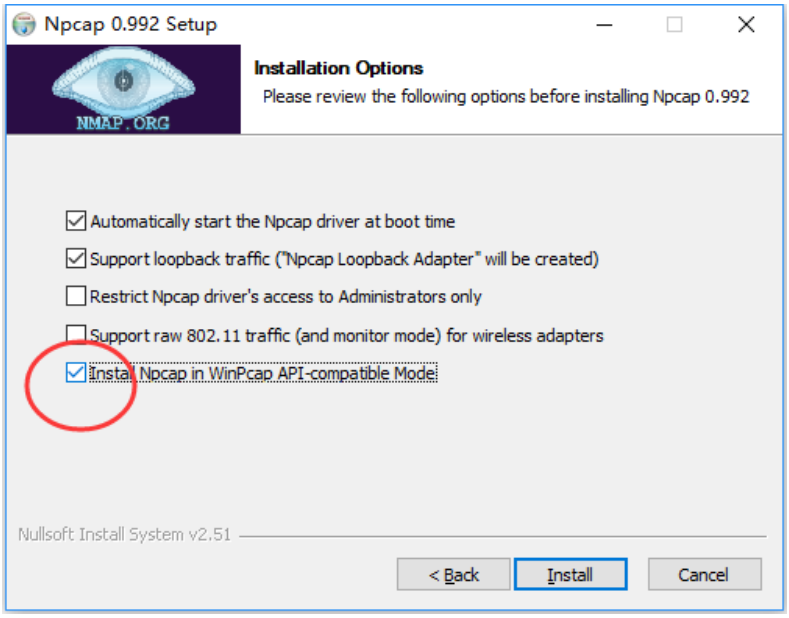
(1) 双击 npcap-0.992.exe 文件，根据提示安装 npcap；

图1-10 Npcap 安装界面



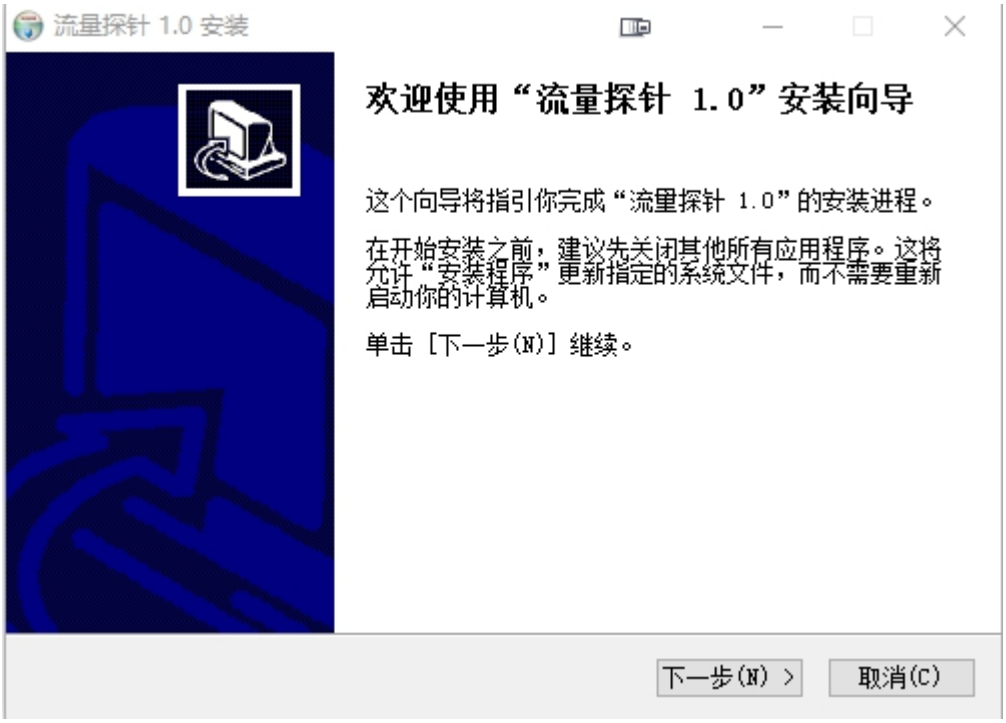
(2)　点击“I Agree”，进入下一步，勾选下图选项后，点击“Install”安装；

图1-11　Npcap 安装选项界面




(3)　双击 flowagent.exe 文件，根据提示安装客户端。

图1-12 流量探针安装界面




## 2. 流量探针客户端的配置

安装完成后，打开流量探针客户端，进行流量探针配置。

(1)　填写数据库审计设备管理接收转发流量的网卡 IP；

(2)　选择数据库服务器通信网卡/IP (数据库服务器上通信网卡 IP，一般情况下为本机的 IP)；

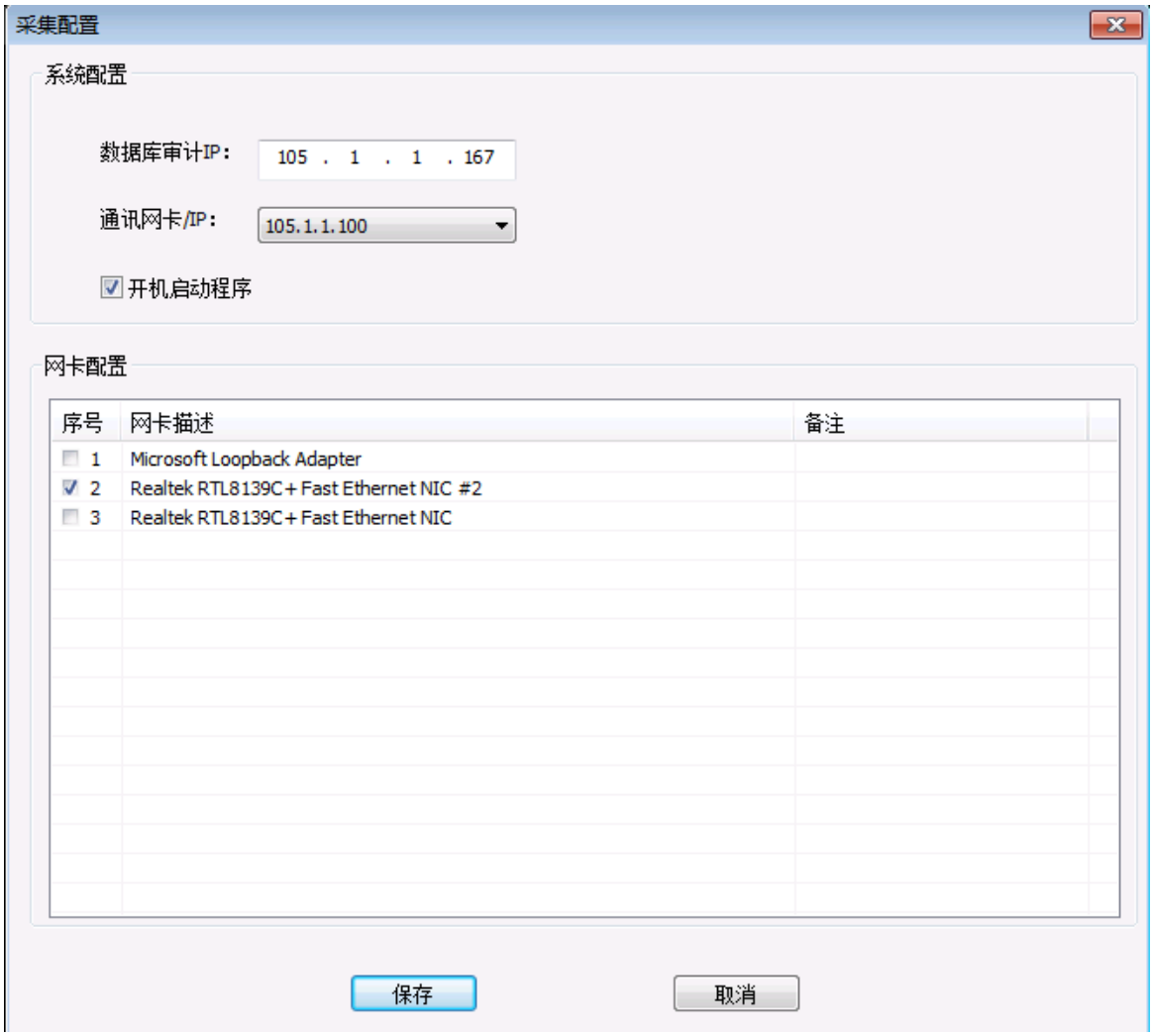
(3) 勾选是否需开机启动；

(4) 勾选数据库服务器需要转发流量的网卡，使用鼠标双击备注区域，可对该网卡进行备注。网卡描述中带有“loopback”字样的网卡为本地回环网卡，部分操作系统安装好后会出现两个或者多个本地回环网卡，如需监听本地回环数据，必须将带有“loopback”字样的网卡都勾选转发。如下图中带有“loopback”字样的网卡 1、2 必须都勾选后，才可正常监听本地回环数据。如果只是监听本地网卡（不需要回环数据），只需勾选对应的网卡即可；

(5) 点击“保存”按钮，保存配置。

如下图所示：

图1-13 流量探针配置页面



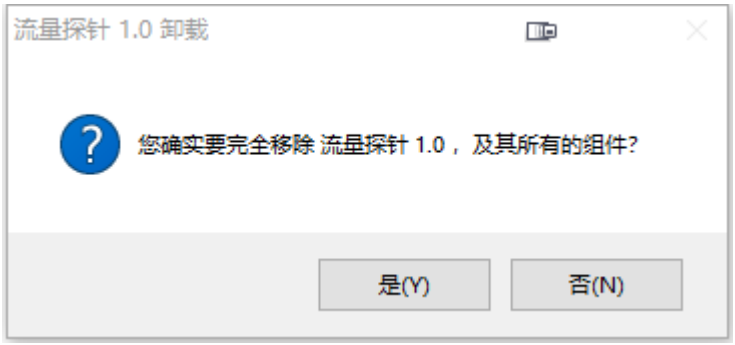

### 3. 流量探针客户端卸载

(1) 卸载流量探针客户端，需先停止流量转发服务，然后退出流量探针客户端。

(2) 在开始菜单中，点击“所有程序”，找到“流量探针”项目并点击，选择“Uninstall”，打开卸载程序，程序询问是否移除，点击“是（Y）”，卸载流量探针客户端。

图1-14 卸载快捷键


图1-15 卸载确定

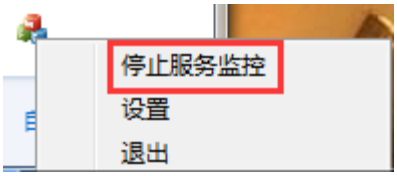



## 4. 流量转发服务管理

(1) 停止服务

在任务栏的流量探针图标上，右键点击“停止服务监控”按钮，即可停止服务。

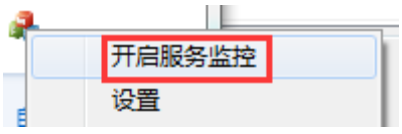
图1-16 停止服务监听




(2) 开启服务

在任务栏的流量探针图标上，右键点击“开启服务监控”按钮，即可开启服务。

图1-17 开启服务监控




(3) 完全退出

在任务栏的流量探针图标上，右键点击“退出”按钮，即可退出服务。

注：完全退出一定要先停止服务监控，再退出。

# 2 FAQ

## 2.1 问题1 提示permission denied问题

使用非 root 权限登录安装 flowagent，运行脚本时可能会出现 permission denied 问题。

解决办法

需要获取管理员权限执行在命令行前加 sudo 即可正常运行。如执行命令：

“sudo /mnt/flowagent/flowagent-ieth0 -seth0 -h172.27.53.96”

## 2.2 问题2 无法随系统启动

使用非 root 权限登录安装 flowagent，自启动脚本会加入 flowagent 启动项，但由于没有执行权限，可能导致重启服务器系统后无法正常启动 flowagent 进程。

解决办法

编辑 rc.local 文件自启动脚本，找到“/mnt/flowagent/flow_system.sh &”行，在改行前面加 sudo。