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

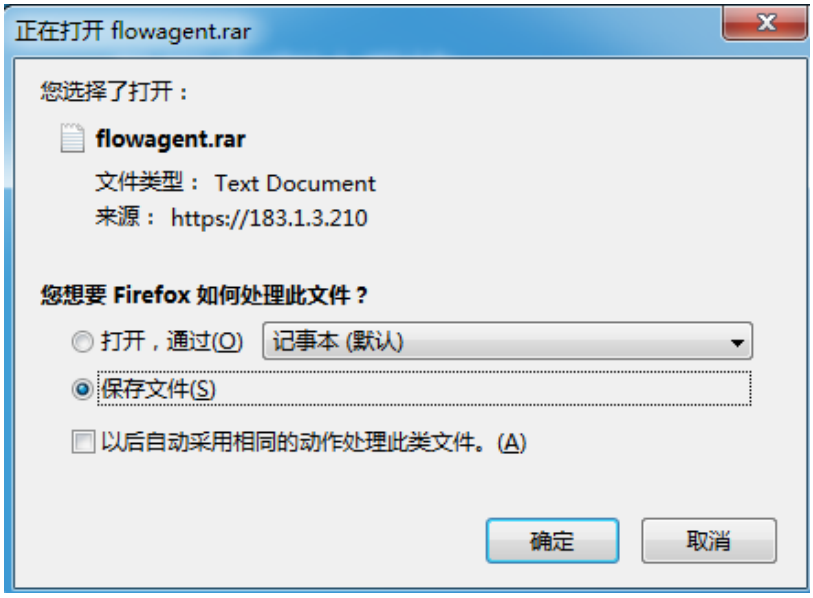
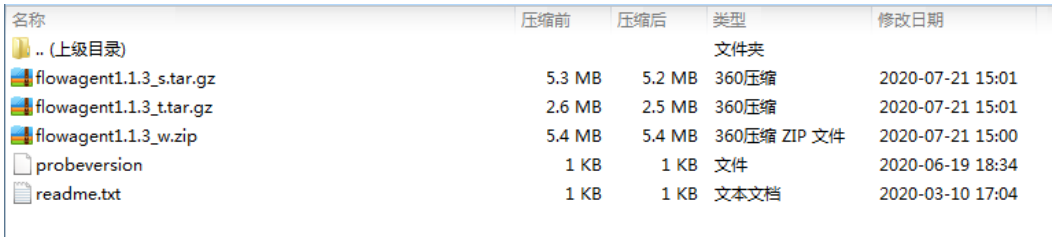


图1-2 压缩包内容



名称	压缩前	压缩后	类型	修改日期
.. (上级目录)			文件夹	
flowagent1.1.3_s.tar.gz	5.3 MB	5.2 MB	360压缩	2020-07-21 15:01
flowagent1.1.3_t.tar.gz	2.6 MB	2.5 MB	360压缩	2020-07-21 15:01
flowagent1.1.3_w.zip	5.4 MB	5.4 MB	360压缩 ZIP 文件	2020-07-21 15:00
probeversion	1 KB	1 KB	文件	2020-06-19 18:34
readme.txt	1 KB	1 KB	文本文档	2020-03-10 17:04

1.2 Linux版本安装与配置

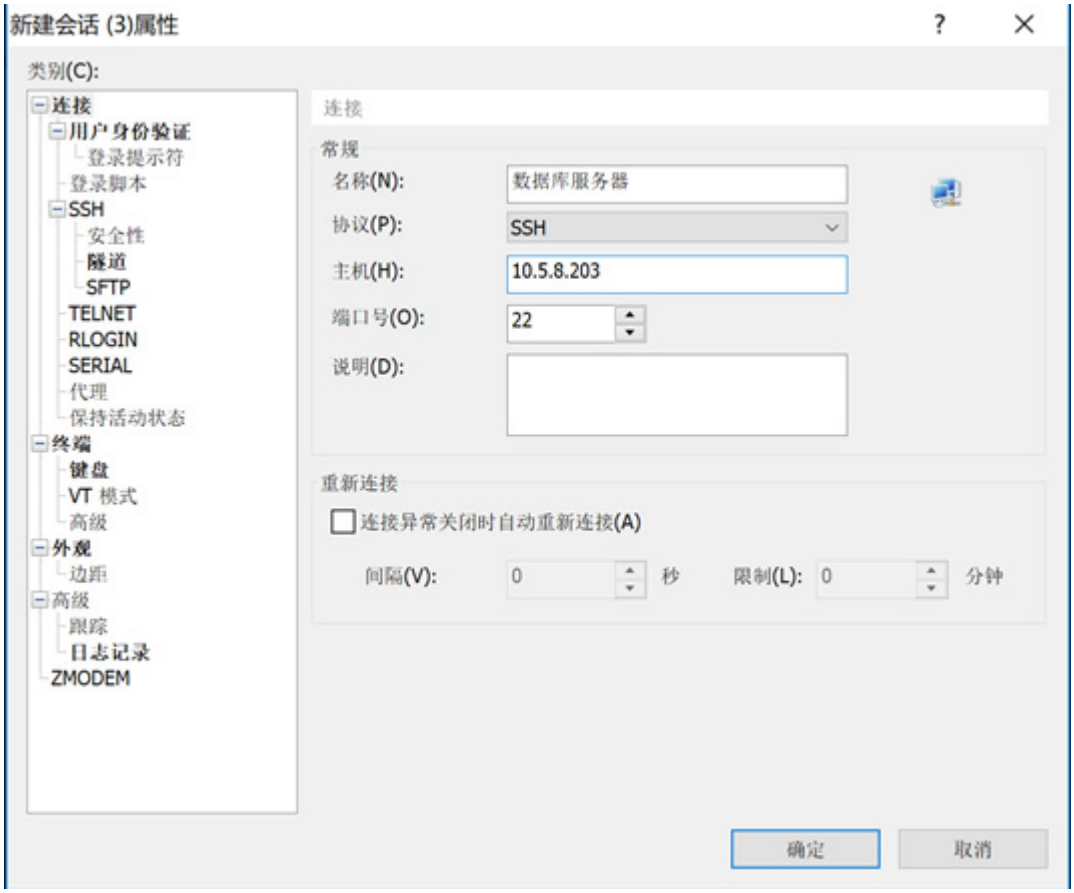
1. 流量探针客户端支持的系统版本

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 Debian 4 X86。

2. 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1-3 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 flowagent1.1.3_s.tar.gz （如果系统版本为 32 位，则使用 flowagent1.1.3_t.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 flowagent1.1.3_s.tar.gz”，解压 flowagent1.1.3_s.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1-4 解压安装包

```
[root@localhost disk]# tar zxvf flowagent1.1.3_s.tar.gz
flowt/
flowt/flowt/
flowt/flowt/flowagent
flowt/flowt/flow_system.sh
flowt/flowt/usage.txt
flowt/flowt/flow_agentd.sh
flowt/flowt/argv.txt
flowt/setup.sh
flowt/readme.txt
[root@localhost disk]#
```

进入解压后的 flowt 文件夹（cd flowt/），输入安装命令“sh setup.sh”，回车后完成安装。完成探针安装后，需修改探针监控程序权限与探针管理程序权限，并在修改完两项权限后，手动运行监控程序。

a. 输入命令“chmod 777 /mnt/flowt/flow_system.sh”，修改探针监控程序权限；

b. 输入命令“chmod 777 /mnt/flowt/flow_agentd.sh”，修改探针管理程序权限；

c. 输入命令“/mnt/flowt/flow_system.sh &”，运行探针监控程序。

图1-5 完成安装界面

```
[root@localhost disk]# cd flowt/
[root@localhost flowt]# sh setup.sh
END

USAGE:
        /mnt/flowt/flowagent -i <if> -s <if> -h <ip>
Options:
=================================================================
        -i <if>             Listen on interface
        -s <if>             Specify the communication interface
        -h <ip>             Specify the serverip
=================================================================

[root@localhost flowt]#
```

3. 流量探针客户端运行

(1) 通过“ifconfig 或 ip a”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1-6 查看网卡信息界面

```
[root@localhost flowt]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 0c:da:41:1d:24:1b brd ff:ff:ff:ff:ff:ff
    inet 108.1.2.240/24 brd 108.1.2.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::c8ea:db22:cb99:2e54/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 0c:da:41:1d:50:2c brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 0c:da:41:1d:dc:07 brd ff:ff:ff:ff:ff:ff
[root@localhost flowt]#
```

(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 eth0 -h 183.1.3.210”。

注：

eth0、eth1、183.1.3.210 根据实际环境填写。

第一个 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。

第二个 eth0：数据库服务器上与审计设备通信 IP 所在的网卡名。

183.1.3.210：数据库审计设备上接收转发流量的网卡 IP。

运行测试命令后，确认流量探针是否正常运行，初次运行时，会打印“LoginResult >>> fail”因为此时探针处于未注册状态：

图1-7 初次运行命令执行后界面

```
[root@localhost flowt]# ./flowagent -i eth0,eth1 -s eth0 -h 183.1.3.210
BEBUILD_TIME : 2020-07-10 16:00
PROBE_VERSION: 1.1.3_s
++++++++++++++++++++++++++++++++++++++++++++++++++++++
    Interface   : eth0,eth1
    Snaplen     : 9000
    LocalIP     : 108.1.2.240
    Server      : 183.1.3.210
    Identity    : 108.1.2.240
    Bpf_filter  : not host 183.1.3.210
++++++++++++++++++++++++++++++++++++++++++++++++++++++
{"list":[{"name":"lo","alias":"lo","status":"1","is_listen":"0"},{"name":"eth0","alias":"eth0","sta
:"eth1","status":"1","is_listen":"1"},{"name":"eth2","alias":"eth2","status":"1","is_listen":"0"}]}
msglen:280
CheckLoginStatus
LoginResult >>> fail
```

使用组合键“Ctrl+C”退出，此时需进入数据库安全审计系统的监控中心/流量探针页面，配置此探针且探针状态为已注册，具体操作参考本文“流量探针管理”章节。

注意：若之前安装卸载过流量探针，当执行上述命令时，会提示另外一个探针进程在运行，此时需先关闭命令，使用“ps aux|grep flowagent”查看进程，使用“kill -9 进程号”关闭该进程，再重新执行上述步骤。

```
[root@localhost flowt]# ./flowt/flowagent -i eth0,eth1 -s eth0 -h 183.1.3.210
BEBUILD_TIME : 2020-07-10 16:00
PROBE_VERSION: 1.1.3_s
Another Flowagent is in processing.
Exit...
[root@localhost flowt]#
```

```
[root@localhost flowt]#
[root@localhost flowt]# ps aux |grep flowagent
root     19206  0.0  0.0   2800   724 ?        S    23:37   0:00 /mnt/flowt/flowagent -ieth0 -seth0 -h10.5.6.221 -D
root     19238  0.0  0.0 112704   928 pts/0    S+   23:39   0:00 grep --color=auto flowagent
[root@localhost flowt]# kill -9 19206
[root@localhost flowt]#
```

(3) 再次运行探针，此时会出现“LoginResult >>> OK”的提示，表示探针安装配置成功，如下图所示：

图1-8 运行命令执行成功后界面

```
[root@localhost flowt]# ./flowagent -i eth0,eth1 -s eth0 -h 183.1.3.210
BEBUILD_TIME : 2020-07-10 16:00
PROBE_VERSION: 1.1.3_s
++++++++++++++++++++++++++++++++++++++++++++++++++++
    Interface   : eth0,eth1
    Snaplen     : 9000
    LocalIP     : 108.1.2.240
    Server      : 183.1.3.210
    Identity    : 108.1.2.240
    Bpf_filter  : not host 183.1.3.210
++++++++++++++++++++++++++++++++++++++++++++++++++++
{"list":[{"name":"lo","alias":"lo","status":"1","is_listen":"0"},{"name":"eth0","alias":"eth0","status":"1
:"eth1","status":"1","is_listen":"1"},{"name":"eth2","alias":"eth2","status":"1","is_listen":"0"}]},246
msglen:280
CheckLoginStatus
LoginResult >>> OK
```

此时先“Ctrl+C”停止手动运行，再执行“./flow_agentd.sh start”，让探针在后台自动运行。

```
[root@localhost flowt]# ./flow_agentd.sh start
BEBUILD_TIME : 2020-07-10 16:00
PROBE_VERSION: 1.1.3_s
[root@localhost flowt]#
```

(4) 执行命令“netstat -ant|grep 7766”，如出现以 tcp 开头的内容，表示流量探针注册成功后已在正常工作，如下图所示：

图1-9 探针正常运行界面

```
[root@localhost flowt]#
[root@localhost flowt]# netstat -ant |grep 7766
tcp6       0      0 108.1.2.240:35764       183.1.3.210:7766        ESTABLISHED
[root@localhost flowt]#
```

4. 修改流量转发网卡配置

(1) 若需要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。

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 或 ip a 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. 示例

假设流量探针安装在 MySQL 服务器 10.5.19.89 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 10.5.6.71。

(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 10.5.6.71 -D”，保存，退出；

(3) 启动流量转发服务

修改流量探针配置完成后，输入命令“/mnt/flowt/flow_agentd.sh start”，启动流量转发服务。

7. 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；

```
[root@localhost flowt]#
[root@localhost flowt]# /mnt/flowt/flow_agentd.sh stop
[root@localhost flowt]#
```

注：出现“command not found”错误，以 centos 系统为例，使用命令”yum install psmisc -y”

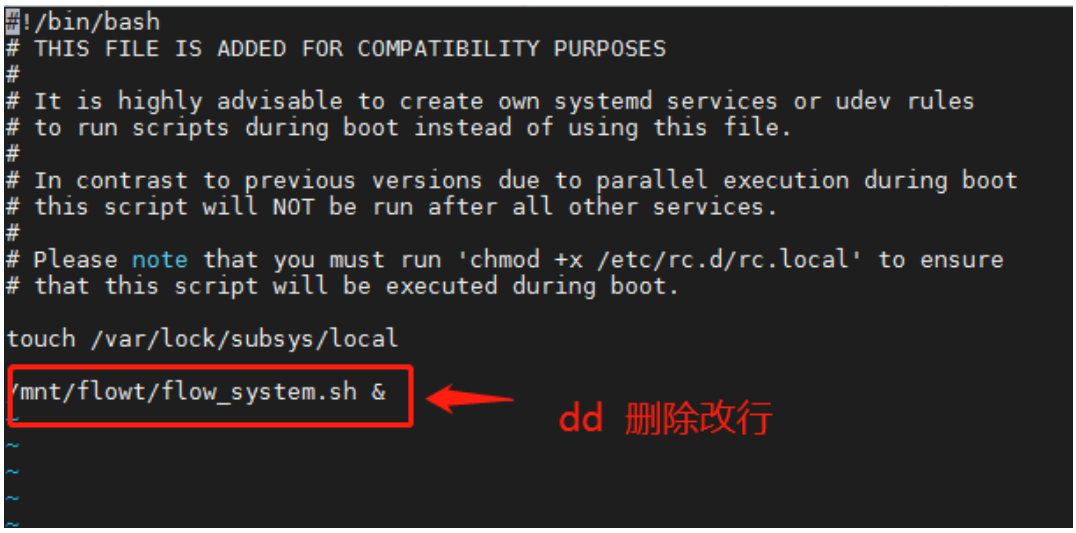
```
[root@localhost flowt]# /mnt/flowt/flow_agentd.sh stop
/mnt/flowt/flow_agentd.sh: line 45: killall: command not found
[root@localhost flowt]# yum install psmisc -y
Loaded plugins: fastestmirror
```

(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；

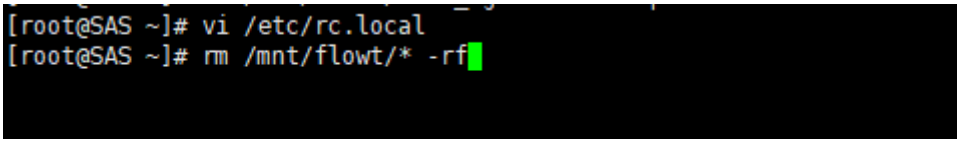
b. 移动光标到“/mnt/flowt/flow_system.sh &”这行，输入“dd”，删除这行；

图1-10 删除行界面



c. 输入“:wq”，回车，保存退出；

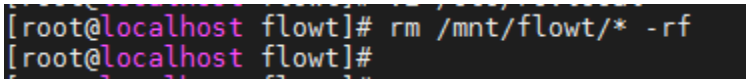
图1-11 保存退出后界面



注：如 B 步骤误删其它行，请输入“:q!”， 回车，不保存修改退出，重新操作即可。

d. 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。

图1-12 删除文件目录



1.3 Windows版本安装与配置

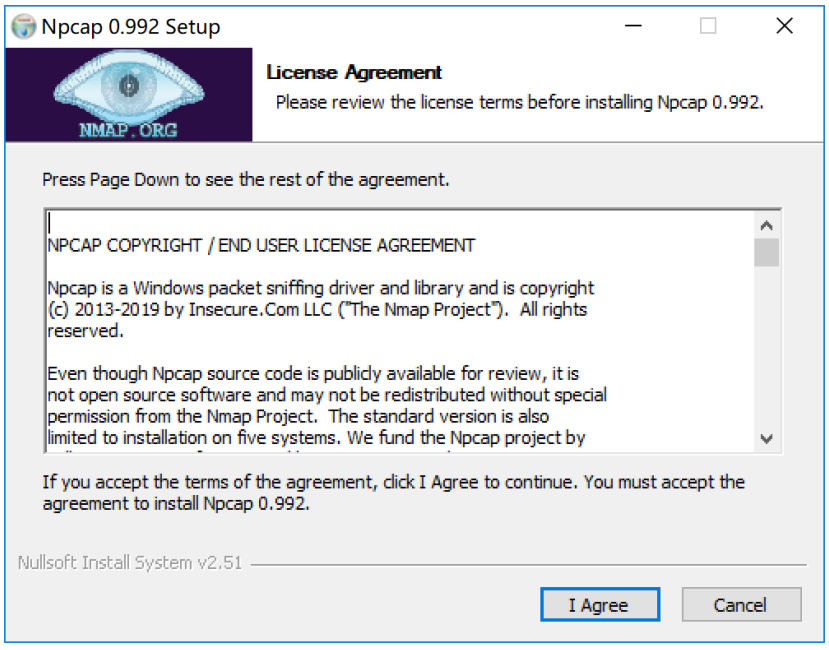
1. 流量探针客户端支持的系统版本

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。

2. 流量探针客户端安装

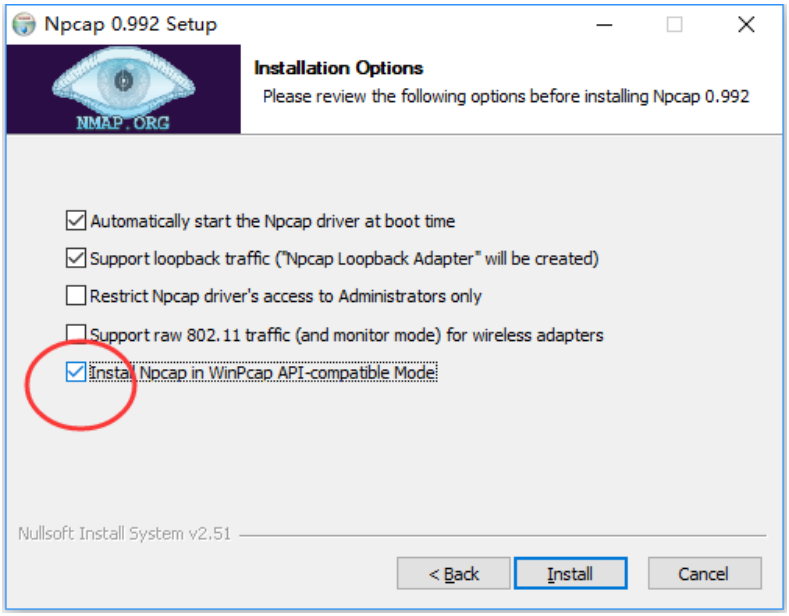
(1) 双击 npcap-0.992.exe 文件，根据提示安装 npcap；

图1-13 Npcap 安装界面



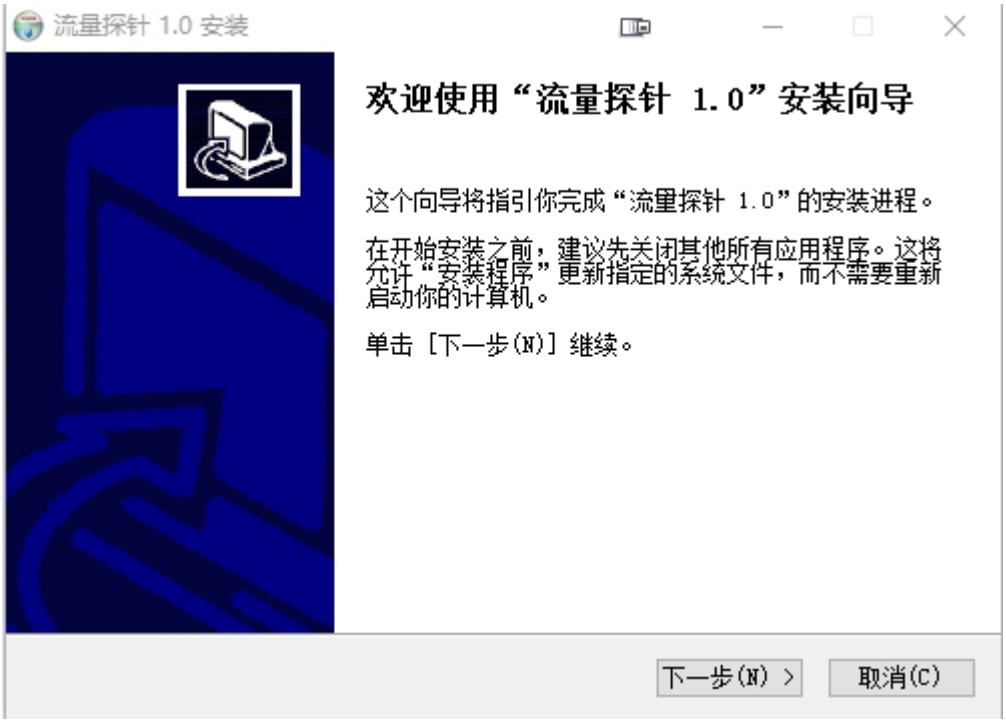
(2) 点击“I Agree”，进入下一步，勾选下图选项后，点击“Install”安装；

图1-14 Npcap 安装选项界面



(3) npcap 安装完成后，双击 flowagent.exe 文件，根据提示安装客户端。

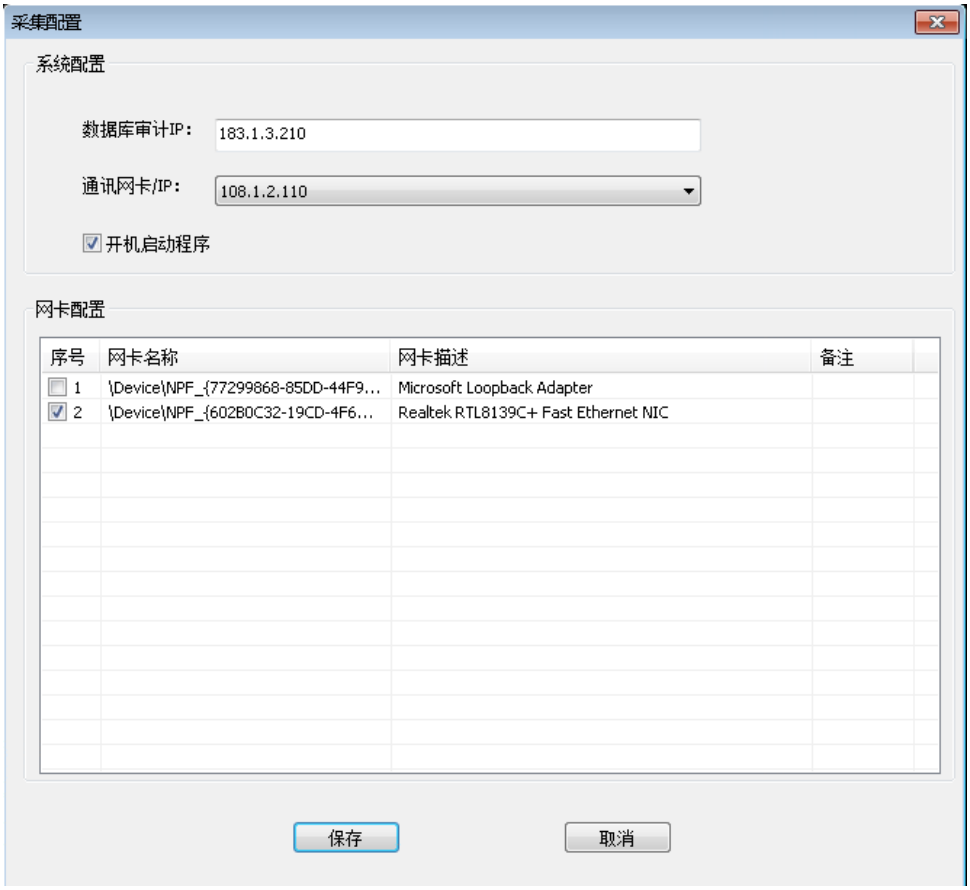
图1-15 流量探针安装界面



3. 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。

图1-16 流量探针配置页面



(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。如果安装后有多个“loopback”字样的网卡，则带有“loopback”字样的网卡必须都勾选后，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。

(6) 进入数据库安全审计系统的监控中心/流量探针页面，配置此探针且探针状态为已注册，具体操作请参考“流量探针管理”章节。

(7) 点击保存，使用 admin 账号登录数据库管理系统，在“监控中心-流量探针”模块配置探针，具体参考本文“流量探针管理”章节。

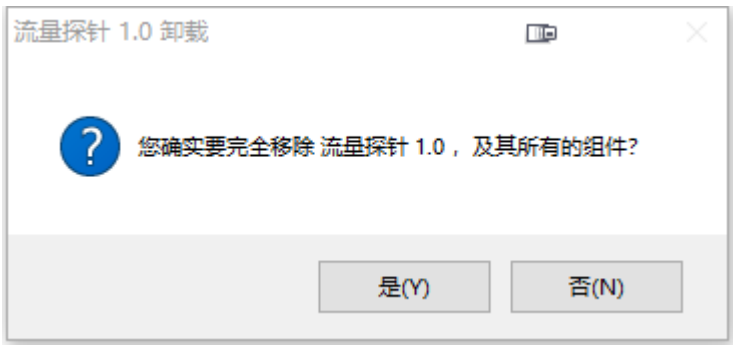
4. 流量探针客户端卸载

(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1-17 卸载快捷键

图1-18 卸载确定

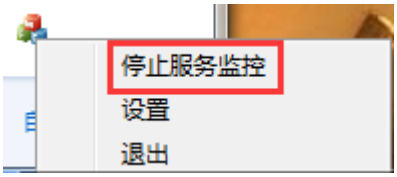


5. 流量转发服务管理

(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。

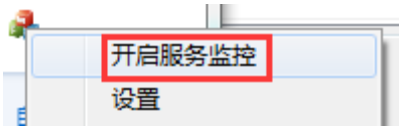
图1-19 停止服务监听



(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1-20 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 流量探针管理

2.1 流量探针确认

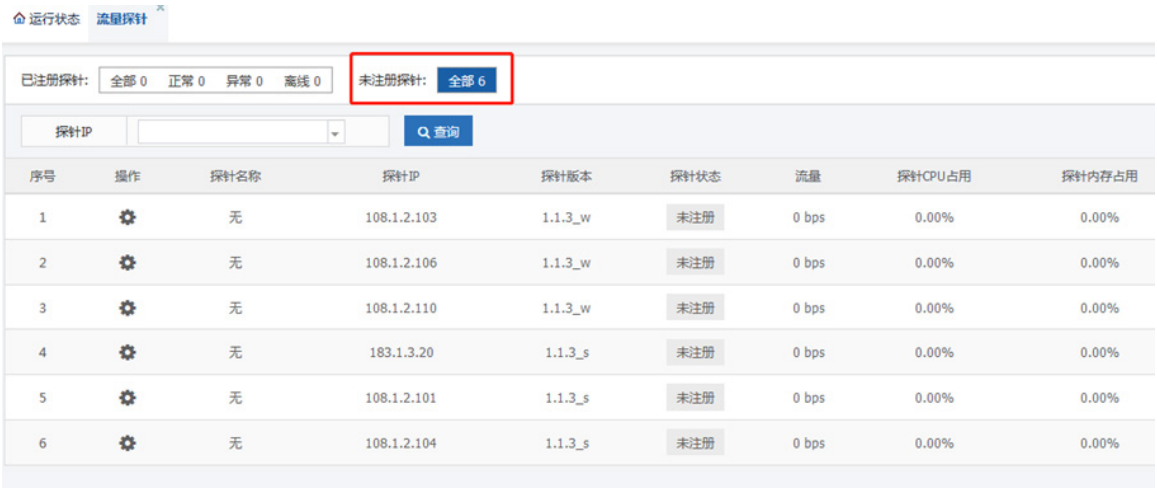
按照“流量探针的安装指导”章节安装流量探针，确保流量探针已与数据库安全审计系统通讯成功。下文中提到的“系统”，皆指数据库安全审计系统。

注：可使用 ping 查看探针客户端所在服务器与数据库审计系统是否网络可达。

2.2 流量探针配置

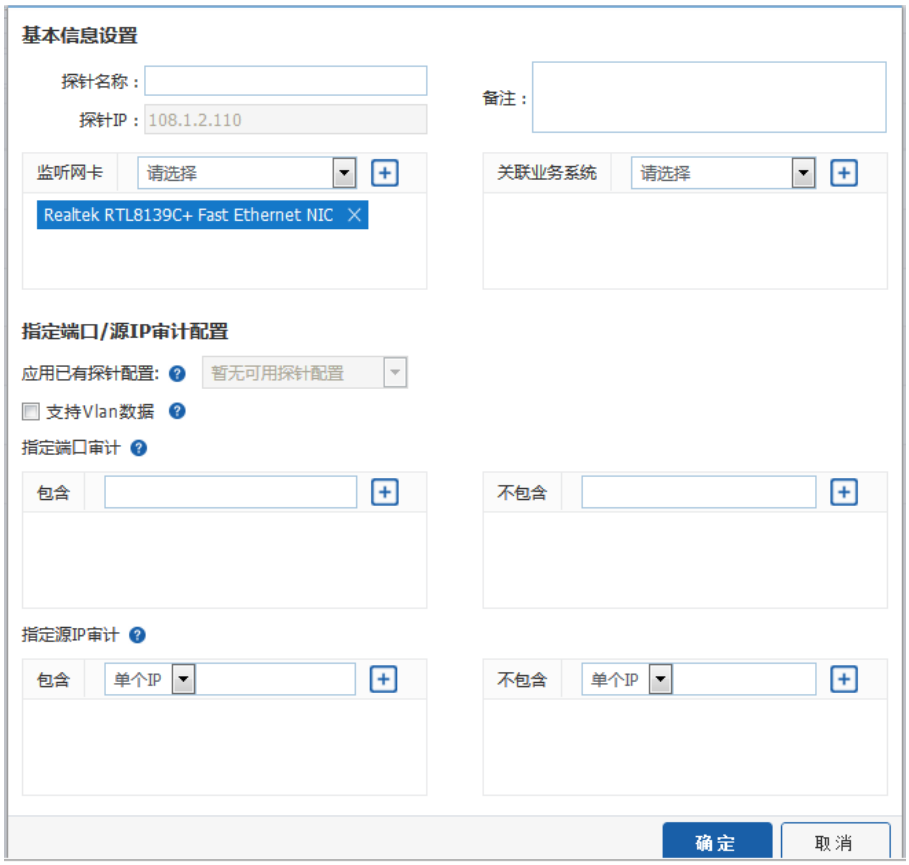
(1) 客户端安装配置完成之后，使用“admin”账户登录系统，进入[监控中心/流量探针]页面，可看到已在服务器上安装配置完成，并与数据库安全审计系统成功通讯且探针状态为“未注册”的流量探针，如下图所示。

图2-1 未注册探针页面



(2) 点击某个未注册探针前的 图标，弹出探针配置窗口，用户可根据需要对流量探针进行详细配置，如探针名称、探针 IP、备注、监听网卡选择、关联业务系统，指定端口/源 IP 审计配置等，配置完成之后，点击<确定>按钮，系统提示修改探针配置成功，该流量探针移入已注册探针列表，并开始转发流量。

图2-2 探针配置页面



- 探针名称：用于标识探针名称，为必填项。
- 备注：用于备注流量探针相关信息，便于用户查阅和管理，为选填项。
- 监听网卡：用于配置流量探针客户端需要转发流量的网卡，为必填项。
- 关联业务系统：用于标识流量探针转发的数据源，关联业务系统，为选填项。
- 应用已有探针配置：可选择已配置的探针配置应用到此探针，为选填项。
- 支持 Vlan 数据：当监听的数据流量中有 vlan 数据时勾选，当不确定是否含有 vlan 数据时，建议先勾选。
- 指定端口/源 IP 审计配置：流量探针支持转发流量过滤，可转发对指定端口/源 IP 的流量。支持过滤内容包括端口、IP 及 IP 网段信息，数据范围支持包含与不包含。设置包含后，仅在包含范围内的数据才会被转发。设置不包含后，在不包含范围内的数据不会被转发。如包含与不包含的配置范围重叠，不包含的优先级更高。

注意：若探针客户端配置的数据库审计 IP 不是审计设备管理口（即 GE0/0 口地址），需要手动将探针业务口 ip 加入过滤规则，或者将探针的 7766 端口加入过滤规则，如下图。

图2-3 非管理口（GE0/0）口地址

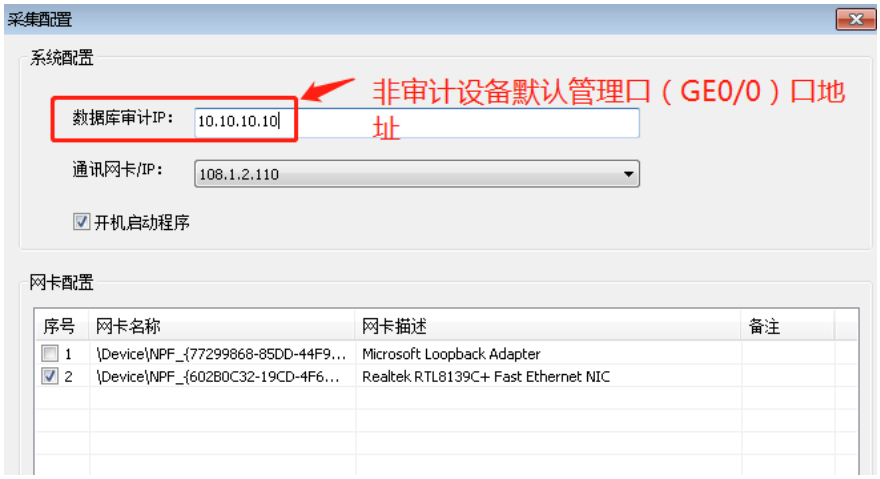
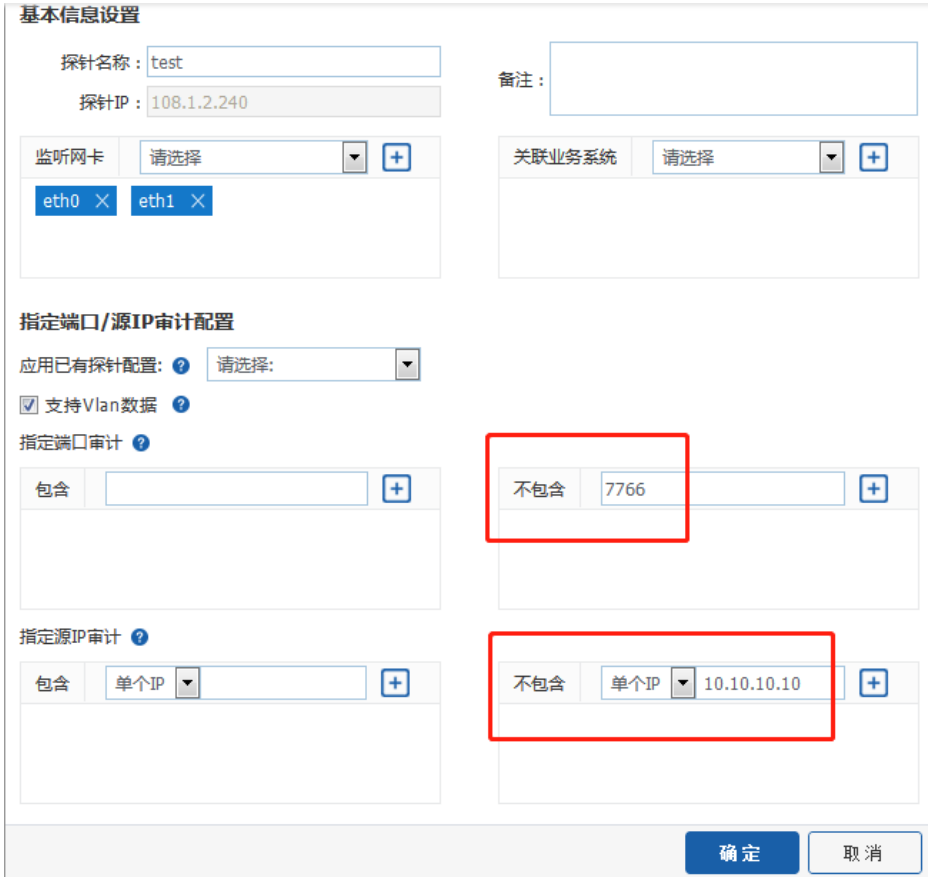


图2-4 加入过滤规则



(3) 完成流量探针配置后，点击左侧菜单栏“策略中心-监听配置-业务系统配置”，添加探针客户端所属的数据库信息，如下图。

2.3 流量探针参数介绍

1. 检索栏

检索栏分为两部分，第一部分按照已注册探针与未注册探针区分，并统计对应部分的探针总数。点击已注册探针的<全部>、<正常>、<异常>、<离线>等按钮，或点击未注册探针的<全部>按钮，在下方以列表方式展示该类流量探针信息。第二部分包括探针名称、探针 IP、服务器操作系统、关联业务系统等，用户可根据以上条件检索流量探针，方便用户管理流量探针。

2. 探针状态说明

已注册流量探针状态可分为：正常、离线、异常。

(1) 正常

流量探针正常运行，未出现异常状况。

(2) 离线

流量探针与数据库安全审计系统失去通讯超过两分钟，则系统判断为为离线状态。若离线超过 10 分钟，将触发系统弹窗告警。

(3) 异常

目前存在 3 种异常状况：

a. 系统超过 10 分钟未收到流量探针转发的流量，则认定为为异常状态，并触发弹窗告警。

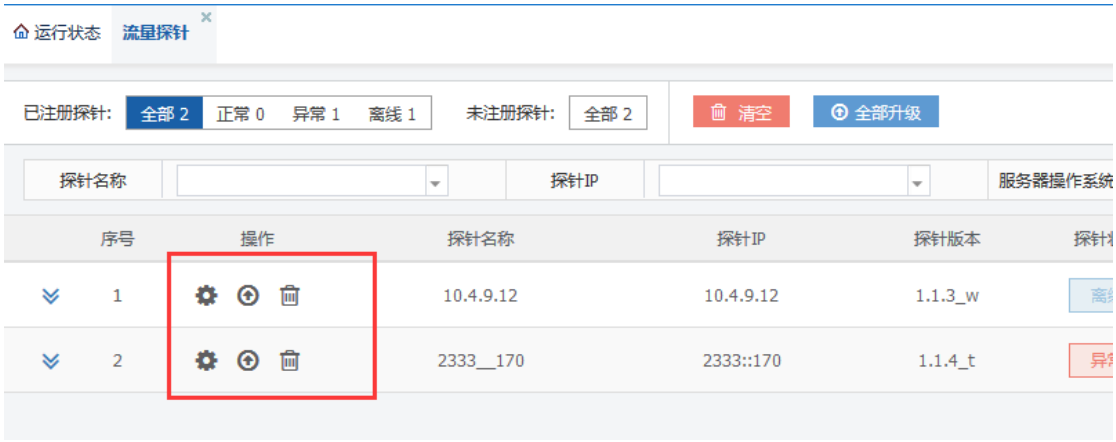
b. 流量探针 CPU 使用率超过 10%，则认定为异常状态，并触发弹窗告警。

流量探针内存使用率超过 5%，则认定为异常状态，并触发弹窗告警。

3. 流量探针列表

流量探针列表流量探针的所有信息，包括序号、操作、探针名称、探针 IP、探针版本、探针状态、流量、探针 CPU 占用、探针内存占用、监听网卡、服务器操作系统、备注等信息。同时并提供流量管理操作，包括配置、升级、删除等。如下图所示：

图2-5 探针基本操作



(1) 配置

点击需配置流量探针操作列的 图标，弹出该流量探针的探针配置窗口，具体配置方法可参考“流量探针注册”章节。

(2) 升级

点击需升级版本流量探针操作列的 图标，系统提示是否确定升级探针到系统内置的流量探针版本，点击<确定>，如果符合升级条件（系统内置的流量探针安装包版本高于连接上系统的流量探针版本），系统开始升级流量探针。

依据现场网络情况，升级过程可能会持续一段时间。此时，刷新流量探针页面，会发现探针可能处于升级准备或者升级中状态。

若流量探针升级成功，系统更新该流量探针的版本信息。若升级失败，系统提示相关的失败信息。

系统支持批量升级流量探针，点击页面的<全部升级>按钮，系统批量升级已注册列表下的全部流量探针。

(3) 删除

点击需删除流量探针操作列的 图标，系统提示是否确定删除该探针，点击<确定>按钮，系统在页面移除该流量探针。如果在服务器上的探针未被卸载，且与数据库安全审计系统再次通讯成功后，则此探针会进入未注册探针列表。

点击<清空>按钮，则可删除已注册列表下的全部探针。

4. 流量探针二级信息展示

在流量探针列表，点击某行流量探针的任意位置，可展开该流量探针的二级信息，以图表的方式展示该流量探针的运行情况。如下图所示：

图2-6 探针二级信息展示

3 FAQ

3.1 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”

3.2 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。

```
[dzkauser@dzka-qqsyyy flowagent]$ sudo vi  /etc/rc.local
[dzkauser@dzka-qqsyyy flowagent]$
[dzkauser@dzka-qqsyyy flowagent]$
[dzkauser@dzka-qqsyyy flowagent]$ cat /etc/rc.local
#!/bin/bash
# THIS FILE IS ADDED FOR COMPATIBILITY PURPOSES
#
# It is highly advisable to create own systemd services or udev rules
# to run scripts during boot instead of using this file.
#
# In contrast to previous versions due to parallel execution during boot
# this script will NOT be run after all other services.
#
# Please note that you must run 'chmod +x /etc/rc.d/rc.local' to ensure
# that this script will be executed during boot.

touch /var/lock/subsys/local

sudo /mnt/flowagent/flow_system.sh &
```