**Windows agent使用手册**

**文档版本：V2.0**

**发布日期：2020/07/28**

# 目录

[目录 2](#_Toc47358252)

[一、本文档适用范围 3](#_Toc47358253)

[二、安装前准备 3](#_Toc47358254)

[1.1 环境说明 3](#_Toc47358255)

[1.2 安装环境确认 4](#_Toc47358256)

[1.3 安装前注意事项 4](#_Toc47358257)

[三、Agent安装说明 5](#_Toc47358258)

[2.1 上传并解压Windows agent包 5](#_Toc47358259)

[2.3 安装Windows agent程序 5](#_Toc47358260)

[四、Agent相关功能操作 9](#_Toc47358261)

[3.1 启动Windows agent程序 9](#_Toc47358262)

[3.2 终止Windows agent程序 11](#_Toc47358263)

[3.3 Agent运行状况的确认及检查 11](#_Toc47358264)

[五、设置开机启动服务 12](#_Toc47358265)

[4.1 设置开机启动服务 12](#_Toc47358266)

[4.2 更新Agent服务 13](#_Toc47358267)

[4.3 取消开机启动服务 15](#_Toc47358268)

[六、卸载Windows agent 15](#_Toc47358269)

[七、常见问题说明 16](#_Toc47358270)

# 一、本文档适用范围

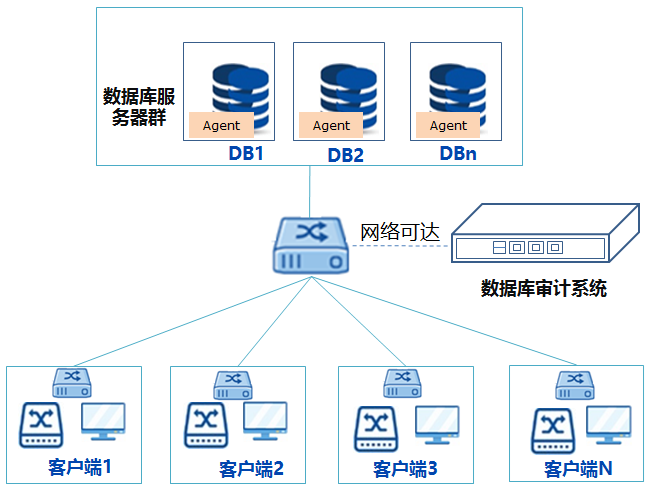
|  |  |
| --- | --- |
| **类型** | **版本** |
| 适用Agent版本 | Windows agent-5.1.1-Auth |
| 适用数审版本 | 数据库审计 V6.0及以上版本 |
| 适用操作系统 | Windows7 64位  Windows10 64位  Windows server 2008  Windows server 2012  Windows server 2016  Windows server 2019 |

# 二、安装前准备

## 2.1 环境说明

1. Agent插件部署在数据库服务器上，它负责将数据库指定的数据库流量转发到数据库审计设备，Agent引流环境中，数据库服务器和数审设备需网络可达
2. Agent插件部署在应用服务器上，它负责将应用服务器到数据库指定的数据库流量转发到数据库审计设备，Agent引流环境中，应用服务器和数审设备需网络可达
3. 环境示例（Agent部署在数据库服务器）：

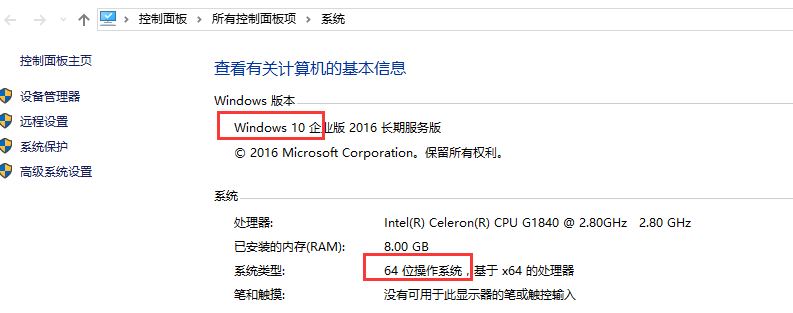
数据库审计设备的IP地址是172.24.1.115， MySQL数据库安装Windows服务器上，服务器的地址是172.21.1.10，所以，需要将Windows agent放在172.21.1.10服务器上运行



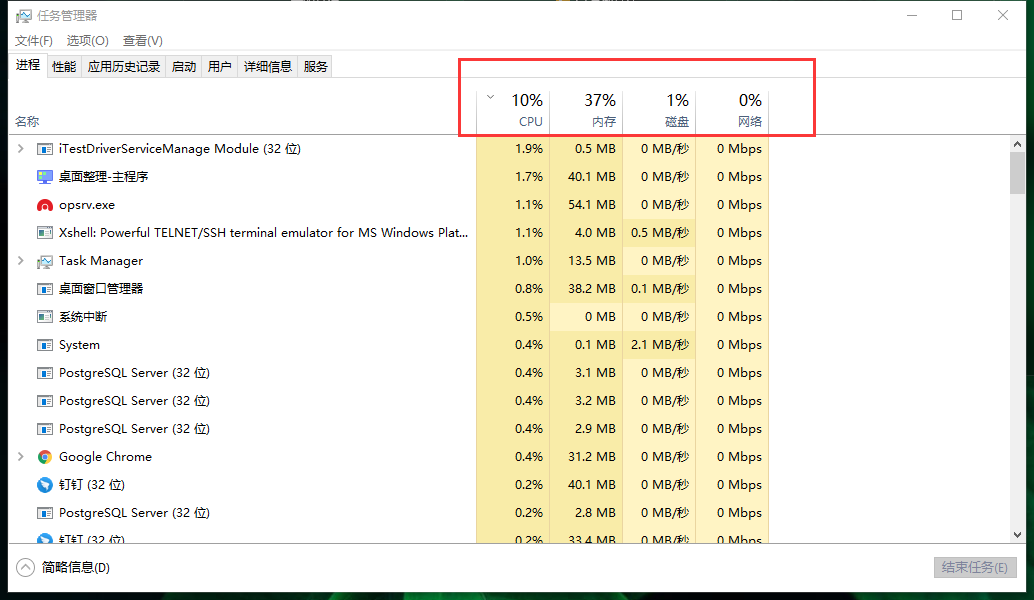
拓扑示意图

## 2.2 安装环境确认

1. 右击【我的电脑】，选择属性，查看操作系统信息，确认操作系统是在兼容列表中



2. 打开【任务管理器】查看数据库服务器资源，如服务器CPU和内存资源占用超过80%，建议不要运行Agent



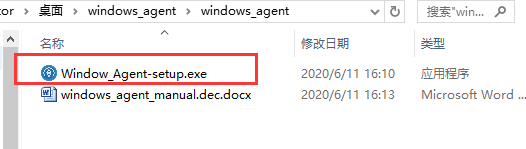
## 2.3 安装前注意事项

1. 数据库服务器和数审设备之间如果有防火墙，注意要把TCP的9999端口放开。Agent和数审设备之间是通过TCP进行连接的，有时候虽然能ping通，但是中间的防火墙有可能会阻断TCP连接

# 三、Agent安装说明

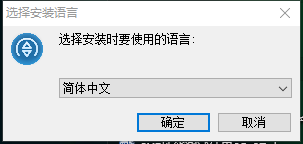
## 3.1 上传并解压Windows agent包

将安装包Windows\_agent.tar.gz上传到windows数据库服务器上并解压，解压后的文件夹中就是Windows agent的安装程序

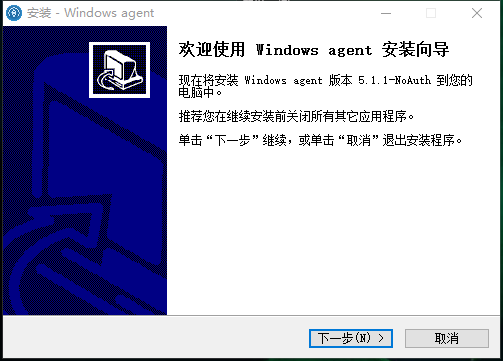


## 3.2 安装Windows agent程序

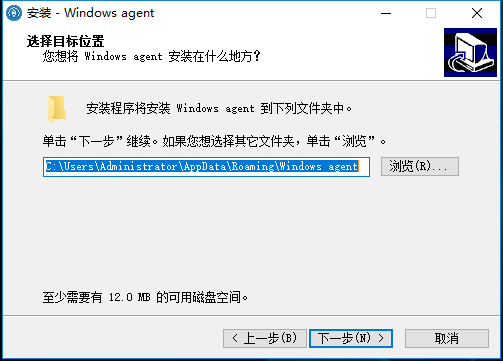
1. 双击Window\_Agent-setup.exe，进入安装程序界面，选择【简体中文】



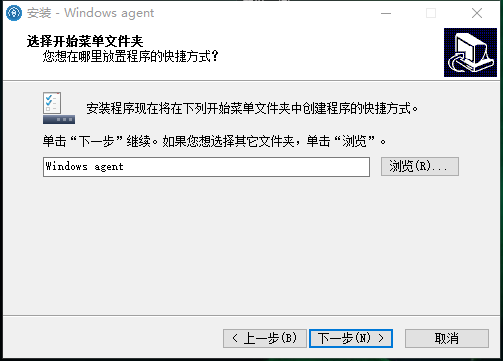
2. 选择【下一步】



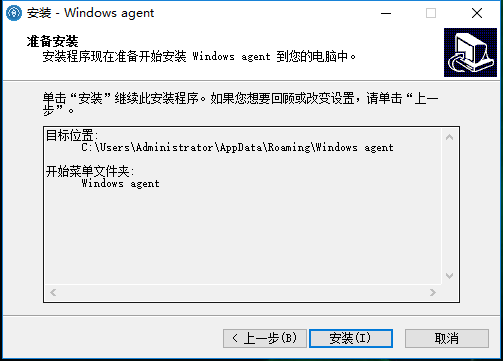
3. 选择安装目录后，点击【下一步】



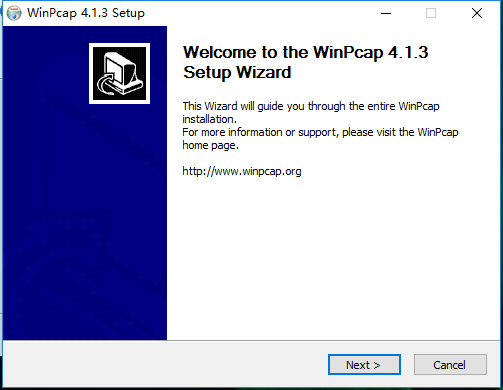
4. 设置程序的快捷方式后，点击【下一步】



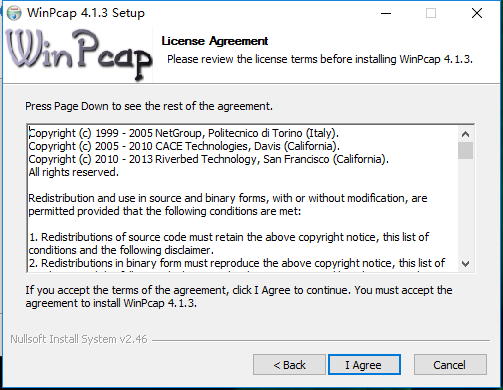
5. 点击【安装】，执行安装操作



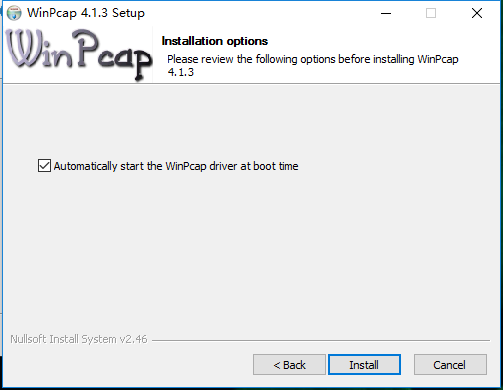
6. Agent安装完成后，会跳出WinPcap4.1.3的安装弹窗，点击【Next】



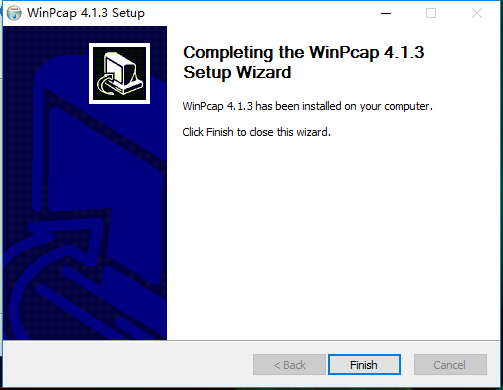
7. WinPcap4.1.3安装协议确认，点击【I Agree】



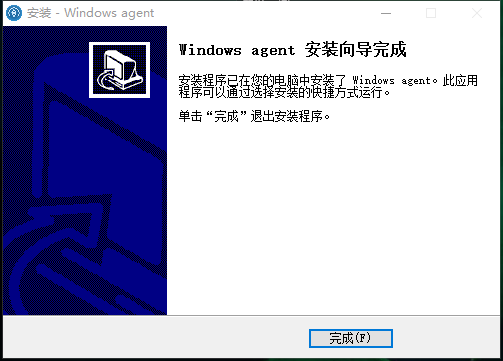
8. 选择【Install】，执行安装操作



9. WinPcap安装完成后，点击【Finish】



10. Windows agent安装完成后，点击【完成】后结束安装



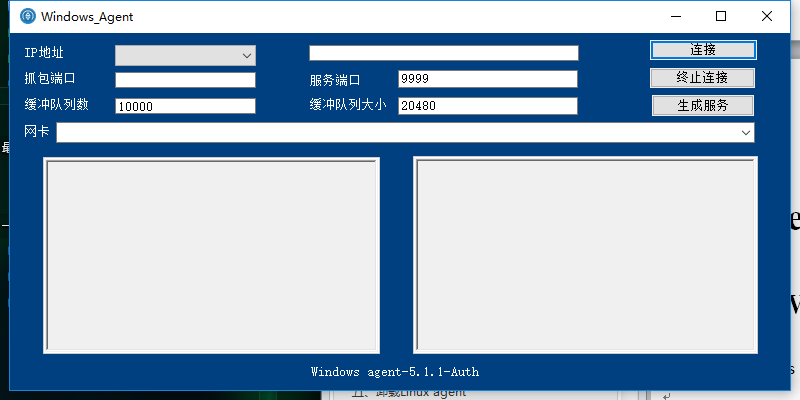
11. 安装成功后，桌面会生成一个Windows agent启动快捷方式



# 四、Agent相关功能操作

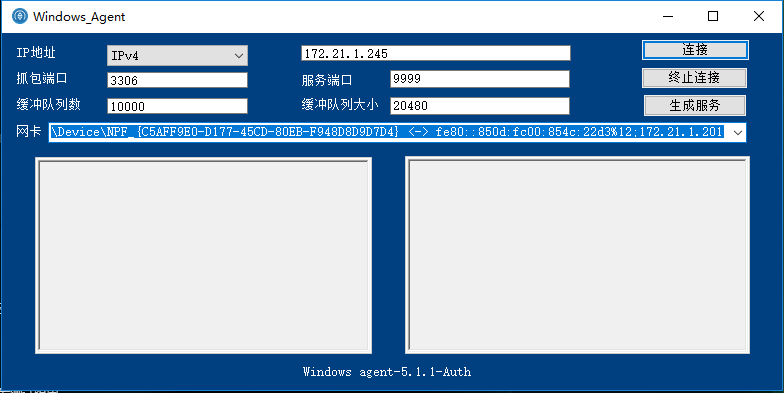
## 4.1 启动Windows agent程序

1. 点击Windows agent程序快捷方式，启动Agent程序。会弹出Agent运行窗口（Agent版本号见窗口下方）



2. 设置相关的参数。参数说明如下：

1. IP地址：填写数审设备的IP地址。如果是IPv4就选择IPv4，如果是IPv6就选择IPv6
2. 抓包端口：抓取指定端口的流量 ，和数据库服务器业务端口保持一致，如果有多个端口，中间用英文逗号进行分隔，例：80,3306,1521
3. 服务端口：默认为9999
4. 缓冲队列数和缓冲队列大小：保持默认即可，如果要修改请联系相关研发人员
5. 网卡：网卡和数据库业务数据网卡保持一致

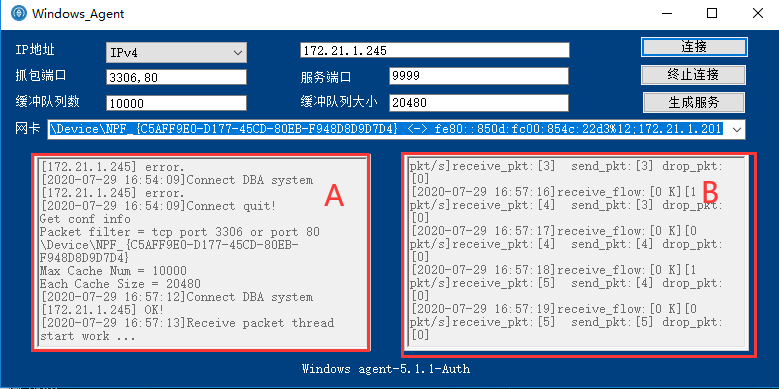


3. 点击【连接】，启动Agent程序

如下图所示，A窗口显示Agent运行状态是成功还是失败，B窗口显示每秒转发的流量日志信息（每秒刷新1次）

1. 如果启动成功，那么A窗口会显示start work，B窗口会有实时流量的转发日志信息
2. 如果启动失败，那么A窗口会报error错误，B窗口也不会有实时流量的转发日志信息

启动成功：

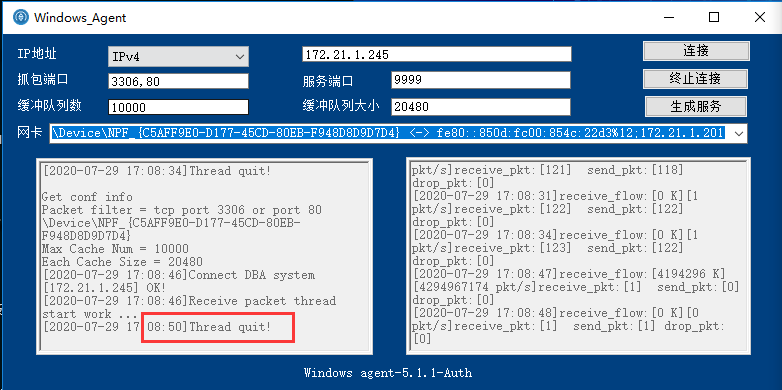


启动失败：



## 4.2 终止Windows agent程序

点击【终止连接】即可终止Windws agent程序的运行，左边窗口会出现Thread quit程序退出的提示

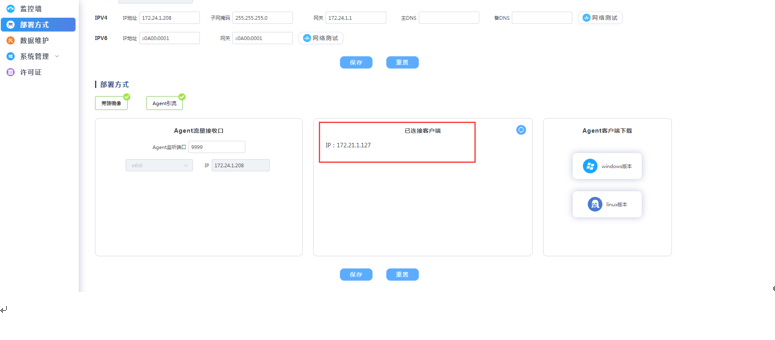


## 4.3 Agent运行状况的确认及检查

1. Agent运行正常时，左边窗口提示start work字样，右边窗口能实时显示每秒转发的流量日志，如下图所示：



2. Agent正常运行中，在数据库审计系统使用sysadmin登录，可以在【部署模式】模块中，查看已连接数据库服务器的客户端IP信息

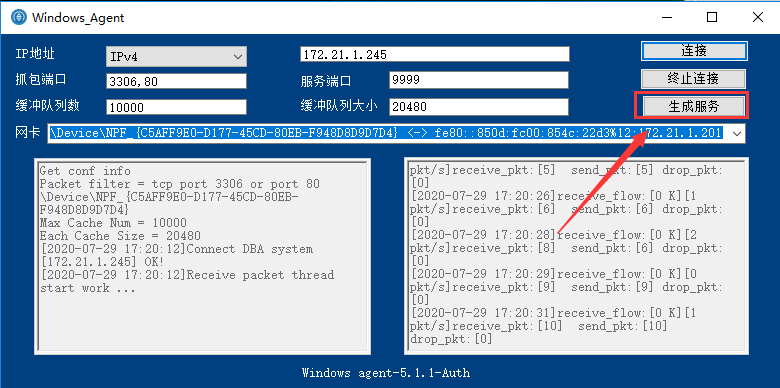


# 五、设置开机启动服务

## 5.1 设置开机启动服务

如果需要数据库服务器每次重启后，audit\_agent都能自动运行，则可以将Agent生成系统服务：

1. 点击【生成服务】按钮



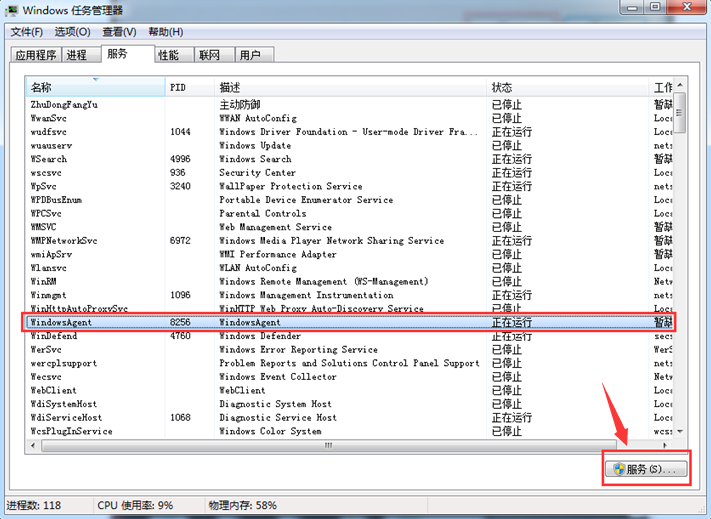
2. 会自动弹出控制台，完成设置操作后，会提示服务启动成功。生成服务过程中，如果中间有弹窗需要获取管理权限，请点击【是】，如果杀毒软件有提示，请点击【同意】



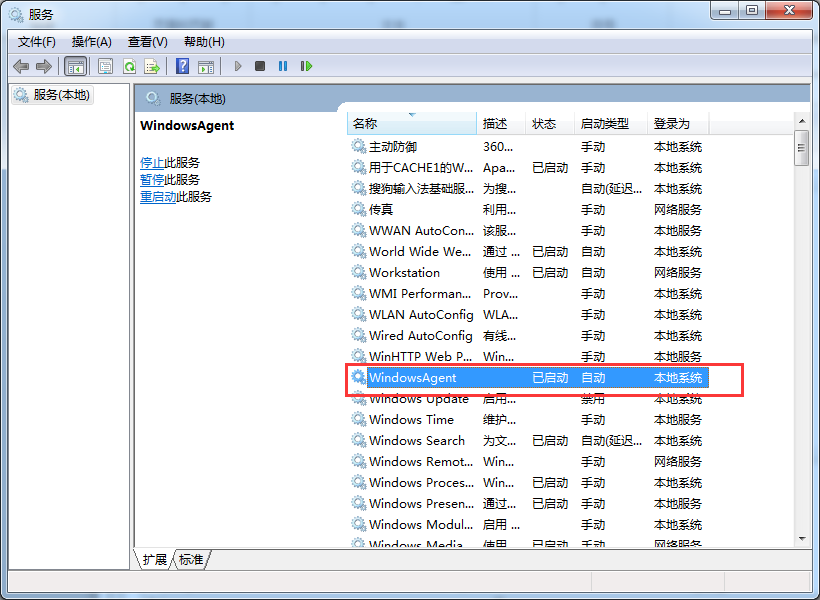
## 5.2 更新Agent服务

如果需要对Agent服务的已设定的配置参数进行变更，那需要对服务进行更新

1. 注意：需要重新配置，需要先停止服务。找到对应服务WindowsAgent右键停止服务，若出现提示错误无法停止说明权限不够，需要点击右下角的管理员权限标志 -【服务】按钮，如下图所示：



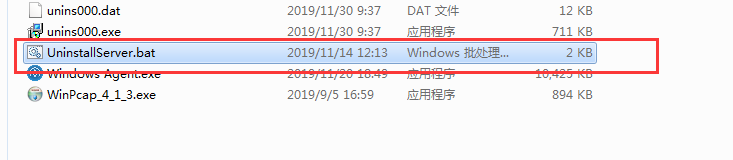
2、用管理员权限来对服务进行停止操作：

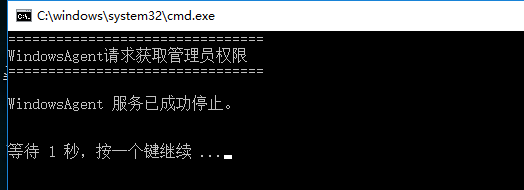


3、停止服务之后，则可以双击桌面快捷方式进行重新参数配置，启动运行Agent后，然后再生成Agent开机启动服务

## 5.3 取消开机启动服务

如果当前服务器不想agent开机启动，则需要把启动服务卸载掉，找到程序安装的位置（右键桌面快捷方式，打开文件所在位置），双击目录下的UninstallServer.bat脚本。其中，可能有其他提示，比如360等防护软件警告信息提示，需同意





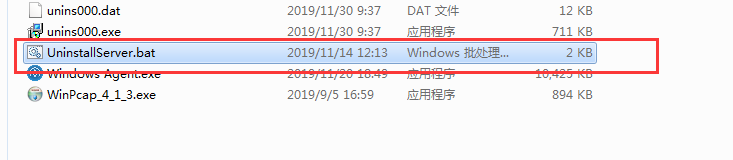
# 六、卸载Windows agent

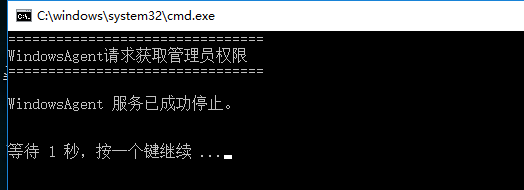
1. 卸载前需要退出Windows agent程序，找到通知栏中，鼠标右击，点击【退出】即可



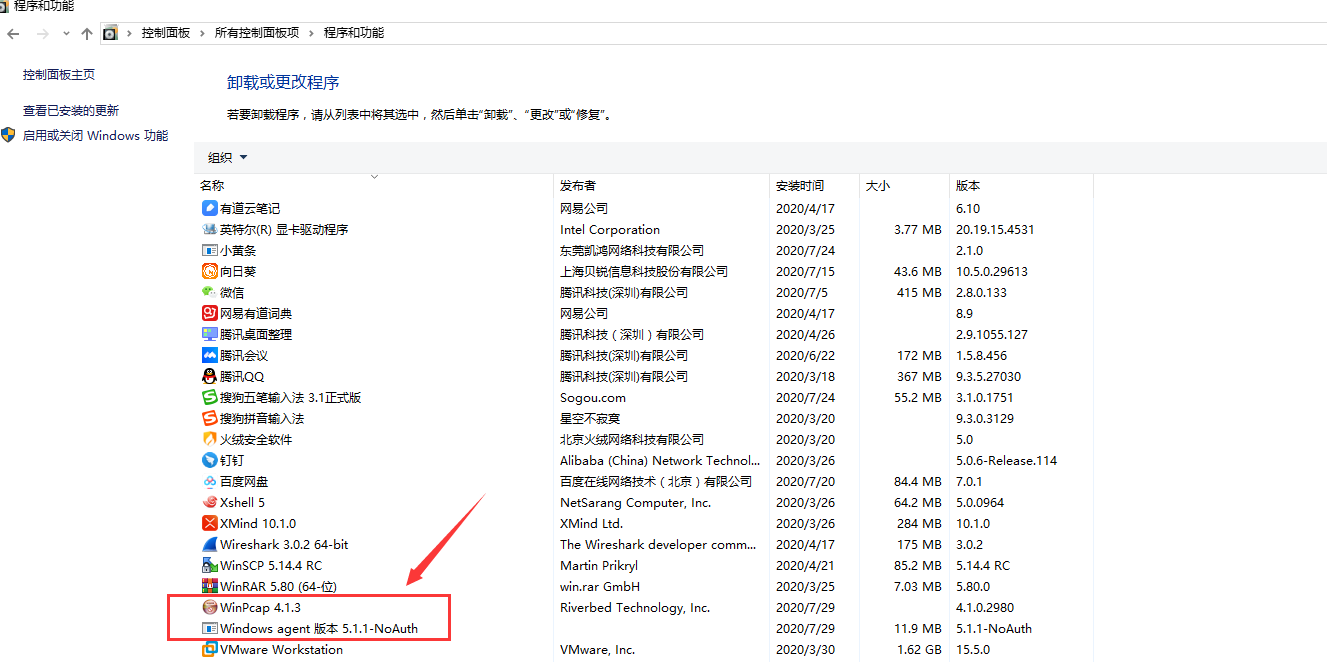
2. 取消开机启动服务（如果未设置开机启动服务，则忽略此步骤）

找到程序安装的位置（右键桌面快捷方式，打开文件所在位置），双击目录下的UninstallServer.bat脚本。其中，可能有其他提示，比如360等防护软件警告信息提示，需同意





3. 进入windows系统的安装或卸载程序，依次卸载WinPcap和Windows agent这两个程序即可。（注：卸载完成时，因系统差异可能会有弹窗询问是否执行重启服务器操作，请特别注意！！！）



# 七、常见问题说明

1. Windows agent是否支持多个Agent与一台数审设备对接？

答：支持

2. Windows agent是否支持一个Agent与多个数审设备对接？

答：不支持。但目前Windows agent程序已放开线程限制，一台服务器可重复开启多个Agent程序，可分别连接不同的数审设备进行流量转发

3. Agent是否会因为网络原因或者服务端异常，导致流量数据一直阻塞？

答：当网络原因或者服务端异常时，接收到的流量数据会逐渐写满设置的缓存空间，当缓存空间无空闲时，Agent会直接丢包处理，以保障Agent和数据库服务器的正常运行

4. Agent启动失败，一直提示error

答：请确认数审端的部署方式是否设置成Agent引流方式，或者参数设置有误

5. Agent启动成功，但是无法转发数据

答：先确认Agent 的网卡和抓包端口是否设置正确，再确认Agent的数审服务端IP以及端口信息是否设置正确

6. 对配置文件进行了修改，但是并没有生效

答：对配置文件进行修改后，需要停止连接后再重连接

7. 如果出现一些Agent启动后连接失败的异常，但却只能选择关闭程序，无法修改参数情况如何处理？

答：可进入Windows agent安装目录，删除agent.cfg文件后，再重新启动Agent程序