F 监控助手

用户手册

2018 年 11 月

目录

一、产品简介

F 监控助手是用于监控并守护 windows 服务器正常运行的专业工具软件。实时显示与服务器通信的每个 IP 地址的流量，统计访问服务器的独立 IP 数、IP 归属地分布，监控程序运行，文件监控和守护，服务器性能，Windows 事件转发等，全方位展示服务器运行状态，让服务器的运行从此变得透明。

如果您的服务器有网站或应用，F 监控助手能让你实时查看哪些 IP 正在访问网站或应用，每个 IP 的流量大小，以及这些 IP 的地理位置信息，更有丰富的统计功能，统计独立 IP 数，IP 地域分布，有效网络流量等。

文件守护功能，能让你在服务器被入侵时，能方便查找上传文件的位置位置，定位被修改、删除的文件，结合 F 监控助手提供的详细 IP 访问记录，能快速定位入侵者 IP 地址。即使入侵者为掩盖痕迹，将这些文件删除或改名，F 监控助手也会记录操作行为，显示哪些文件被创建、修改、删除，这些信息还可以通过 syslog 格式发送到您的集中监控系统中，进行告警。使用 F 监控助手，你可以自行设置监控目录，对这些关键目录进行保护，能自动删除新创建的文件，或使用事先备份的文件自动恢复被篡改的文件。

智能性能指数分析，不再是一条条简单的 cpu/内存的使用曲线，通过内置专业算法，，从 CPU 指数、内存指数、硬盘指数、网络指数等方面对性能数据进行评估。不需要你自己判断，F 监控助手简单直接的告诉你服务器在哪个方面存在瓶颈以及如何应对。

F 监控助手安装简单，即装即用，无需安装数据库等其它软件。图形化界面操作简单易用、信息丰富。零部署成本，零学习成本。

产品特色

- ✓ 基于 IP 的网络流量实时监控，精准定位占用流量的内网和外网 IP 地址；
- ✓ 网站和业务系统访问量实时统计，独立 IP 数统计，按小时、天、月、地理位置；
- ✓ 服务器审计，详细的日志记录 Windows 事件、程序启动/退出，文件变动，网络 IP 地址变动，访问服务器的所有 IP 地址记录；
- ✓ 进程守护，监控进程运行，并自动拉起退出的进程；
- ✓ 文件守护，监控文件创建，修改，自动恢复被篡改的文件，一键查看上传到服务器的新文件；
- ✓ 文件内容监控，将文件内容以 Syslog 格式发送给日志服务器。
- ✓ 实时性能监控，CPU，内存，网卡，进程、网络连接、磁盘 IO，磁盘容量使用情况；
- ✓ 智能性能指数分析，内置专家算法对实时性能数据分析，简单明了显示服务器性能瓶颈，服务器配置是否满足你的网站和应用；
- ✓ Syslog 日志转发，Windows 事件、IP 访问统计数据、性能数据等可通过 Syslog 转发到指定的日志服务器；

- ✓ 采用旁路式检测技术，无干扰，占用资源少，不影响服务器运行；

名词解释

- **PID**：即进程 ID，操作系统用于唯一标识进程的一个数值。
- **接收流量**：指服务器从对方接收到的网络流量，比如上传一个文件到服务器，主要就是接收流量；
- **发送流量**：指服务器发送给对方的网络流量，比如从服务器下载一个文件，主要就是发送流量；
- **访问量（IP 数）**：访问服务器的独立 IP 数量，计算规则：一个小时内，同一个 IP 多次访问算一次；
- **独立 IP 数**：访问服务器的独立 IP 数量，计算规则：一天内，同一个 IP 多次访问算一次。
- **内存页面与硬盘交换**：指操作系统将数据从硬盘读取到内存，或从内存写回到硬盘的每秒字节数。

二、快速入门

2.1、安装

F 监控助手提供图形化安装界面，安装过程十分简单，与普通 windows 软件过程一样，无需输入任何参数。F 监控助手软件占用资源极小，对服务器配置无专门要求，支持的操作系统包括：Windows 2003/2008/2012/2016，中英文版不限。

产品下载请访问官网：http://www.ipneed.com

2.2、主界面介绍

F 监控助手运行后，主界面如下图所示：

标题栏右边是设置菜单，点击“设置”为弹出主菜单，如下图：

菜单项说明：

“打开 F 监控助手”：用于在悬浮窗状态下打开主界面。

“显示悬浮窗”：控制最小化时，是否在桌面显示悬浮窗。

“悬浮窗类型”：选择悬浮窗样式。

“字体”：选择主界面的字体。

“设置”：弹出设置窗口，详细的设置说明，请见“系统设置”章节。

“清空文件/进程日志”：删除文件/进程的历史日志记录。

“导出文件/进程日志”：将所有的“文件/进程日志”记录导出成 txt 文件，便于您永久保存，F 监控助手只保留 50 万条日志，超过这个数量会自动清空。

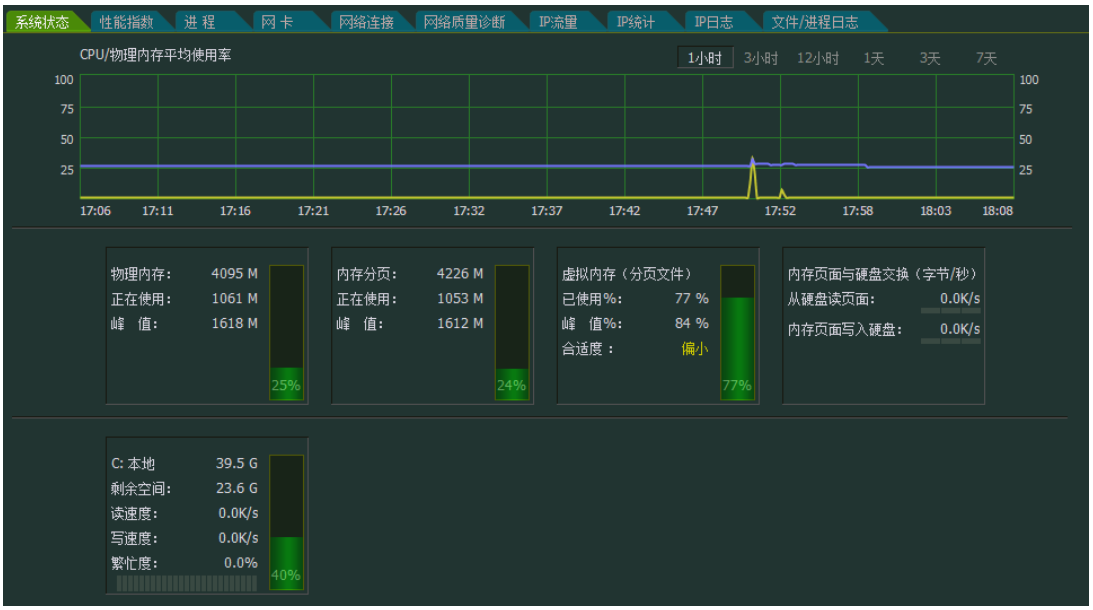
“产品注册”：用于订阅 F 监控助手，使用期到后，点击这里，进行订阅或续订。

“开机自动运行”：服务器启动后，是否自动运行 F 监控助手。

“退出”：退出 F 监控助手。

三、功能说明

3.1、系统状态



系统状态显示服务主要的性能信息。

1、CPU/物理内存利用率的实时和历史趋势图。

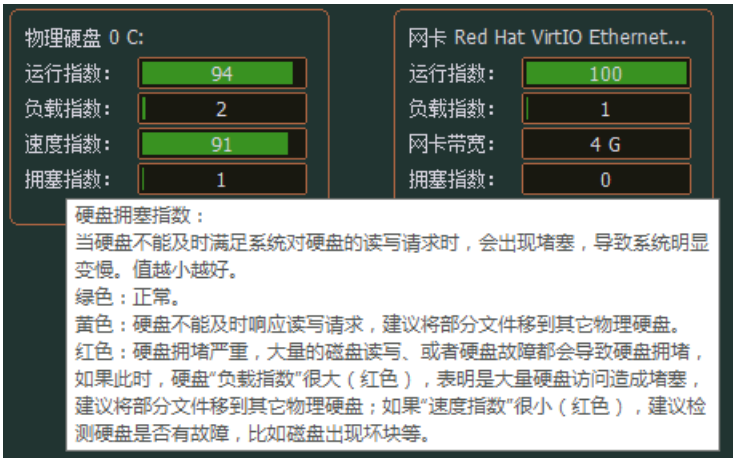
2、当前内存的配置和使用情况。虚拟内存是指用硬盘空间作为内存的大小，F 监控助手会根据使用情况自动判断分页文件的设置是否合理，即合适度。

3、硬盘信息，每个硬盘分区一个图形，分别显示每个分区的总容量，剩余空间，空间使用比例，硬盘当前的读写速率（字节/秒），以及硬盘的繁忙程度，如果硬盘繁忙度过高，标记块会变黄色或红色。

3.2、性能指数

性能指数从 CPU、内存、硬盘、网卡 4 个方面衡量服务器的性能是否满足网站/应用系统的要求，当出现红色块时，说明该项是性能瓶颈。如下图中，物理硬盘 0（上面有 3 个分区，即 C、D、E 盘）的负载指数成红色，说明该物理硬盘读写频繁，而且导致硬盘发生堵塞（如图中拥塞指数为黄色），影响服务器性能，应将部分文件迁移到其它物理硬盘，来转移硬盘的读写负载。

界面已内置了对指数的说明，鼠标移至指数名称上，即会弹出提示框，如下图，鼠标移到“拥塞指数”时，弹出拥塞指数的说明。



重要说明：性能指数的检测，是采集服务器正常业务访问的数据，不会通过额外加压增加服务器负载，不会对服务器造成影响。

3.3、进程

进程信息，显示服务器上目前正在运行的程序，以及这些程序占用资源情况，在表格中点击鼠标右键，会弹出菜单，如下图所示：

操作说明：

定位文件位置：会打开 windows 的文件管理器，跳转至该文件所在地目录，定位该文件的位置。

复制文件路径：将文件完整的路径名称（包括目录）copy 到剪切板中。

查看网络连接：如果该程序有网络连接，点击后会跳转至“网络连接”界面，显示该进程目前所有的网络连接。另外，点击“网络连接数”列中的数字，也会跳转。

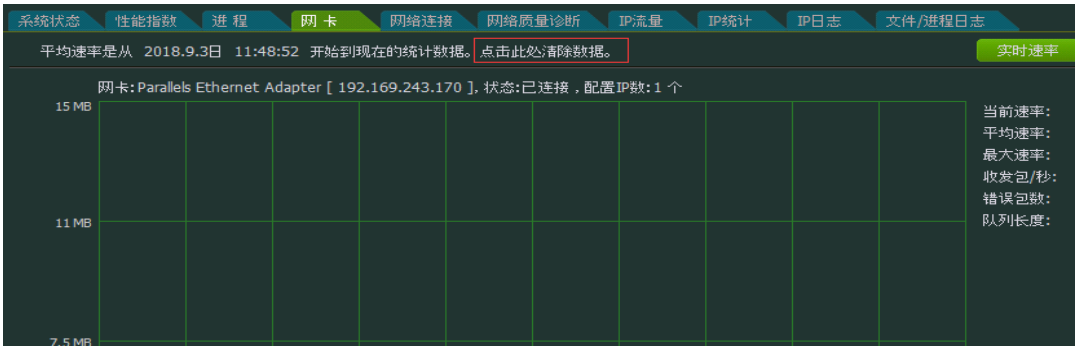
查看进程启动日志：查看该程序的启动历史记录，跳转至“文件/进程日志”界面，显示该程序启动/退出的所有记录。

结束进程：强制关闭进程，与 windows 任务管理器的功能一样，会弹出确认框，确认后才会执行关闭操作。

表格排序：点击表格字段名，可以按该字段进行排序（灰色字段—文件位置，不支持排序操作）。

3.4、网卡

显示服务器每块网卡实时网络流量以及每 5 分钟的平均网络流量，鼠标移至如下图红框处的位置，并单击鼠标左键，则重新开始显示（当前曲线会清除）。



界面说明：

图形上方为网卡名称，网卡配置的主 IP 地址，网卡是否在使用（状态=已连接，表示正在使用），以及该网卡配置的 IP 数量。

当前速率：该网卡每秒发送字节与接收接收之和。

平均速率：IP 雷达启动后，检测到的平均速率，如果网卡曾中断（掉线，变更主 IP 地址等）则自动重新计算平均速率。

最大速率：指从检测开始时间起，网卡流量的最大值。

收发包/秒：指网卡每秒发送和接收到的数据包数量。

错误包数：指网卡在发送和接收数据包时，检测到的错误的数据包数量。

队列长度：指网卡队列中等待发送的数据包数量，一般应该为 0，如果>0，则说明网络流量太大。

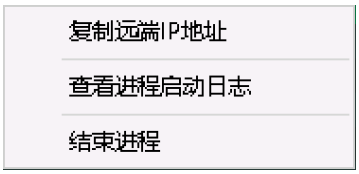
3.5、网络连接

网络连接显示服务器当前的网络连接情况，信息如下图所示：

操作说明：

点击“**刷新**”按钮，刷新表格数据，获取当前所有的网络连接并更新表格数据。

右键菜单，在表格的任意一行点击鼠标右键，可以弹出右键菜单，对所选中的行进行操作，如下图所示：



复制远端 IP 地址：将远端 IP 地址复制到剪切板。

查看进程启动日志：查看该程序的启动历史记录，跳转至“文件/进程日志”界面，显示该程序启动/退出的所有记录。

结束进程：强制关闭进程，与 windows 任务管理器的功能一样，会弹出确认框，确认后才会执行关闭操作。

表格排序：点击表格字段名，可以按该字段进行排序（灰色字段—远端 IP 位置，不支持排序操作）。

3.6、网络质量诊断

网络质量诊断用于检测服务器与对方 IP 的网络通信质量，最重要的指标是“TCP 重传”和“TCP 重连”，当检测到这 2 种连接，会用明显的颜色进行标记。偶尔出现这类连接，属正常情况，网络没有问题。当出现大量的 TCP 重传和 TCP 重连，参考下面 3 条进行判断：

1、*当服务器与某个 IP 有大量的这 2 种类型的连接，这时该用户访问你的网站会明显变慢。*

2、*有很多 IP 都出现这 2 种连接，说明服务器的网络连接不稳定（可能的原因：网站被攻击或服务商网络质量不好）。*

3、*只是某几个 IP 出现大量这种连接，则可能是对方的网络问题。*

网络质量诊断界面如下图：

左侧窗口：显示当前服务器所有 TCP 连接活动；连接标记说明：

“<==”：表示对方主动连接你的服务器，通常，当对方访问你的网站或应用时，对方会主动连接你的服务器。

“==>”：表示服务器主动连接对方。

“-x-”：表示服务器与对方断开连接。

右侧窗口：为监视窗口，用于显示某个特定 IP、端口或进程的 TCP 活动，可以在右键菜单中选择要监视的连接类型。

下侧窗口：显示最近 24 小时 TCP 活动的统计图，每个小时的网络连接、断开、重传的次数。以及网络连接的错误率，如果某个时段网络连接的错误率>50%，说明在那个时段，服务器的网络连接很不稳定。统计图默认不显示，点击如下图的位置，可以打开和刷新统计图。

弹出菜单：在 TCP 活动窗口单击鼠标右键，可以弹出菜单，进行停止监测、导出结果等操作。并可以将指定的监测目标单独放在在监视窗口进行显示。

说明：

- ✧ *对 Windows server2003 系统，连接类型只有 3 种：TCP 重传、连接断开、TCP 重连。*
- ✧ *网络质量诊断采用旁路式检测技术，不会对服务器造成额外压力，可以不限时间的持续监测。*

3.7、IP 流量

IP 流量功能，显示所有访问服务器的 IP 的流量。有 2 个按钮分别显示实时流量和最近 IP 访问记录。实时流量界面如下图所示：

“当前 IP 流量”窗口分为上下 2 部分，通过**“收缩/展开”**按钮可以控制是否显示下方的窗口。

操作说明：

右键弹出菜单：上下 2 个窗口，均支持右键弹出菜单。

只显示某个进程的 IP 流量：在上方窗口双击要显示的进程，恢复显示全部，则点击刚才选中的行，即可取消选中，显示所有进程的 IP 流量。

发送字节/秒：指服务器每秒发送给对方的网络流量（字节数）。

接收字节/秒：指服务器每秒从对方接收的网络流量（字节数）。

总数/秒：指服务器每秒与对方传输的网络流量，即：发送字节/秒 +接收字节/秒。

当前访问 IP 数：指与进程正在通信的 IP 数量。

表格排序：上下 2 个表格均支持排序，鼠标左键点击表格字段即可以排序（*注：灰色字段不支持排序*）。

最近 IP 访问记录窗口

显示最近访问过服务器的所有 IP 的详细记录（*最大 1 万条，要查看全部 IP，请在“IP 日志”页签中查看*）。

访问次数：该 IP 最近访问服务器的次数，计算规则：每小时计数一次，一个小时内多次访问只算一次。即 1 天最多计数 24 次。

最后访问时间：该 IP 最后一次访问服务器的时间。

操作说明：

显示 PID 的进程名称：鼠标移至 PID（进程 ID）列所在的行，鼠标停留 2 秒左右，会弹出提示框，显示该 PID 对应的进程名称。如下图，鼠标移至 952 上，显示 PID=952 对应的进程名称为 svchost.exe。

导出表格数据：在表格中点击鼠标右键，可以弹出菜单，选中“导出表格数据”。

如何在表格中搜索：

最近 IP 访问记录，默认最近访问过服务器所有 IP 的详细记录（最大 1 万条），可以通过搜索框过滤，搜索符合条件的记录。鼠标移至“搜索端口号/PID”位置，并停留 2 秒左右，会弹出搜索提示，如下图所示：

搜索条件说明：

按进程 ID 进行搜索：数字+P，如搜索 PID 为 952 的记录，则输入 952P，然后点击“搜索”按钮。

按远程端口号搜索：端口号+R。如　80R，即搜索对方端口是 80 的 IP 记录。

按本机端口号搜索：端口号+L。搜索最近哪些 IP 访问了本服务器的 443 端口，可以输入： 443L

搜索远端 IP：数字+点符号。如 83. 表示搜索所有 83.*.*.* 的 IP 地址，输入 83.101，则表示搜索 83.101. *.* 的 IP 地址。

如果输入框中只输入数字，则显示 PID 或远端端口或本机端口等于该数字的记录。如输入 80，则 PID=80 或者 远端端口=80 或者 本机端口=80 的记录都会显示。

显示全部：忽略搜索条件，显示全部记录。

数据刷新：最近 IP 访问记录不自动刷新表格数据，请点击“最近 IP 访问记录”按钮刷新。

3.8、IP 统计

统计单位定义：

接收流量：指服务器从对方接收到的网络流量，比如上传一个文件到服务器，主要就是接收流量；

发送流量：指服务器发送给对方的网络流量，比如从服务器下载一个文件，主要就是发送流量；

访问量（IP 数）：访问服务器的独立 IP 数量，计算规则：一个小时内，同一个 IP 多次访问算一次；

独立 IP 数：每天访问服务器的独立 IP 数量，计算规则：一天内，同一个 IP 多次访问算一次。

统计类型：

今天：当天 00:00-23:59 分，每小时访问服务器的独立 IP 地址数量，网络流量。

最近 24 小时：最近 24 小时，每小时访问服务器的独立 IP 地址数量，网络流量。

本月：当月 1 号至当天，每天访问服务器的独立 IP 地址数量，网络流量。

最近 30 天：最近 30 天，每天访问服务器的独立 IP 地址数量，网络流量。

今年：当年，每月访问服务器的独立 IP 地址数量，网络流量。

最近 12 个月：最近 12 个月，每月访问服务器的独立 IP 地址数量，网络流量。

周总结：从监控之日起，周一至周日访问服务器的独立 IP 地址数量，网络流量。

今天 IP 地区分布：当天访问服务器的地域排名，按 IP 数量排名，国内按省，国外按国家。（*注：需要勾选“自动保存 IP 日志”，参见“设置”章节*）。

今天 IP 流量分布：当天访问服务器的地域排名，按网络流量排名，国内按省，国外按国家。（*注：需要勾选“自动保存 IP 日志”，参见“设置”章节*）。

自定义查询：选择统计类型、开始日期、时间跨度进行统计。跨度选择框，可以输入数字，如选择了天统计，则跨度，可以选择整月，也可以直接输入 1-31 的数字，输入 5 表示，只统计 5 天的。如下图：

操作说明：

导出：自定义查询的统计结果可以导出，点击“**确定**”按钮查询结果后，再点击“**导出**”按钮将当前统计结果导出为 csv 文件。

重要提示：系统安装后，默认统计所有与服务器进行通信的 IP 地址的流量，如果只要统计特定的流量（比如只统计网站的访问流量和 IP 数），请在“设置”中，勾选 “启用流量过滤”，并设置端口号。详细参见“设置”章节。

3.9、IP 日志

F 监控助手将所有访问服务器的 IP 保存到日志中，通过 IP 日志功能进行查询和搜索。

发送字节：一小时内的发送到对方 IP 的流量之和。

接收字节：一个小时内服务器从对方 IP 接收到流量之和。

最后访问时间：一个小时内，该 IP 最后一次的访问时间。

举例:61.151..*这个 IP 地址在 18 点—19 点和 22 点至 23 点多次访问服务器，在当天的 IP 日志记录中，会有 2 条记录，分别记录在这 2 个时段发送和接收到总字节数，以及在这 2 个时段最后一次的访问时间。*

操作说明：

查询：选择要查询的日期，点击“打开”按钮，即可以打开所选日期的 IP 日志记录。点击“导出”按钮，可以将查询结果导出为 txt 文件。

搜索 IP：在搜索框中，输入完整 IP，可以搜索该 IP 地址，最近 30 天的访问记录。

提示：只支持查看最近 1 年的 IP 日志。

3.10、文件/进程日志

F 监控助手对服务器上发生的重要行为，如程序启动/退出，文件创建/删除/改名/写文件行为，Windows 事件，网卡主 IP 变动，网卡掉线，守护文件的行为（恢复的文件，自动删除的新建文件），守护进程的行为（自动拉起退出的程序）生成操作日志，用于查询和审计。

日志字段说明：

进程日志中，“**启动[1208]**”方括号内的数字为该进程启动时的进程 ID；“**退出[1208]**” 方括号内的数字为该进程退出时的对应的进程 ID；方便分区多个同名文件的启动和退出。

文件日志中，“**改名_原名**”，指文件改名操作，为该文件名称被修改前的文件名（原文件名）。**改名_新名**”是该文件名称被修改后的新的文件名称。

操作说明：

导出：在表格中的数据行（非空白行），单击鼠标右键，弹出菜单，选择“导出表格数据”，导出表格数据为 txt 文件。

定位文件位置：鼠标右键弹出菜单，选择“定位文件位置”，可以打开文件浏览器，定位到文件所在位置。

新文件：在菜单中选择“新文件”选项，显示最近新增加的文件记录。（在最近 5 万条记录中搜索，如果记录数量太多，请使用 fn>命令进行搜索。）

搜索：在搜索框中输入关键字或搜索命令查找日志，搜索命令如下：

> 关键字；> login"，日志中含“login”的日志。

p> 搜索进程日志；ps> 、pq> 、psq> 、pid>

ps> 搜索所有进程的启动记录；

pq> 搜索所有进程的退出记录；

psq>搜索所有进程的启动/退出记录；

pid> 按进程 ID 搜索，如 pid>468 搜索进程 id 为 458 的启动/退出记录；

f> 搜索文件日志；fc>,fn>,fd>,fcd>,fw>,fr>,frn>,fro>

fc> 搜索文件的创建记录；如 fc> .exe 搜索所有曾经创建过多 exe 文件。

fd> 搜索删除文件的记录；

fcd> 搜索创建/删除文件的记录；

fw> 搜索写文件的记录；

fr> 搜索改文件名称的记录；

frn> 搜索改文件名后，新文件名的记录，如 frn> setup.exe 搜索文件名被改为 setup.exe 的记录。

fro> 搜索改文件名后，原文件名的记录，如 fro> .png 搜索那些 png 文件的名称名被修改了。

fn> 搜索新增加的文件，即新建后没有被删除的文件。如 *fn<2> 表示搜索最近 2 天新增的所有文件。*

****>*** 带*号操作的日志。*,*>,p*>,ps*>,f*>,fc*>,fd*>

*对于守护行为，包括文件守护和进程守护，日志中会包含*号。这个命令搜索所有守护行为。*

p>和 ps*> 程序退出后，被 F 监控助手自动拉起的程序启动记录。*

f> 搜索文件被 F 监控助手恢复，自动删除的记录。*

fc> 搜索文件被 F 监控助手恢复的记录。*

fd> 搜索文件被 F 监控助手自动删除的记录。*

w> 搜索 windows 事件。

s> 搜索网卡主 IP 变动日志和网卡掉线记录。

| 反向搜索；可以与上述搜索命令联合使用。fc> |.asp 搜索新建的所有非 asp 文件。

<x> 指定搜索的时间段，搜最近 x 天的日志。<1>当天的日志。可以与上述搜索命令联合使用。

x 后跟 d,h,m，可指定天<xd>,小时<xh>,分钟<xm>。

如：**p<3-5>** 搜索 3 天前，且 5 天内的所有进程日志。

p<2h> 搜索最近 2 小时的所有进程日志。

P<30m> 搜索最近 30 分钟内的所有进程日志。

搜索示例：

fn> .jpg 在最近 5 万条记录中搜索新建的 jpg 文件的记录，而且该文件没有被删除。
fn<1-3d> .jpg 搜索 1 天前，且 3 天内的新增 jpg 文件。
fn<72h> .jpg 搜索最近 72 小时内，新建 jpg 文件，而且该文件没有被删除。
fc<72h> .jpg 搜索最近 72 小时曾经创建的 jpg 文件的记录，不管该文件是否被删除。

四、系统设置

在主菜单中，选择“设置”选项弹出设置主界面，在设置界面中，在设置界面中，可以进行如下设置：

- ✓ 启用/关闭IP流量监控。
- ✓ 启用/关闭文件监控。
- ✓ 启用/关闭进程监控。
- ✓ 启用/关闭发送syslog日志。
- ✓ 启用/关闭Windows 事件监控。

*重要提示：设置项修改后，必须点击“**确定**”按钮才会生效。*

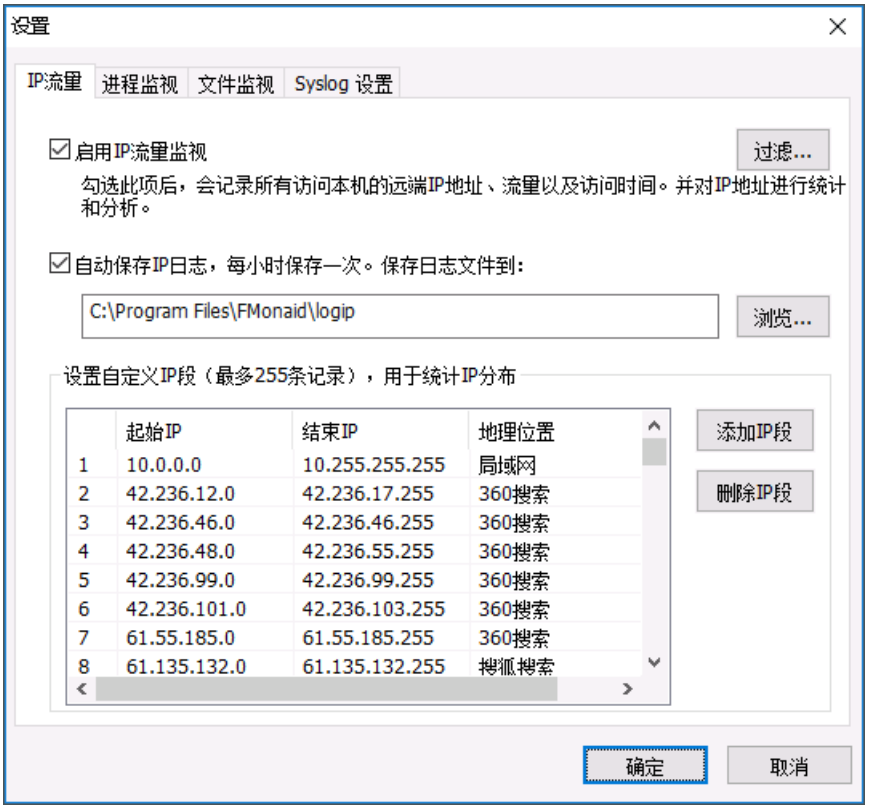
4.1、设置 IP 流量监视

IP流量用于监视与服务器通信的所有IP地址的流量，你可以在这里设置启用和关闭IP流量监视功能。流量监视功能关闭后，停止显示每个IP地址的流量，IP统计，但不影响网卡流量的显示。即关闭IP流量监视后，只能显示服务器总的网络流量，不再对每个IP的流量进行监视。

在这个设置界面中，你可以：

- ✓ 启用和关闭IP流量监视功能。
- ✓ 设置IP统计过滤规则。
- ✓ 修改保存IP日志的默认目录。
- ✓ 自定义IP地址段的地理位置。

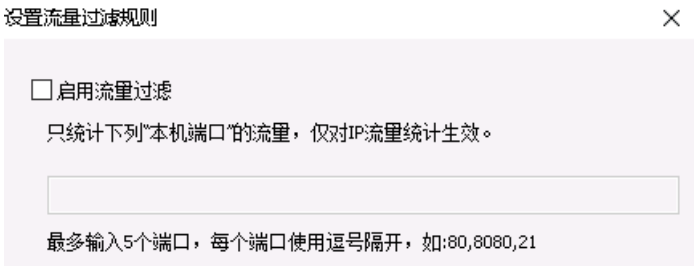
设置界面如下图所示：



设置说明：

启用IP流量监视：勾选表示启用IP流量功能，IP流量，IP日志，IP统计才会有数据，默认勾选。如果不需要监视IP流量，取消勾选，并点击“确定”按钮。

过滤：按指定的端口号（本机）统计IP流量和IP数量，勾选表示启用。不勾选则统计全部，默认不勾选。*举例：只统计网站的流量和IP数，请勾选“启用流量过滤”，并在下方编辑框中输入网站的端口号，一般是80（http）或443（https）。*



*重要提示：启用流量过滤，并不会影响IP实时流量和IP日志，仅对IP统计功能有效。即：**IP日志**和**IP流量**功能总是会记录所有与服务器通信的IP流量（除非关闭IP流量监视）。*

保存IP日志：如果需要永久保存访问服务器的所有IP记录，请勾选此功能。IP日志每天生成一个新文件，并每小时更新一次，所以IP日志中最新的数据是上一个小时的IP记录。已生产的IP日志文件永久保存，不会自动删除，如需清理历史IP记

录，请使用文件管理器，在保存日志的目录中，删除对应日期的文件即可。*（备注：如果取消了IP流量监视，这期间不会生成IP日志文件）*

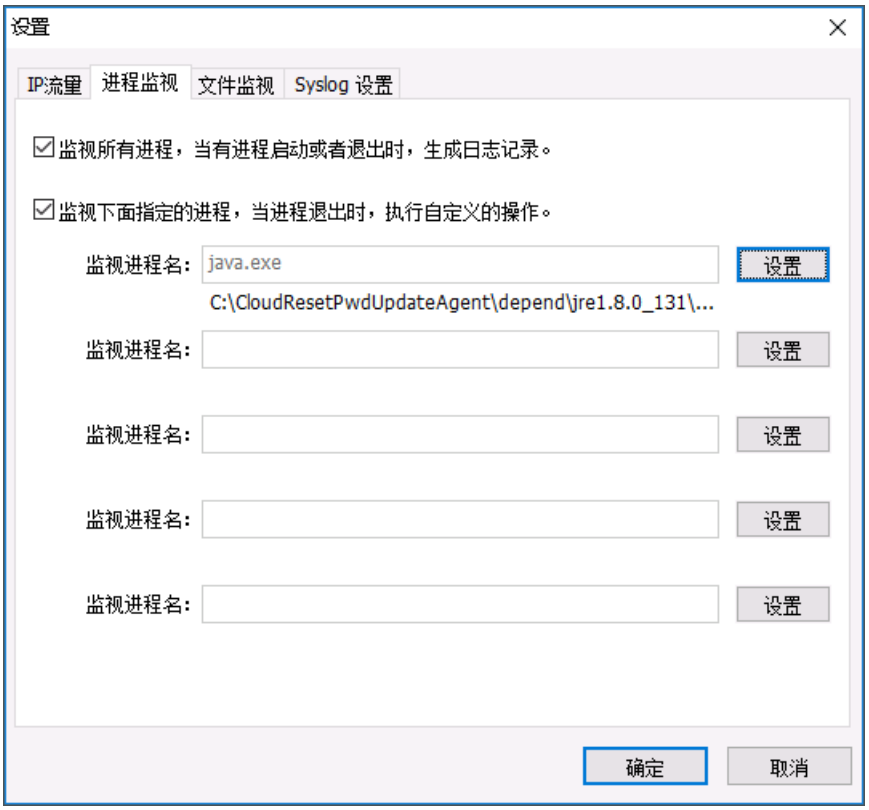
自定义IP段：自定义IP地址的用途，在显示IP地址位置时，将优先使用这里的定义。

4.2、设置进程监视

进程监视用于监视服务器上程序的运行和退出情况，在这个设置界面，你可以：

- ✓ 启用和关闭进程监视功能。
- ✓ 设置需要监视的程序。
- ✓ 检测到程序退出后，是否自动重新运行退出的程序。
- ✓ 检测到程序退出后，是否执行你指定的程序。

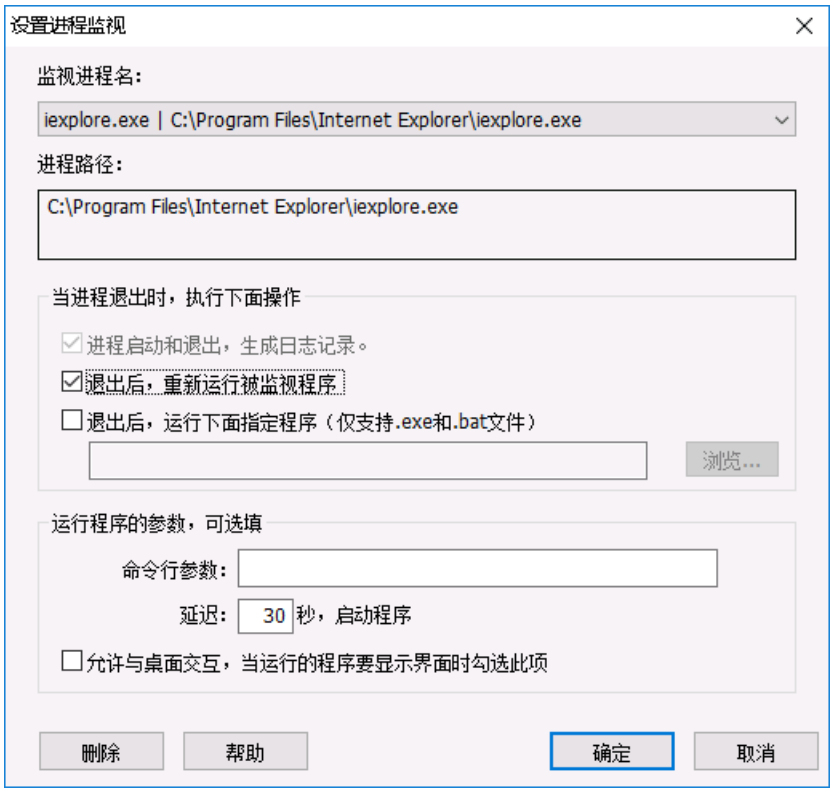
设置界面如下图所示：



监视所有进程：当勾选此项后，表示启用进程监控。每当有程序启动或退出，会生成日志记录，在“文件/进程日志”页签中可以查看，否则，不会生成日志记录。（*注：勾选此项，并没有进程守护功能，即不能自动运行退出的进程。如果你想守护进程，需设置监视指定进程。*）

监视指定进程：监控指定的进程具备进程守护功能，即当进程退出后，自动运行该程序。最多同时守护5个不同的进程（按进程名区分），取消勾选，则暂停指定进程的监视，守护功

能也暂停。点击“**设置**”按钮，弹出详细设置界面，如下图：（*守护多个同名进程，请慎用，参见下方“重要说明”。*）



操作步骤：

1、 在下拉框中选择需要守护的进程（*注：该进程必须已经在运行*）。
2、 选择被守护的进程退出后，需要执行的操作，三种操作，第1个生成日志记录必须选项，不能取消。执行守护进程本身和执行其它程序，选择其中一种，不能同时选择。
3、 设置运行程序所需的参数，如果有的话，没有则留空。
4、 设置启动延迟时间，即检测到守护进程退出后，延迟多次时间再启动程序。
5、 允许与桌面操作，只有当运行的程序要显示图形界面时，才勾选此项。比如上图中，设置守护的进程是ie浏览器，浏览器是有图形界面的，就需要勾选“允许与桌面交互”，如果不勾选，程序启动后，将看不到图形界面。即在任务管理器中能看到该进程，但没有界面显示。

“**删除**”按钮表示删除该进程的监视和守护。

“**帮助**”按钮，在设置过程中，可以点击该按钮查看帮助信息。

重要说明：

1、 程序的识别是按程序的完整路径作为关键字符串，如果守护的程序同时有多个在运行，请慎重使用守护功能，比如Java程序（其程序名都是java.exe）。但如果只是监视功能，则可以放心使用。

2、 被守护的程序自动拉起后，有5分钟的窗口期，即5分钟内程序又退出，则不再重新拉起。

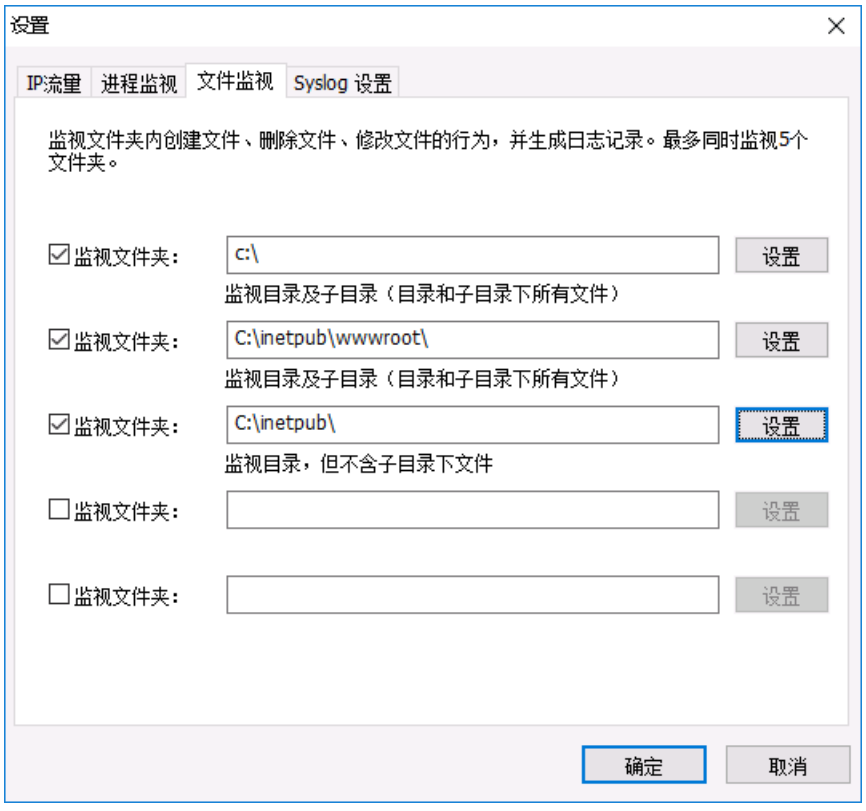
应用示例：进程退出后，一般在什么情况下使用“运行指定程序”的操作选项，比如当被守护的进程退出后，你并不想自动运行它，而是想发送一封email给你，你可以选择执行一个有邮件发送功能的批处理程序（推荐一个windows发邮件的命令行小工具：blat）。这样，F监控助手检测到被守护的程序退出后，会执行你事先指定的这个程序来发送邮件。

4.3、设置文件监视

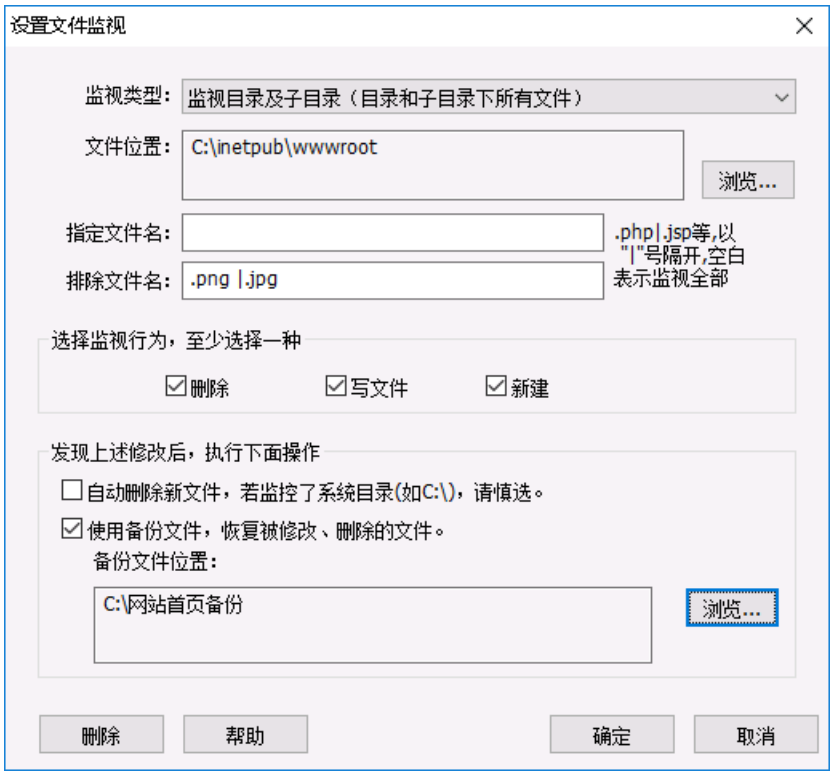
文件监视用于监视指定文件夹下文件的创建、删除、写文件行为，最多同时监控5个不同的文件夹。在这个设置界面中，你可以：

- ✓ 启用和关闭文件监视。
- ✓ 设置要监视的文件目录。
- ✓ 设置是否自动删除新增加的文件。
- ✓ 设置是否恢复被修改的文件。

设置界面如下图所示：



在上图中，勾选表示启用该文件目录的监视，取消勾选，则暂停该文件夹的监视。点击“**设置**”按钮，进行详细的设置，如下图：



操作步骤：

1、 先选择监视类型，有2个选项，2者区别在于是否监视子目录下的文件。

2、 如果只想监视某种类型的文件，在指定文件名中输入关键字，如只监控exe文件的创建，可以输入.exe;如果某种类型的文件，不想监视，则在排除文件名中输入关键字，比如你不关心图片文件的创建，可以输入所有图片文件的后缀，如:.jpg|.png|.gif|.jpeg。如果你排除这些文件，F监控助手不会记录和守护这些文件。*详细请见下方“文件过滤”描述。*

3、 设置监视行为，勾选“删除”表示监视文件的删除行为。当被监视的目录中有文件被删除时，被删除文件的完整路径会记录到日志，你可以在“**文件/进程日志**”中看到该日志。如果不勾选，则该行为不会做记录。三种行为至少选择一个。*详细请见下方“监视行为”描述。*

4、 保护文件，选择执行的操作，（*如果不需要保护文件，跳过这一步，不要勾选*）。

- ✧ 自动删除新文件：勾选后，当检测到新文件被上传或拷贝，则自动删除这些新文件。
- ✧ 使用备份文件恢复：勾选后，使用备份文件恢复被修改的文件。点击“**浏览**”按钮设置备份文件所在目录。恢复操作必须勾选“删除”或“写文件”行为之一，否则无效。

详细请见下方“执行操作”描述，并仔细阅读下方“警告”段落。

5、 点击“确定”按钮，返回配置主界面，并点击主界面的“确定”按钮后，才能最终生效。

“**删除**”按钮，取消该文件夹的监视。

“**帮助**”按钮，打开设置帮助文档。

文件过滤：

用于过滤受监视目录下的文件，如果想指定或排除目录下的某些文件，可以在“指定文件名”和“排除文件名”项中填写字符串。字符串不区分大小写。

两项都为空白，表示监视所有文件，多个文件名用“|”符号隔开，最多个分隔符，且字符串总长度不超过个字符。

1、指定文件名：设置需要监控的文件名，文件路径（目录名和文件名）中包含指定字符串的文件会被监视，否则会忽略。空白表示监视受控目录下所有文件。

示例：（假设受监控文件夹为upload，在“指定文件名”编辑框中输入以下字符串）
data　文件路径包含data字符串的文件。
.jsp　文件路径包含.jsp字符串的文件。
\pic\　*pic 目录下的所有文件。*
*上述条件可以组合输入，如.*jsp|\pic\ *表示监视upload目录下所有文件路径包含.jsp的文件以及*upload\pic*目录下的所有文件。*

2、排除文件名：设置需要排除的文件名，当文件名中包含了排除字符串，该文件将被忽略，不会被监控。“排除文件名”优先级高于“指定文件名”。

以“.”开头的字符串表示文件扩展名（只检查文件扩展名。）；以\开头的字符串表示目录名。

示例：（在“排除文件名”编辑框中输入以下字符串）
.jpg　文件扩展名等于jpg的文件被排除，不受监控。
tmp　文件名（不含目录名）中包含tmp字符串的文件将被忽略。
\tmp　*文件名（含目录名）中包含tmp字符串的文件将被忽略;*
\tmp\　*tmp目录下的所有文件将被忽略;*
*上述条件可以组合输入，如.*jpg|\tmp\|tmp|

监视行为:

删除：监控对目标文件的删除操作，包括重命名文件。

写文件：监控对目标文件内容的修改操作。

新建：监控在目标目录下新建文件的操作。对目标文件进行重命名的操作，也被视为新建文件。

执行操作:

当符合条件的受监控文件，发生了被勾选的监视行为后，《F监控助手》自动执行的操作。

自动删除新建文件：当勾选此项后，受监控的目录中出现的任何新文件，包括文件重命名，都会被删除。该项操作只有在监控了目录的情况下才可选。对监控了整个盘符的(即监控C:、D:等），不建议勾选此项。请仔细阅读下方“警告”段落。

使用备份文件，恢复被修改、删除的同名文件：勾选此项后，受监控的文件被修改或删除，《F监控助手》会使用备份目录中的同名文件进行恢复。备份目录按同名路径查找文件，例如：受监控目录为C:\web\jpg，备份目录为D:\jpgbak，当受控目录下的文件C:\web\jpg\A\AA\c.jpg被删除后，将使用D:\jpgbak\A\AA\c.jpg来恢复，而不是D:\jpgbak\c.jpg文件来恢复。请仔细阅读下方“警告”段落。

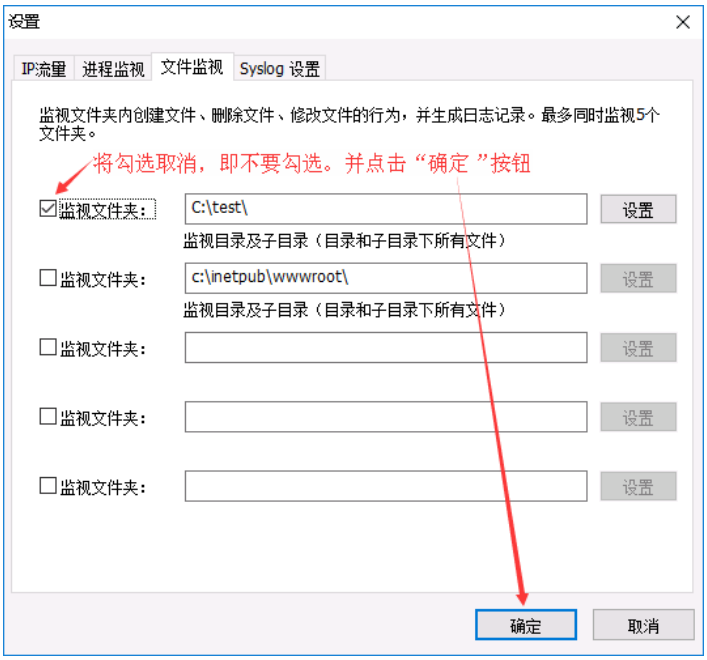
应用示例：*要实现网站上的某个目录只允许上传图片文件。操作如下：*

在监视类型中选择“监控目录及子目录”类型，然后选择要监控的目录名，在“指定文件名”中不输入任何字符，在“排除文件名”中输入 .jpg|.png|.bmp|.gif 等常用图片文件类型名，并在监视行为勾选“新建”，在执行操作中勾选“自动删除新建文件”。点击确定后生效，以后除了指定类型的图片文件，其它类型文件均会被自动删除。

警告：

文件监控的自动删除和恢复功能，并不区分文件是谁创建和修改的，只要满足设置的条件就会执行。即便是你自己拷贝文件到受保护目录或修改受保护目录中的文件，也会被自动删除或使用备份文件恢复。

如果你勾选了自动删除或自动恢复操作，当你需要正常拷贝文件到被监控目录，请先暂停该目录的监控，完成文件拷贝后，再启用。暂停该目录的监控很简单，找到对应的目录，取消勾选，点击“确定”按钮即可。如下图说明（比如要取消c:\test目录的守护）：

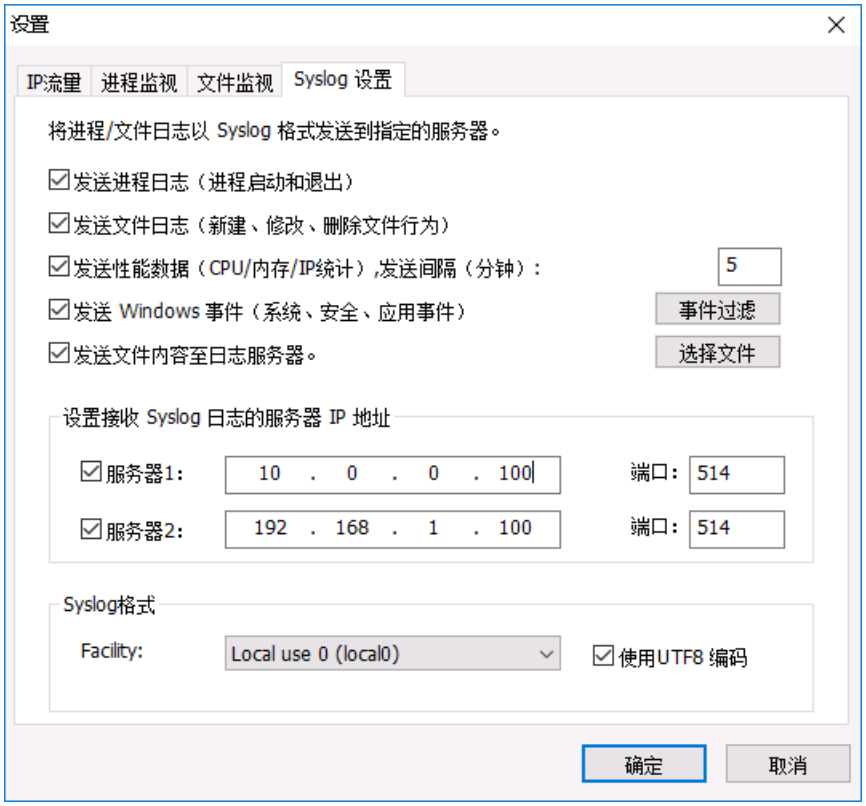


4.4、发送 SYSLOG 日志

F监控助手可以将检测到数据，以syslog格式发送到你指定的服务器上。在这个设置界面中，你可以：

- ✓ 启用和关闭Syslog日志发送功能。
- ✓ 是否发送进程的启动和退出日志。
- ✓ 是否发送文件创建、修改、删除日志。
- ✓ 是否发送服务器性能数据（CPU/内存/磁盘容量/IP统计）
- ✓ 是否发送Windows事件
- ✓ 是否发送文件内容（仅对文本文件）
- ✓ 设置接收syslog日志的服务器，支持2个日志接收服务器。
- ✓ 设置syslog日志格式和编码。

设置界面如下图所示：



操作步骤：

1、 选择要发送日志的类型：勾选表示发送，取消勾选，表示不发送。
2、 设置接收日志的服务器IP地址和端口。
3、 设置Syslog格式，使用默认值即可。

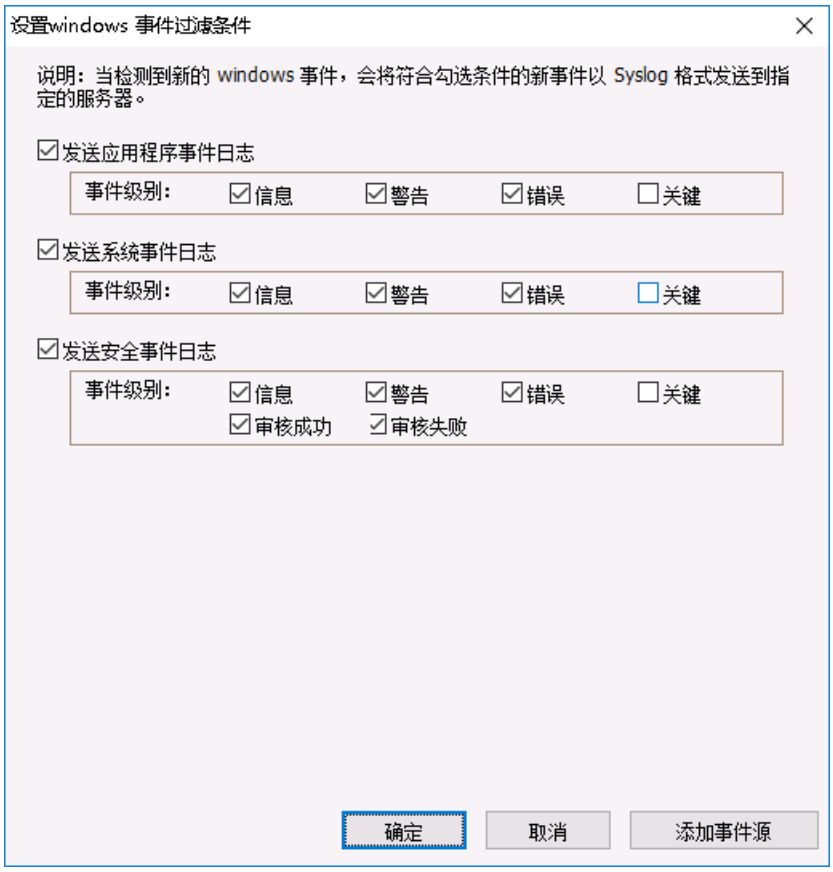
日志发送的时间间隔：性能数据为定时发送，在对应的右侧编辑框中输入间隔的时间，单位为分钟。其它类型日志为实时发送，即产生就发送。

4.5、监视 WINDOWS 事件

启动该功能后，当产生了新Windows事件时，将事件转换成Syslog格式发送到日志服务器，（之前已经生成的Windows事件不会发送）。在这个设置界面中，你可以：

- ✓ 启用和关闭Windows事件发送。
- ✓ 选择发送Windows 事件的类型和事件级别。

在“Syslog设置”页面下，点击“**事件过滤**”按钮，弹出设置界面，如下图所示：



操作步骤：

勾选要监视和发送的 Windows 事件类型和事件级别，点击“确定”按钮。

添加事件源：默认监视“应用程序事件”，“系统事件”，“安全事件”，可以点击“**添加事件源**”按钮增加新的事件类型。

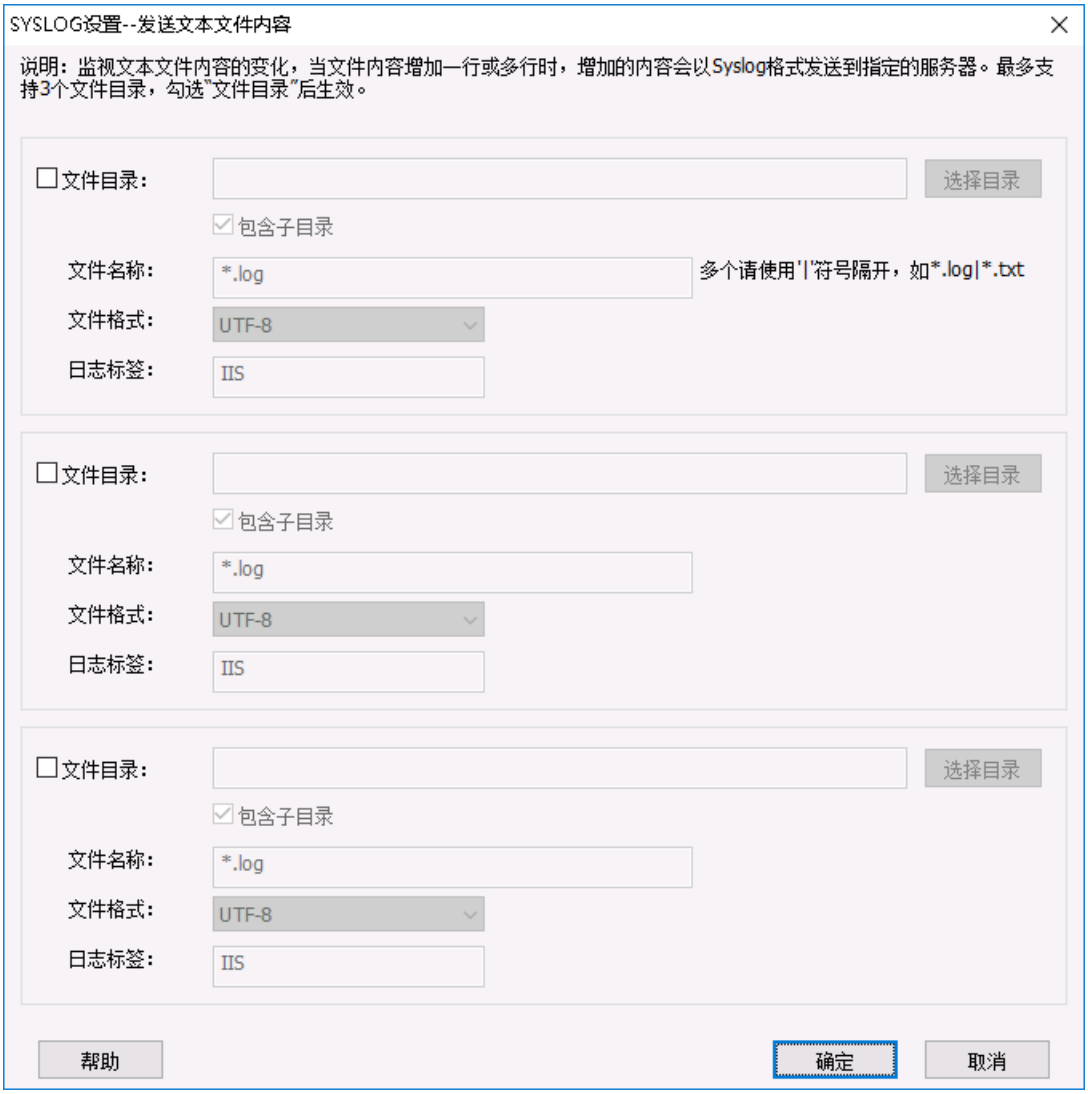
4.6、监视文件内容

当文本文件的内容发送变化时，将新增加的内容以syslog格式发送到日志服务器。在这个设置界面中，你可以：

- ✓ 启用和关闭文件内容监视。
- ✓ 设置文件所在目录。

提示：“文件内容监视”与“文件监视”功能的区别在于，文件监视只监视文件的创建、修改和删除的行为，不读取文件内容。“文件内容监视”是读取文本文件内容，并将内容发送到日志服务器。启用文件内容监视后，当目标文件的内容新增加一行或多行时，新增的内容会以Syslog格式发送到日志服务器。

在“Syslog设置”页面下，勾选“发送文件内容至日志服务器”，弹出设置界面，如下图所示：



选项说明：

1、“文件目录”勾选框：选中，表示启用。

2、“选择目录”按钮：选择目标文件所在目录。

3、“包含子目录”勾选框：选中表示包括子目录下的文件。

4、“文件名称”编辑框：需要匹配的文件名，多个文件名用’|’符号隔开，支持*号通配符，如：u*.log|*.txt表示所有以u开头并且后缀名为log，以及所有后缀名为txt的文件。

5、“文件格式”：即文本文件的编码格式，通常为UTF-8或者ASCII格式。选择错误的格式会导致乱码。

6、“日志标签”：用于说明日志的用途，比如是IIS日志可以填写IIS，该内容可以为空。为空表示不需要标签。

五、联系方式

F 监控助手官网：http://www.ipneed.com

联系邮箱：ipneed@163.com

QQ 号：609324269