F-Mon 服务器监控助手

(V6.1版)

用户手册

目录

一、产品简介	3
二、快速入门	5
2.1 安装	5
2.2 主界面介绍	5
三、功能说明	7
3.1 系统状态	7
3.2 性能指数	10
3.4 网速	12
3.5 网络连接	14
3.6 TCP 诊断	15
3.7 IP 流量	17
3.8 IP 统计	20
3.9 IP 日志	23
3.10 监控日志	24
3.11 巡检报告(仅高级版)	27
四、系统设置	29
4.1 设置 IP 流量监视	29
4.2 设置进程监视	30
4.3 设置文件监视	32
4.4 发送 Syslog 日志(仅高级版)	37
4.5 监视 Windows 事件	
4.6 监视文件内容(仅高级版)	

一、产品简介

F-Mon 服务器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,实现 Windows 服务器的深度监控和审计。F-Mon 能实时显示与服务 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。

服务器网络流量分析, F-Mon 服务器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。

服务器瓶颈分析,通过智能算法,从 CPU 指数、内存指数、硬盘指数、网络 指数等方面对服务器性能数据进行实时评估。不需要你自己判断,F-Mon 服务器 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。

服务器文件分析,监控服务器文件新建、修改、删除行为,并生成日志记录, 支持 syslog 日志发送。当你检查服务器可疑文件时,能方便查找上传文件的位置,定位被修改、删除的文件,结合 F-Mon 服务器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。

服务器文件守护,使用 F-Mon 服务器监控助手,你可以设置监控目录,对这 些关键目录进行保护,根据自定义规则自动删除新创建的文件,自动恢复被篡改 的文件,保护网站首页。

服务器进程守护,监控服务器进程运行状态,详细记录进程启动、退出行为, 并生成日志记录,支持 Syslog 日志发送。并能根据自定义规则,当进程意外退 出后,能自动拉起进程。

Windows 事件分析,采集 Windows 应用、系统、安全事件并支持 Syslog 格式转发。分析 Windows 事件,生成巡检报告。

F-Mon 服务器监控助手安装简单,即装即用,无需安装其它支撑软件。图形 化界面操作简单易用、信息丰富。

产品功能和特点

- Windows 服务器网络流量深度采集和分析,精准定位占用流量的应用程序和 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、IP 地理位置等;
- 服务器性能指数分析,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网站和应用系统的需要。
- 3. Windows 事件监控, 支持 syslog 转发。
- 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 记录;重要日志提醒。
- 5. 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。
- 7. 日志文件内容监控,将各种日志文件文本内容以 Syslog 格式发送。
- 8. 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。
- 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。
- 服务器巡检,自动生成服务器巡检报告,内容包括关键 Windows 事件巡 检,服务器访问量统计,CPU,内存使用检查;进程资源使用检查;磁盘 空间检查;服务器开放端口检查。
- 11. 系统安装简单,占用资源少,不影响服务器正常运行。

二、快速入门

2.1 安装

F-Mon 服务器监控助手提供图形化安装界面,安装过程简单,无需任何第三方软件支持。F-Mon 服务器监控助手软件占用资源小,支持的操作系统包括:Windows 2003/2008/2012/2016,中英文版不限。

2.2 主界面介绍

F-Mon 服务器监控助手运行后,主菜单(高级版)如下图所示:

🕎 F-	Mon 服务器监控	空助手									—		×
		L 性能指数	參 进程		の の 络 连 接	<u>⑧</u> TCP诊断	P IP流量	IP统计	三 IP日志	66 监控日志	ご ※ たんしまた。 ※ たんしまた。 ※ たんしまた。 ※ たんしまた。 ※ こので、 ※ で、 ※ で、	:	∎×
主势	哀单栏最	右侧是	设置菜	E单	, 点	击后弹b	出主菜	单,如⁻	下图:				
打 显易 (中) () () () () () () () () () () () () ()	J开 F-Mon 등示學学會 操手會美型 毕体缩放 外速显示 全面 "监控日志"… "品注册… 都注册… 都注册。 "品注册… 能注册。 "品注册…	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>											

菜单项说明:

"打开 F-Mon":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。
- "字体缩放":选择界面的字体大小。

"设置":弹出设置窗口,详细的设置说明,请见"系统设置"章节。

"**清空监控日志**":删除 F-Mon 生成的进程、文件、windows 事件等监控日志,但不 包括 IP 日志。

"**导出监控日志"**:将所有的"监控日志"记录导出成 txt 文件。F-Mon 服务器监控助 手最多只保留 50 万条日志,超过这个数量会自动清空。

5

"产品注册":用于 F-Mon 服务器监控助手产品注册。

"开机自动运行":服务器启动后,自动运行 F-Mon 服务器监控助手。

"退出":退出 F-Mon 服务器监控助手界面程序,但 F-Mon 后台服务程序不会退出,仍然保持运行。

三、功能说明

3.1 系统状态

系统状态标准版和高级版略有不同。

标准版主界面如下图



底部显示服务器连续运行时间,上网 IP 地址,以及网卡(所有网卡)流量趋势图。

高级版主界面如下图:

▶ F-Mon 服务器监控助手			- 🗆 X
上 上 <td></td> <td></td> <td>2 E E E E E E E E E E E E E E E E E E E</td>			2 E E E E E E E E E E E E E E E E E E E
100 75 50 25	CPU/物理内存使用 CPU: 5% 100M Mem: 13% 10M	实时 1小时 3小时 12	2小时 1天 3天 7天 硬盘读写(字节/秒) 体读:87/M 写:93.0M
物理内存: 15 G 正在使用: 2236 M 峰值: 2312 M 13%	内存分页: 18 G 正在使用: 1431 M 峰值: 1618 M 译值 7%	存(分页文件) ※: 0% ※: 0% : 未知 0%	内存页与硬盘交换(字节/秒)) 从硬盘读页面 81.7M/s 内存页面写入硬盘 0.0K/s
C:本地 199.4 G 剩余空间: 185.9 G 读速度: 0.0K/s 写速度: 0.0K/s 繁忙度: 0.0% 7%	D: 本地 1.6 T 则余空间: 1.4 T 读速度: 0.0K/s 写速度: 93.0M/s 繁忙度: 57.2% 16%	1. 1.8 T 1. 1.6 T 1. 0.0K/s 1. 0.0% 1. 0.0%	G: 本地 3.6 T 剩余空间: 3.3 T 读速度: 87.7M/s 写速度: 0.0K/s 繁忙度: 82.1%
受 开机运行时间: 0 天 00 小时 37 分 46 秒	▲ 进程监视:29	🖌 文件监视 : 正常	🝐 Windows事件:25

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-Mon 服 务器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。

当磁盘数量大于4个时,磁盘信息区域右下角会出现翻页符号>,点击翻页符可以展示 其它磁盘的使用情况,在磁盘信息区双击鼠标左键(当磁盘数量>4),会显示所有磁盘 的缩略信息(磁盘已使用百分比以及读写状态),如下图:

☑ F-Mon 服务	器监控助手							– 🗆 X
公 系统	2 計 状态 性能指数	⊗ x 进程	M 速 网 M M M m 和 m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m m	24 8 区 各连接 TCP诊	D 断 IP流量	い IP統计 IP		三 - 巡检报告
100 75 50 25		~~~~	СРИ	/物理内存使用 CPU: 5% Mem: 13%	200M 100M 10M 1M	81 1/485 3/48	1 12小时 1天 硬盘道	3天 7天 \$\$\$(字节/秒) \$\$:93.0M
	物理内存: 正在使用: 2 峰 值: 2	15 G 2236 M 2312 M 13%	内存分页: 正在使用: 峰 值:	18 G 1431 M 1618 M 7%	虚拟内存(已使用%: 峰 值%: 合适度:	分页文件) 0% 0% 未知 0%	内存页与硬盘交 从硬盘读页面 内存页面写入砌	换(字节/秒)) <u>81.71\/s</u> [■] 盘0.0K/s
C:	D: E: 0% 0%	F: G: H	t: I: J: % 0% 0%	K: L:	M: N: 0% (O: P: Q: 0% 0% 0%	R: S: T: 0% 0% 0%	U: V: W: 0% 0% 0%
🕜 开机运行	时间:0天00	小时 37 分 46 秒	>	▲ 进程监视:	29	🕗 文件监视:正常	🔺 Windo	ws事件:25

系统状态面底部的状态栏实时显示服务器连续运行的时间,以及新生成的进程、文件和 windows 事件的数量,鼠标点击数字区域后可直接跳转到"监控日志"页面。

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,说明该项可能出现性能瓶颈。

如下图中,物理硬盘0(上面有1个分区,即D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(如图中拥塞指数为红色),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。



刷新,性能指数的计算是从 F-Mon 启动时开始检测并实时计算,如果需要重新计算, 需点击页面上方的"刷新"区域。当新增加或者卸载磁盘,也需点击"刷新"更新磁盘 信息。

重要说明:性能指数的检测,采用旁路式监测,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:

当于14 2 新。160 年6			最大CP	最大CPU: System - 0%			最大 IO 读写:		xe - 0.4 KB/s			
	小相注的过去	01±4X; 20	大陸立住住	最大内容	存: \	WINWORD.	XE - 199 MB	最大网络连挂	賽: QQ.exe	- 28		
进程	PID	CPU	CPU 时间	内存使用	内存	使用峰值	IO读速率	10写速率	网络连接数	-		
svchost.exe	2132	0	0:00:00	7.88 MB	3	8.13 MB	0 B/s	0 B/s	-	C:\Windows\System32\svchc		
svchost.exe	6844	0	0:00:00	定位文件	位置		0 B/s	0 B/s	-	C:\Windows\System32\svchc		
svchost.exe	2464	0	0:00:00	复制文件	路径		0 B/s	0 B/s	-	C:\Windows\System32\svchc		
svchost.exe	5416	0	0:00:00	查看网络连接	大王回修う	本王网络》			0 B/s	0 B/s	8	C:\Windows\System32\svchc
RuntimeBroker.exe	9760	0	0:00:00		查看网络连接		0 B/s	0 B/s	-	C:\Windows\System32\Runti		
svchost.exe	2560	0	0:00:00	首有进程	금제다	*	0 B/s	0 B/s	-	C:\Windows\System32\svchc		
svchost.exe	5808	0	0:00:00	结束进程			0 B/s	0 B/s	-	C:\Windows\System32\svchc		
vmnat.exe	3080	0	0:00:00	7.36 MB	3	7.54 MB	0 B/s	0 B/s	-	C:\Windows\SysWOW64\vm		

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"监控日志"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 网速

显示服务器公网网速和每块网卡实时网络流量以及每5分钟的平均网络流量。

🖾 F-N	lon 服务器监控助	手									-	
	至 系统状态 15		▲ 网速	の会正接	<mark>⑧</mark> TCP诊断	P IP流量	íí IP统计	IPE]志 监	2 <mark>.98</mark> 注日志	いいしょう (End) (End	≡·
10 1 7.5 1 5.0 1 2.5 1	公网网速 Abps vbps vbps 09:26	■ 发送 09:48 表	I 接收	1 分钟平均 1 分钟平均 10:10 网卡发送: 0.00 l		00 Mbps	10:56		1 分钟 11 11	▶ 5 分钟	15 分钟 30 	分钟 10 Mbps 7.5 Mbps 5.0 Mbps 2.5 Mbps 1:41
网卡ID	网卡IP	发送	接收	数据包/秒	配置IP数量	状态	丢弃包数	错误包数	队列长度		P	网卡描述
17	192.168.99.1	0	0	0	1	已连接	0	0	0	VMware V	irtual Etherr	net Adapter for
7	192.168.49.1	0	0	0	1	已连接	0	0	0	VMware V	irtual Etherr	net Adapter for
6	192.168.1.118	0.85 Kbps	1.2 Kbps	4	1	已连接	0	0	0	Qualcomn	n QCA9565	802.11b/g/n W
20		0	0	0	0	未连接	0	0	0	Intel(R) Et	hernet Conn	ection (7) 1219-
18		0	0	0	0	未连接	0	0	0	Microsoft	Wi-Fi Direct	: Virtual Adapte
15		0	0	0	0	未连接	0	0	0	Microsoft	Wi-Fi Direct	t Virtual Adapte
9		0	0	0	0	未连接	0	0	0	Bluetooth	Device (Per	sonal Area Net
<												>
() म	闲运行时间: 7	天 21 小时 00 分	}47秒	🔺 i	进程监视: 112	26	🔺 文件监视	l: 552		🔺 Window	/s事件: 634	4

界面说明:

中间小图形显示所有网卡的速率之后,鼠标点击图形任何位置,可以查看每个网卡的流 量趋势图,如下图所示:

	应 网卡流量趋势	网卡 发送: 0.00 Mbps 接收: 0.00 Mbps	网卡实时速率	5分钟平均速率
	VMware Virtual Ether	net Adapter for VMnet8 [192.168.99.1],状态:已连接 ,配置IP数:1 个		
70 Mbps			发送速率:	0 bps
53 Mbps			接收速率:	0 bps
35 Mbps			数据包/秒:	0
18 Mbps			错误包数:	0
10 10 10 10 10			等待发送包:	0
	Oualcomm OCA9565	802.11b/a/n Wireless Adapter [192.168.1.118],状态:已连接 ,配置P数:1 个		
70 Mbps		, , , , , , , , , , , , , , , , , , ,	发送速率:	0.00 Mbps
53 Mbps			接收速率:	0.00 Mbps
35 Mbps			数据包/秒:	12
19 Mbpc			错误包数:	0
to wipps			等待发送包:	0

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。

发送速率: 该网卡每秒发送字节数量,单位 bps(比特每秒)和 B/s(字节每秒)可以 在系统菜单中"网速显示"菜单项进行设置。

接收速率: 该网卡每秒接收字节数量。

数据包/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。

等待发送包: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:

	刷新	TCP 连接数: 48	UDP: 55					连接状态:	显示全部 ▼	
	协议	进程	本机IP	本机端口	远端IP	远端端口	状态	PID	远端IP位置	^
5	TCP	vmware-authd.exe	0.0.0.0	912	0.0.0.0	0	LISTEN	4372	N/A	÷
6	TCP	vmware-authd.exe	0.0.00	902	0.0.00	0	LISTEN	4372	N/A	
7	TCP	System Idle Process	192.168.1.108	50134	52.109.124.5	443	TIME_WAIT	0	新加坡Microsoft公司	
8	TCP	System	0.0.00	5357	0.0.00	0	LISTEN	4	N/A	
9	UDP	System	192.168.1.108	137	0.0.00	0		4	N/A	
10	TCP	System	0.0.0.0	445	0.0.0.0	0	LISTEN	4	N/A	
11	UDP	System	192.168.1.108	138	0.0.0.0	0		4	N/A	

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									
查看进程启动日志									
结束进程									

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 TCP 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:

🛃 F-Mon 🛚	股务器监控助 习	£									-		×
[系	<mark>ン</mark> 充状态 性	副	參 进程 [∽ 网速 网	CC Main a set a s	<mark>@</mark> TCP诊断	P P流量	ííí IP统计	IP日志	<mark>99+</mark> 三 监控日志	ご ※ 総 板 振告		≡-
📕 刷新统计	+图								搜索端口:	或远端IP:		Q	
TCP活动(P8120 > 08/2 P13548 > 08, P16352 > 08, P16352 > 08, P13788 > 08, P13788 > 08, P13788 > 08, P1756 > 08/2 P13548 > 08, P1756 > 08/2 P1756 > 08/2 P1756 > 08/2	加速加速をした 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.18 1.11 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13 1.13												
TCP重传: 连接失败:	58 0	断开次数: 连接次数:	2074 2012	TCP重连:	400		TCP重传: 连接失败:	58 0	断开次数: 连接次数:	0	TCP重连:	0	
800 600 400	- 断开次数 -	— 建立连接 ·		- TCP重连	— 连接:	关 败	100% 75% 50%		م	的路连接错误率		0	\otimes
200	:00 15:00 17	:00 19:00 21:	00 23:00 1:00	3:00 5:00	7:00 9	:00 11:00	25%	15:00 17:00	19:00 21:00 2	3:00 1:00 3:0	0 5:00 7:00	9:00	11:00
	MININ: 1	大 21 小时 (02分58秒		西进	框	2	👛 又件监视	: 554	A Windo	ws事件: 649		

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。

15

"-x-":表示服务器与对方断开连接。

右侧窗口:为<u>监视窗口</u>,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,点击左上角图标,可以打开和刷 新统计图。

📕 显示TCP连接活动统计图

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 server 的不同版本,连接类型会变化,比如 windows server 2003 只显示3 种类型: 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,可以长时间的持续监测。

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:

🖾 F-N	Non 服务器监控助手								- 0	×
	 系统状态 性能指 	》 数 进程		CC M络连接	図 TCP诊断 IP設	D 前 猛 IP统i	│ <u>=</u> + IP日志	<mark>16</mark> 上 上 上 注 日志	送回 巡检报告	∎
<u>一</u> 隆	藏进程流量表							当前IP流起	最近IP访问记	灵
PID	进程		发送字节/秒	接收字节/秒	今天流量 (发送)	今天流量 (接收	() 当前访问IP数	[]	描述	^
1756	QQ.exe		0	0.03 KB/s	531.81 KB	209.84 1	MB 1	腾讯QQ		
1320	firefox.exe		0	0	1.72 MB	53.79 1	MB 1	Firefox		
13788	WeChat.exe		0	0	5.71 MB	6.48 1	MB 1	WeChat		
16352	DingTalk.exe		0	0	125.25 KB	5.48 1	MB 1	钉钉		
14992	SearchUI.exe		0	0	167.79 KB	3.91 1	MB 1	Search and	d Cortana application	n
2440	svchost.exe		0	0	283.81 KB	549.98	KB 1	Windows #	669年进程	
13020	smartscreen.exe		0	0	224.28 KB	565.39	KB 1	Windows [Defender SmartScree	n
11260	MicrosoftEdgeCP.ex	e	0	0	35.89 KB	605.05	KB 14	Microsoft	Edge Content Proces	is 🖉
<			^	^	100 00 100	*****	··· ·	••••		>
PID	进程	远端IP	迈端端口	本机IP	本机端口	发送字节/秒	接收字节/秒	息数/秒	远端IP位置	^
1756	QQ.exe	120.204.17.12	2 8000	192.168.1.1	18 62966	0	0.03 KB	0.04 KB	上海市	移动
14992	SearchUI.exe	23.1.244.77	443	192.168.1.1	18 55351	0	0	0	美国Akamai	节点
7388	MicrosoftEdgeCP.exe	23.32.241.8	443	192.168.1.1	18 55387	0	0	0	日本Akamai	节点
7388	MicrosoftEdgeCP.exe	27.151.12.70	443	192.168.1.1	18 55379	0	0	0	福建省福州市	电信
11260	MicrosoftEdgeCP.exe	49.7.36.27	443	192.168.1.1	18 55390	0	0	0	北京市	电信
11260	MicrosoftEdgeCP.exe	49.7.36.94	443	192.168.1.1	18 55409	0	0	0	北京市	电信
11260	MicrosoftEdgeCP.exe	49.7.36.100	443	192.168.1.1	18 55406	0	0	0	北京市	电信
11260	MicrosoftEdgeCP.exe	49.7.40.174	443	192.168.1.1	18 55404	0	0	0	北京市新浪	电信
9632	mcshield.exe	52.69.144.176	443	192.168.1.1	18 55364	0	0	0	日本东京Amazon数据	中心
13020	smartscreen.exe	52.163.89.138	443	192.168.1.1	18 55408	0	0	0	美国加利福尼亚州圣克	拉 丶
Æ	刊、运行时间: 8 天 0	0 小时 34 分 2	5秒	🔺 进程	监视: 241	🔺 文件监	视: 8	🔺 Windo	ows事件: 239	

"*当前 IP 流量*"窗口分为上下 2 部分,通过"*隐藏进程流量表*"按钮可以控制是否显示进程流量统计信息。

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。

今天流量(发送/接送):该程序当天零点开始到23:59分的累计网络流量。

当前访问 IP 数: 指进程正在通信的 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:

<u>显示 PID 的进程名称</u>: 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"。

显	示全部 公科	3	搜索端[]号/PID/IP位置:	Q IP数量: 215				当前IP流量	最近IP访问记录
PID	远端IP	远端端口	本机IP	本机端口	发送字节	接收字节	总字节	访问次数	最后访问时间	远端IP位置
4	192.168.1.108	138	192.168.1 255	100	^ B	16.88 KB	16.88 KB	2	10/11 16:58:18	局域网
4	192.168.198.255	138	192.168.1	复制远端IP地址	B	0 B	4.56 KB	2	10/11 16:58:17	局域网
4	192.168.198.1	138	192.168.1	查看IP日志	В	17.40 KB	17.40 KB	2	10/11 16:58:17	局域网
4	192.168.68.255	138	192.168.6	查看进程启动日志	Б. В	0 B	4.94 KB	2	10/11 16:58:17	局域网
4	192.168.68.1	138	192.168.6	清空最近IP记录	В	17.76 KB	17.76 KB	2	10/11 16:58:17	局域网
5416	192.168.1.1	1024	239.255.2	导出表格数据	В	77.52 KB	80.10 KB	2	10/11 16:56:45	局域网
5644	52.109.56.34	443	192.168.1.108	50138	וא ככ.עדB	21.91 KB	41.46 KB	1	10/11 16:55:48	印度

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。支持按 ip 位置,端口后和进程 PID 进行搜索。

搜索提示: 鼠标移至"搜索端口号/PID/IP 位置"位置,并停留 2 秒左右, 会弹出搜索提示, 如下图所示:

显	示全部 公	NG .	搜索端口号/F	PID/IP位置:	局域网	Q	IP数量: 11		当前IP流量	最近IP访问记录
PID	远端IP	远端端口	本机IP	搜索提示:			-#D:2##CD	访问次数	最后访问时间	远端IP位置
5416	192.168.1.253	1025	239.255.255.250	数字: 如 60 数字+L: 本	, 漫送)全10(P10), 足 机端口, 如 80L .表示	355500、4 【按本机端日		3	10/11 17:08:04	局域网
2308	10.220.250.50	53	192.168.1.108	数字+R: 远	端端口,如 80r,表示	按远端端口	=80搜索。	3	10/11 17:07:50	局域网
5416	192.168.1.1	1024	239.255.255.250	数字+P: 进程ID, 如 80p,表示按PID=80搜索。		3	10/11 17:06:45	局域网		
2308	192.168.1.120	5353	224.0.0.251	数字+.: 远端IP, 如 192.,表示搜索所有192升头的IP。				3	10/11 17:04:58	局域网
4	192.168.1.255	138	192.168.1.108	138	4.04 KB	0 B	4.04 KB	2	10/11 16:58:18	局域网

搜索条件说明:

- <u>按进程 ID 进行搜索</u>: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。
- <u>按本机端口号搜索</u>: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
- <u>搜索远端IP</u>: 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。

<u>数据刷新</u>: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"或"显示全部"按钮刷新数据。

3.8 IP 统计

☑ F-Mon 服务器监控	助手								_	
¥.	Ŧ	۲	~	<u>م</u>	<u>s</u> (9	ĩi I	E (17	E	≡-
系统状态	性能指数	进程	网速	网络连接 TCI	P诊断 IP》	能量 IP	统计 IPE	1志 监控日志	巡检报告	
✓ 统计规则	访问量:	806	独立IP数:	统计日期范围: 20 543	020.8.28 至 2 发送流量:	020.8.28 35.40 MB	接收流量:	473.20 MB 总济	建 : 508.60) MB
今 天	300 MB									300 MB
最近24小时	240 MB									240 MB
本月	180 MB									180 MB
最近30天	60 MB									60 MB
今年	00 110				.					
最近12个月		广东省 湖北省	皆 上海市	美国	河北省 日		諸 天津市	1 北京市 福	建省 其它	
		地区		访问量 (IP数)	独立IP数	发送济	糧 (字节)	接收流量 (字节)	总流量 (字节	j) ^
周总结	3	上海市		60		46	0.52 MB	48.78 MB	49.3	0 MB
	4	美国		180		123	25.02 MB	9.49 MB	34.5	1 MB
·→·入IP地区力和	5	河北省		8		12	0.03 MB	28.85 MB	28.8	7 MB
▶ 今天IP流量分布	7	中国		17		24	0.20 MB	12.98 MB	13.2	S IVID
	8	天津市		29		24	0.09 MB	13.09 MB	13.1	8 MB
自定义查询	9	北京市		98		70	1.63 MB	8.70 MB	10.3	4 MB
	10	福建省		3		2	4.08 KB	7.15 MB	7.1	6 MB
	11	江苏省		12		10	0.06 MB	4.15 MB	4.2	1 MB
	12	江西省		4		4	0.16 MB	3.09 MB	3.2	5 MB 🗸
🕜 开机运行时间:	8天00小时	t 37 分 13 秒		🔺 进程监袖	l: 253	🔺 文(牛监视: 8	🔺 Windo	ws事件: 240	

根据自定义统计规则,统计服务器的访问流量。

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**"按钮当前统计结果导出为 csv 文件。

自定义统计规则:按指定的端口号(本机)统计IP流量,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"<u>启用流量过滤</u>",并在下方 编辑框中输入网站的端口号,一般是80(http)或443(https)。*

段置IP流量统计规则	\times					
按端口流里过滤 勾选此项,表示按下列"本机端口"统计服务器流里。如果只统计服务器网站的流 里,请勾选此项,取消勾选,则统计所有流里。						
80,443 最多输入5个端口和范围,使用逗号隔开,如:80,443,21-300,8080						
公网/内网流里过滤 【仅统计公网流里						
说明: 规则修改后,下个统计周期(1小时)开始生效。						
<u> </u>						

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)。 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"<u>启</u> <u>用流量过滤</u>",并设置端口号。

规则修改后,下一个整点时间(小时)生效。

3.9 IP 日志

F-Mon 服务器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。

选择	峄日期: 2020/09 ▼	日: 30	▼打开	导出记	录数量: 1243		搜索	IP: Q
PID	远端IP	远端端口	本机IP	本机端口	发送字节	接收字节	总字节	最后访问时间
1864	224.0.0.251	5353	192.168.1.108	5353	17.09 KB	0 B	17.09 KB	2020/09/30 22:48:55
1864	192.168.1.108	5353	224.0.0.251	5353	0 B	13.03 KB	13.03 KB	2020/09/30 22:48:55
4196	40.90.189. 192.168.1.1	08:局域网	192.168.1.108	57447	13.92 KB	27.54 KB	41.46 KB	2020/09/30 22:48:55
1864	224.0.0.252	5355	192.168.1.108	50145	399 B	0 B	399 B	2020/09/30 22:48:55
2392	239.255.255.250	3702	127.0.0.1	57293	92.28 KB	0 B	92.28 KB	2020/09/30 22:48:55

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 监控日志

F-Mon 服务器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,文件创建、删除、修改记录, 进程启动、退出记录,用于查询和审计。



重要日志:

F-Mon 已自动筛选出如服务器登录,账号变动,服务器主 IP 变动等作为重要日志,并显示未查看的重要日志数量,点击数字,可以打开重要日志表格,未读日志用蓝色标记。

最近 24 小时日志统计:

F-Mon 统计每小时所检测到的日志数量,并以柱状图显示最近 24 小时数据, 点击每个柱状图,可以显示所选中时段的所有日志。

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,通过<>设置搜索时间范围,如果不设 置时间范围,默认在最近5万条日志中搜索。搜索命令如下:

- > 关键字; 如: ">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*>被F-Mon 服务器监控助手自动拉起的程序启动记录。

f*> 搜索文件被F-Mon 服务器监控助手恢复,自动删除的记录。

fc*> 搜索文件被F-Mon 服务器监控助手恢复的记录。

fd*> 搜索文件被 F-Mon 服务器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。

重要说明:

监控日志最大存储容量为 50 万条,当日志达到 50 万时,所有监控日志(不含 IP 日志) 自动清除,如果需要留存日志,可以在主菜单中手动导出监控日志。

3.11 巡检报告(仅高级版)

F-Mon 自动生成服务器巡检报告,内容包括重要 Windows 事件巡检,服务器访问量统 计,CPU、内存使用检查,进程资源使用检查,磁盘空间检查,服务器开放端口检查等。

点击"今天最新数据"按钮可以立即生成最新的巡检报告,所有巡检报告支持导出。

☑ F-Mon 服务器	监控助手							- [) ×
云 系统状态	世能指数	參 进程		CC <u>(</u> 図 () CP	D D D D D D D D D D D D D D D D D D D	ííí IP统计		近し、	≡.
最近7天报告		今天	最新数	居 导出(CSV)	复制报告内	容		<u>/</u> 6	置
	1 份报告		25	服务器访问量	外网IP访问: 31	3个			^
2020年09月08日	08:00				内网IP访问: 6	个			
2020年09月07日					外网流入: 24.3	MB	流出: 43.3 MB		
2020年09月06日					内网流入: 0.1	MB	流出: 0.0 MB		
2020405/5000			26	昨日访问量	外网IP访问: 51	2个			
2020年09月05日					内网IP访问: 6	个			
2020年09月04日					外网流入: 42.3	MB	流出: 66.3 MB		
2020年09月03日					内网流入: 0.18	B MB	流出: 0.04 MB		
2020-05/3051			Wind	ows事件					
2020年09月02日				名称	当天数量	最近7天	事件ID		
更多历史报告 🗸			27	错误事件	6	23	事件类型="错误"的事件…		
			28	用户登录成功	64	627	4624		
			29	登录失败	2298	11529	4625		
			30	创建用户帐号	0	0			
			31	删除用户帐号	0	0			
			32	用户帐号改变	0	0			~
🙆 开机运行时间:	141 天 00 小	时 27 分 19	秒	🔺 进程监视		✓ 文件监视: Ī	E常 🔺 Windov	/s事件: 3	

巡检报告配置

报告配置			×
报告标题:			
肥冬翠田泽,	, 		
服为番用还:			
报告保存目录:	C:\Program Files\FMon	aid	浏览
每天巡检时间:	巡检开始时间	(时:分)	增加时间
	1 08:00 2 18:00		删除时间
Windows事件:	名称		增加事件
	1 用户登录成功	3#528,540,4624	28/38 - 11
	2 登录失败	3#529-537,539,4625	删除事件
	3 创建用户帐号	3#624,645,4720,4741	
	4 删除用户帐号	3#630,647,4726,4743	「広田時」」は
	5 用尸帐亏奴发	3#625-629,642,644,646,4.	"恢复默认值
	7 审计政策改变	3#612 4719	
	8 创建计划任务	3#602.4698	
	C CILE / ANT /		
	<	>	
🗆 上传报告至	· · ·	端口: 8080	连接测试
□ 上传IP日志			
		确定	取消

增加 Windows 巡检事项:

巡检报告支持自定义 Windows 事件巡检项目,点击"增加事件"按钮,弹出如下对话框。

设置Windows事件检查项						
名称:	登录失败					
事件 ID:	3#529-537,539,4625					
		确定				
	格式如: 528,600-620,539					

输入名称以及匹配的 Windows 事件 ID。事件 ID 的输入格式为:来源 ID#事件 ID;其 中来源 ID 定义为

1=应用程序事件

2=系统事件

3=安全事件

如 3#4625,即匹配安全事件且事件 ID=4625 的事件作为登录失败巡检项目。

来源 ID 可以省略,如果不指定来源 ID,则只按事件 ID(EventID)进行匹配,多个 ID 使用逗号隔开。

巡检报告支持集中管理:

巡检报告和 IP 日志文件支持集中管理,但需要另外部署 fmon 集中管理软件。

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:

- ✓ 设置IP流量监控。
- ✔ 设置文件监控。
- ✔ 设置进程监控。
- ✓ 设置发送syslog日志。
- ✓ 设置Windows 事件监控。

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:

启用	IP流量监视				
包洗	此项后,会记录所有	頁访问本机的远端IP地址	、流量以及访问时	间。并对IP地	址进
和分	'n∏∽				
自动	保存IP日志,每小时	保存一次。保存日志文	牛到:		
Dule	nviolog				
10:4	nyipiog				浏览
,					
設置自	定义IP段(最多512	条记录),用于统计IP分	```		
	起始IP	结束IP		添加	ΩIΡ₿
1	5.9.66.0	5.9.156.255	网络爬虫		_
2	5.45.207.0	5.45.207.255	网络爬虫		
3	5.189.160.0	5.189.160.255	网络爬虫	删除	₿₽₽
4	5.196.87.0	5.196.87.255	网络爬虫		
5	5.255.250.0	5.255.250.255	网络爬虫		
6	10.0.0.0	10.10.255.255	北京分公司		
7	10.11.0.0	10.20.255.255	上海分公司		
8	10.30.0.0	10.40.255.255	浙江分公司		
9	10.50.0.0	10.60.255.255	物流分公司		
10	40.77.167.0	40.77.167.255	网络爬虫		
11	42,120,160,0	42,120,161,255	网络爬虫		
12	42,120,234,0	42.120.236.255	网络爬虫		
13	42, 156, 136, 0	42, 156, 139, 255	网络爬虫		
14	42,156,254,0	42, 156, 254, 255	网络爬虫		
15	42,236,10,0	42,236,17,255	网络爬中		
16	42,236,46.0	42,236,46,255	网络爬中		
17	42,236,48.0	42,236,55,255	网络爬虫		
	42 236 00 0	47 736 00 755	网络爬击	×	
18					

- **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。
- **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:

设置	×
IP流量 进程监视 文件监视 Syslog 设置	
☑ 监视所有进程,当有进程启动或者退出时,生成日志记录。	
☑ 监视下面指定的进程,当进程退出时,执行自定义的操作。	
监视进程名: java.exe	设置
C:\CloudResetPwdUpdateAgent\depend\jre1.8.0_131\	
监视进程名:	设置
监视进程名:	设置
监视进程名:	设罟
监视进程名:	设置
确定	取消

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:要启用进程 守护, 需使用"<u>监视指定进程</u>"功能。*)

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,参见下* 方"重要说明"。)

监视进程名:
iexplore.exe C:\Program Files\Internet Explorer\iexplore.exe $\qquad \lor$
进程路径:
C:\Program Files\Internet Explorer\iexplore.exe
当进程退出时,执行下面操作
☑ 进程启动和退出,生成日志记录。
☑ 退出后,重新运行被监视程序
□ 退出后,运行下面指定程序(仅支持.exe和.bat文件)
浏览
运行程序的参数,可选填
命令行参数:
延迟: 30 秒,启动程序
□ 允许与桌面交互,当运行的程序要显示界面时勾选此项
删除 帮助 确定 取消

进程守护重要说明:

- 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实例 在运行(比如Java程序,其程序名都是java.exe),任意一个实例退出,都会自动 启动。
- 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。

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。

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。这样,F-Mon服务器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。(仅标准版有此功能)
- ✔ 设置是否恢复被修改的文件。

设置界面如下图所示:

22200000000000000000000000000000000000		;	×
IP流量 进程监视 S	[件监视 Sys	slog 设置	
监视文件夹内创建] 文件夹。	7件、删除文	件、修改文件的行为,并生成日志记录。最多同时监视5个	
☑ 监视文件夹:	c: \	设置	
	监视目录及	子目录(目录和子目录下所有文件)	
☑ 监视文件夹:	C:\inetpul	b\www.root\ 设置	
	监视目录及	子目录(目录和子目录下所有文件)	
☑ 监视文件夹:	C:\inetpul	b\ 设置	
	监视目录,		
□监视文件夹:		设置	
□监视文件夹:		设置	
		确定取消	

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:

设置文件监视	×					
监视类型: 监视目录及子目录(目录和子目录下所有文件)	~					
文件位置: C:\inetpub\wwwroot	浏览					
指定文件名:	.phpl.jsp等,以 "I"是隔开 公白					
排除文件名: .png .jpg	表示监视全部					
选择监视行为,至少选择一种						
发现上述修改后,执行下面操作 □自动删除新文件,若监控了系统目录(如C:\),请慎选。 ☑ 使用备份文件,恢复被修改、删除的文件。 备份文件位置:						
C:\网站首页备份	浏览					
删除 帮助	确定 取消					

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-Mon服务器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"<u>删除</u>"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(仅标准版有此功能): 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。<u>"排除文件名"优先级高于"指定文件名"</u>。

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。

<u>写文件</u>:监控对目标文件内容的修改操作。

<u>新建</u>: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-Mon服务器监控助手》自 动执行的操作。

自动删除新建文件(仅标准版有此功能):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-Mon服务器监控助手》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:

启用了某个目录文件监控的自动删除和恢复功能后,当你需要正常拷贝文 件到这个目录,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 图示例:

设置	×					
IP流量 进程监视 文件监视 Syslog 设置						
监视文件夹内创建文件、删除文件、修改文件的行为,并生成日志记录。最多同时监视5个 文件夹。						
将勾选取消,即不要勾选。并点击"确定"按钮						
☑ 监视文件夹: C:\test\ 设置	:					
监视目录及子目录(目录和子目录下所有文件)						
□ 监视文件夹: c:\inetpub\wwwroot\ 设置	:					
监视目录及子目录(目录和子目录下所有文件)						
□ 监视文件夹: 设置	:					
□ 监视文件夹: 设置						
□ 监视文件夹: 设置						
确定 取消	ŧ.					

图 停止目录监控

4.4 发送 SYSLOG 日志(仅高级版)

F-Mon服务器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:

Ⅳ流量│进程监视│文	(件监视)Windows 事件 Syslog 设置)	
将"监控日志"以 Sys	log 格式发送到指定的服务器。	
区 华泽进程中主 /	进程合动和电力	
	应性后幼稚吃山/ 彭建 修改 画(2-1)	
▶ 反因又任日志 (新建、修改、删除文件们为7 cpu/内方/ps统计) 坚焦问题。 30	0 新
	(件 / 系统、完全、应用事件等)	- 12
☑ 发送 Windows 事	"叶、赤坑、女主、应用事件等" "中主服冬哭,占击"进择文仕"坟知设罢日	标文件。
进 及医文件的语言		
┌设置接收 Syslog E	日志的服务器 IP 地址	
▼ 服务器1:	192 . 168 . 0 . 100	端口: 514
☑ 服务器2:		端口: 1214
_Syslog格式 ────		
Facility:	Local use 0 (local0)	↓ 使用UTF8 编码
	,	
		确定 取消

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:<u>性能数据</u>为定时发送,在对应的右侧编辑框中输入间隔的时间。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:

g置wi	n do ws 事件过滤	条件				X
说明 定的]: 当检测到新的 的服务器。	windows 事件,	,会将符合勾选氛	条件的新事件 以	Syslog 格式发送到排	S F
22	发送应用程序事件	旧志				
	事件级别:	☑信息	☑警告	☑错误	□关键	
<u>لا</u> ك	发送系统事件日志					
	事件级别:	☑信息	☑警告	☑错误	□关键	
<u>لا</u> ك	发送安全事件日志	:				
	事件级别:	☑ 信息 ☑ 审核成功	☑ 警告 ☑ 审核失败	☑错误	□关键	
						-
			确定	取消	添加事件源	

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: "文件內容监视"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。"文件內容监视"是读取文本文件內容,并将內容发送 到日志服务器。启用文件內容监视后,当目标文件的內容新增加一行或多行时,新增的內容 会以Syslog格式发送到日志服务器。

在"Syslog设置"页面下,勾选"<u>发送文件内容至日志服务器</u>",弹出设置界面,如下图所示:

SYSLOG设置发送文本	本文件内容			×
说明: 监视文本文件[持2本文件中录 句谱	内容的变化,当文件内容增加一行 \$***	或多行时,增加的内容会	以 Syslog格式发送到指定的	的服务器。最多支
村が「又日日来,当地	S XHHW ALX .			
□ 文件日寻.				进场中寻
				选择由来
立性 与物。			这个这件中世俗日际五	
文件名称:	*.log		多个 谊 便用 付ち隔井,	χμ. logl. roc
文件格式:	UTF-8 ~			
日志标签:	IIS			
□文件目录:				选择目录
	☑ 包含子目录			
文件名称:	*.log			
文件格式:	UTF-8 ~			
日志标签:	IIS			
□文件目录:				选择目录
	☑ 包含子目录			
文件名称:	*.log			
文件格式:	UTF-8 ~			
日志标签:	IIS			
帮助			确定	取消

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。%f表示使用文件名做标签。

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。