

IMB System 3.6

windows 版本 用户手册

7i24 Information Monitor and Block (IMB) System 3.6 Overview

Abstract

本文档描述 (IMB) System 3.6。本软件和文档是依据许可协议提供的。
有关最新信息，请参见 7i24.Com 主页。

一流信息监控拦截系统 (IMB) System 3.6 是为虚拟主机提供商、空间提供商、ICP 内容提供商而设的信息监控拦截系统。为了解决这些服务提供商的信息管理问题，它集多种功能于一身，让互联网从此告别不受监管的状态，是虚拟主机提供商、空间提供商、ICP 内容提供商的保护神，它从商业的角度保护了这些提供商的自身利益，大大降低了这类提供商的运营风险，让所有用户上传的内容处于可控状态，所有不良内容，影响服务器稳定的内容都无所遁形，运营商不用再担心自己所管理的服务器不稳定，也不用担心服务器里面的内容与政府要求有所冲突，可以完全放心地为最终客户服务。

一流信息监控拦截系统 (IMB) System 3.6 的出现源于国内政府对互联网管理的要求提高，开发小组的成员就深有体验，例如重大政治会议期间，为了防止出现不良信息，大大小小的 ICP,ISP,空间提供商等提心吊胆，让管理人员深夜都加班加点，担心公安部门的电话会打到自己的头上，担心有一天被发文告知自己的服务器有一条法 X 功信息在 BBS 中已出现了一个月却没能及时删除，广东的 j XX 网；就是因为这个原因一纸公文被停办了。

一流信息监控拦截系统 (IMB) System 3.6 同时解决了用户上传的文件的管理问题，例如可以防止用户上传导致系统不稳定的程序(例如江湖、聊天室、电影下载、色情写真)，同时可以自动监控服务器的状态，服务器出现不能访问时可以自动恢复，减轻了管理员的压力，提供了提供商的服务质量。

一流信息监控拦截系统 (IMB) System 3.6 领先的设计理念源于开发小组丰富的实际经验，开发小组的成员管理了各种各样的 24 小时运行的服务器，每台服务器上有大量的各类用户，甚至其中有的服务器的流量达到 500MBPS/S，有些服务器的用户文件数量竟达到 500 万个，正是在这样严酷的条件下，(IMB) System 经受了所有的考验，目前它的 3.6 版本已推出，为用户提供了强劲有效的功能，更为用户带来良好的使用体验。

? 2003 7i24. Com. All rights reserved.

The information contained in this document represents the current view of 7i24.Com the issues discussed as of the date of publication. Because 7i24 must respond to changing market conditions, it should not be interpreted to be a commitment on the part of 7i24.Com, and 7i24.Com cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. 7i24.Com MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Windows NT, Windows 2000, and Windows.Net are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Last Update [2007-1-15](#)

目录 TABLE OF CONTENTS

7i24.com

IMB SYSTEM 3.6	1
7I24 INFORMATION MONITOR AND BLOCK (IMB) SYSTEM 3.6 OVERVIEW	1
1、安装	4
2、IIS 守门员	8
3、首席文件检查官与 IIS 健康检查官	19
4、爱国者智能 COM 组件	31
5、中央控制网站使用说明	33
6、性能报告	37
7、案例研究	40
8、获得技术支持	42
9、如何购买本公司的产品	43

1、安装

为了您能顺利使用本系统的优秀功能，我们强烈建议您在安装系统前请认真阅读以下的安装说明，

1.1、安装的系统要求

操作系统要求：您的服务器可以是以下的操作系统之一：

Windows NT 4.0 安装了 sp6a 及以上的补丁与 .Net 2.0 CLR

Windows 2000 Server 安装了 sp4 及以上的补丁与 .Net 2.0 CLR

Windows 2000 Advance Server 安装了 sp4 及以上的补丁与 .Net 2.0 CLR

Windows Data Center 安装了 sp4 及以上的补丁与 .Net 2.0 CLR

Windows 2003 32 位版本 安装了 sp1 及以上的补丁与 Net 2.0 CLR

Windows 2003 x64 位版本 安装了 sp1 及以上的补丁与 Net 2.0 CLR

所有操作系统在安装软件前都需要先安装好 IIS。

系统盘硬盘空间要求：5M，建议：100M(主要空间用作保存日志用)。

最低配置：CPU PII 400 以上，内存 256M 以上。

1.2、产品下载

商用正式版的软件包请您用正版用户名密码登陆 <http://7i24.com> 网站可以直接下载。

1.3、用户权限

您必须对要安装本产品的计算机具有管理员权限。我们建议您用 Administrator 的用户名登陆您的服务器，下载本产品后再进行安装。

1.4、安装顺序

建议的安装顺序如下：

- A. 首先请安装 .Net CLR
- B. 安全调整
- C. 安装软件运行许可证
- D. 安装一流信息监控拦截系统软件包
- E. **Windows 2003 新内核权限设置的特别说明**

1.5、安装 .Net CLR 与相关补丁：

.Net 2.0 的 *j* 运行环境 *j* CLR(Common Language Runtime)

微软已发布了 .Net 架构的 *j* 运行环境 *j*，所有 .Net 的软件必须安装这个运行环境才能运行的，在安装一流信息监控拦截系统软件包前必须先安装它。请注意，如果您以前通过 Windows update 已安装了 .Net 2.0，则无需要重复安装。

下载地址：(22.4M)

<http://www.microsoft.com/downloads/details.aspx?familyid=0856EACB-4362-4B0D-8EDD-AA B15C5E04F5&displaylang=zh-cn>

1.6、(建议的安全操作：)在 IIS 的全局影射中删除无用的影射

注意，由于 .Net 会自动安装 ASP.Net 的支持，如果您的系统不需要 ASP.Net，请在 IIS 的全局影射中删除相关的影射。

方法如下：打开 Internet 服务管理器 (可以在开始菜单--程序--管理工具中找到)

用鼠标右键点击左栏的计算机图标，选择属性

选择主属性中的"WWW 服务" 点击"编辑"

点击选项卡中的"主目录"

点击"配置"

在应用程序映射中，删除所有您不使用的映射。对一般的服务器来说，保留 .asp,.asa 的映射已足够了，其它除非必要，建议不要保留。

点击"确定"，此时有可能会弹出"继承覆盖"窗口，建议点击"全选",再"确定".

1.7、安装软件运行许可证管理工具

它的安装文件名是：SetupLicense.msi,请双击下载下来的 SetupLicense.msi,按提示一步步进行安装.

1.8、获得运行许可证

安装完成"许可证管理工具"后,可以在"开始菜单--程序; 一流信息监控系统"中找到"软件运行许可证管理"的图标,点击运行这个程序.

输入您的正版软件用户名与密码(如何获得这个用户名与密码请与工作人员联系)

下面的操作请注意!

输入您所安装的服务器的正在使用的公网的 IP 地址.

点击获得许可证,如果是合法的用户,一会儿会提示成功信息的.

如果您输入所有的验证资料都正确，系统但返回了错误的代码，[请将错误代码发给 tec@7i24.com](mailto:tec@7i24.com) 寻求技术支持。

1.9、安装一流信息监控拦截系统

双击下载下来的 infosafe.msi,按提示一步步进行安装，在安装过程中会有一个黑色的窗口弹出来，提示以下内容：

7i24.Com 软件安装平台。(http://7i24.com)

正在安装 IIS 过滤:INFOSAFE...请等待...

PUT Value OK

服务器上运行的是 IIS 6...

下面将自动给 C:\目录增加 IIS_WPG 用户的权限...

如果您选取了否，并且如果网站出现 Service Unavailable 请务必再在开始菜单中装入 IIS，在本选择时选取是，就会正常。

注意设置权限可能要需要五分钟的时间请稍等...

请选择是否现在就增加权限在 C:\下(y 并回车代表是，n 并回车代表否)...

一般情况下，我们建议您输入 y 并回车，软件会自动给 C:\增加它所需要的权限：

对于 Windows 2003，这个权限是 IIS_WPG 用户读与运行的权限。IIS_WPG 是 IIS6 应用程序池的运行用户所在的组。

稍后您会看到以下提示信息：

服务器上运行的是 IIS 6...

为全局删除通配符影射...

PUT Maps Value OK

为标识符是:1015999197 的网站删除通配符影射...

PUT Maps Value OK

为标识符是:1015999198 的网站删除通配符影射...

PUT Maps Value OK

为标识符是:1015999199 的网站删除通配符影射...

提示信息的意思是，软件会先在 IIS 中删除以前版本留下的一流信息监控拦截系统的配置信息。稍后您会看到：

正在为 IIS6 新内核模式作配置，请稍等...

为全局增加通配符影射...

install Maps Value OK

为标识符是:1015999197 的网站增加通配符影射...

install Maps Value OK

为标识符是:1015999198 的网站增加通配符影射...

install Maps Value OK

为标识符是:1015999199 的网站增加通配符影射...

提示信息的意思是，软件自动在 IIS 中添加现在安装的一流信息监控拦截系统的配置信息。

稍后您会看到：

install Maps Value OK

install Restriction Value OK

Create Filter OK

PUT Filter OK

成功安装...

请选择是否现在重新启动 IIS 服务(y 并回车代表是，n 并回车代表否)...

请根据您的情况输入 y 并回车，这样一流信息监控拦截系统中的 IIS 守门员部分会在安装完成后马上生效。否则会在 IIS 下一次启动时才能生效。输入 y 后接着会提示：

正在重新启动 IIS 服务，请稍等，可能需要两分钟的时间...

正在尝试停止...

Internet 服务已成功停止

正在尝试启动...

Internet 已成功重新启动

如果长时间没有反应请按回车。

稍候一会后软件会安装完成。

附注：**IIS6** 支持两种运行模式：工作进程隔离模式(默认模式)与 **IIS5** 隔离模式，如果您在安装本软件后更改了 **IIS6** 的内核模式，请重新运行 "开始菜单--程序\一流信息监控系统"-i 将 IIS 守门员装入 IIS_i。

1.10、Windows 2003 默认内核模式运行权限设置的特别说明

在前面的安装完成后，如果您的 IIS6 是用默认的内核模式运行，如果您的硬盘权限配置不正确，会引起 Service Unavailable 错误。您需要按以下方式正确配置相关的权限：

关键点是：IIS 6 默认使用的工作进程隔离模式需要 IIS_WPG 组对 C:\ 有相关的读的权限，IIS_WPG 组的意义是：该帐户指派了在 Web 服务器上启动和运行工作进程所需的最低权限和用户权限。它相当于 IIS5 中的 IWAM_computername 用户，但权限更低一些。注意，IIS_WPG 并不是 IUSR_computername 用户，因此它和虚拟主机的运行时用户没有关系。给 IIS_WPG 用户授权因而也不会对 FSO 的权限有任何影响。

软件安装时会自动调用 CACLS.EXE 加上 IIS_WPG 对 C:\ 读与运行的权限。如果您的服务器禁止了对 CACLS.EXE 的访问，就会造成自动增加权限失败，因此，如果您禁止了 CACLS.EXE 的访问，先您先允许它，再安装一流信息监控拦截系统。

如果您安装后，出现 Service Unavailable 错误，请在开始中运行，输入 iisreset /stop 这样可以停止 IIS，然后在 "开始菜单--程序--一流信息监控系统"中找到"将 IIS 守门员从 IIS 中卸载"的图标，点击运行这个程序。这样可以先恢复 IIS 的访问，然后再联系我们的技术人员协助您解决权限问题。

2、IIS 守门员

2.1 概述

IIS 守门员智能实时分析所有进出服务器的内容，记录并拦截任何不合法内容，自动生成清晰的报表，并可以通过 web 方式方便地在线检查。

虽然 IIS 守门员可以分析所有的内容，但为了效率，我们建议它只需负责分析拦截动态内容，静态内容应交给文件检查官处理，动态内容往往是即时合成的，例如浏览者提交到虚拟主机用户留言本与 BBS 的内容，这部分内容在未有本软件前是无法检查的，现在可以成功拦截了！国外的反华势力常通过互联网到处发反动信息，由于虚拟主机的用户自行上传 BBS 等程序，服务商无法管理，成为死角，现在有了本软件就再也不用担心了！

从技术角度上来说，IIS 守门员是一个基于 Microsoft IIS 的全局过滤器，安装完成后您可以在 IIS 的全局过滤器中找到它，代号是：INFOSAFE，它具有全局过滤器的特征，注意它只能全局安装。

星外科技在开发时充分考虑了性能上的优化，在处理时充分利用了非同步的 I/O 处理，有效防止了处理大量数据时的阻塞，您完全可以放心的使用在 1000M 网络环境中。

2.2 修改配置文件

IIS 守门员的所有特性由配置文件决定，您可以直接在“开始菜单”；；一流信息监控拦截系统；；管理软件；--“修改配置文件”来打开它，它是位于安装目录中的一个名为 `infosafe.ini` 的文本文件。它的默认安装位置在：C:\Program Files\LIWEIWENSOFTE\iissafe\infosafe.ini，您也可以用任何文本文件编辑器来修改它的。我们建议您修改配置文件前先备份它。

IIS 守门员会在 IIS 每次启动时读取配置文件的信息，因此每次修改配置文件后要重新启动 IIS 才能生效，请参考<2.4 重新启动 IIS>的说明。

配置文件由一节一节的内容组成，有效的变量由；--；为开始。

下面详细说明配置文件的每一项内容：

A. 是否拦截进入服务器中含有关键词的内容

定义：

；--blockin=

默认值：

yes

可选值：

no yes

说明：

此变量决定了是否拦截流入的内容。当后面的配置 **anaintype** 不为 no 时，系统会分析流入服务器的数据，如果含有不允许的内容，当 **blockin=yes** 时，IIS 守门员会执行拦截，阻止数据进入服务器，同时记录对方的 IP 地址，访问地址，时间等信息，IIS 守门员也会马上给对方返回警告信息，格式如下：

一流信息监控系统提醒您：很抱歉，由于您提交的内容中或访问的内容中含有系统不允许的关键词或者您的 IP 受到了访问限制，本次操作无效，系统已记录您的 IP 及您提交的所有数

据。请注意，不要提交任何违反国家规定的内容！本次拦截的相关信息为：法轮！（这些提示信息可以在后面的设置中修改！）

当 **blockin=no** 时，IIS 守门员只记录对方的 IP 地址，访问地址，时间等信息，并不返回警告信息，也不执行拦截。

B. 分析进入服务器的数据

定义：

--anaintype=

默认值：

dgetandpost

可选值：

no all dgetandpost post

说明：

此变量决定了如何分析进入服务器的数据，如果不分析，可以设置为：**no**，如果分析输入数据，可以指定分析的种类，例如是所有数据：（定义为 **all**）或只是动态的 **get** 及 **post** 操作（定义为 **dgetandpost**），一般来说，只有动态的内容才有分析意义的，因此默认值是足够了，除非是特殊要求。其中（**post** 只对 IIS6 有效）（**all** 只对 IIS5 有效）。

当设置为 **dgetandpost** 以下的提交进入服务器的 HTTP 操作会被分析，IIS 守门员会分析；**title=法轮功**；及 POST 里面的内容：

GET /articles/news/today.asp?title=法轮功 HTTP/1.1

POST /articles/news/today.asp HTTP/1.1

但不含动态数据的内容是不会被分析，例如：

GET /articles/news/today.asp HTTP/1.1

对流入的内容启用分级拦截

C. 一级关键词（肯定拦截的关键词）

定义：

--speckey=

默认值：

大法@法轮@李洪志@大纪元@真善忍@六合@阴唇@肉棍@阴户@强奸@淫靡@淫水@阴茎@阴蒂@乱伦@手淫@做鸡@六四事件@江泽民@胡锦涛@罗干@朱镕基@李鹏@江主席@温家宝

可选值：

可以添加您要拦截的关键词，用；@；分隔开，也可以不指定任何内容，设置此值为空

说明：

此变量定义敏感的关键词，用@分隔开，您可以加入自己所要监控的关键字，关键词决定了 IIS 守门员所关注的内容，任何进入或流出的内容如果含有任何一个关键词都会被记录，是否拦截将取决于<--blockin=>这两个变量。您可以根据自己的需要，随时调整关键词，注意每次调整后要重启 IIS 才能生效的。IIS 守门员分析关键词时并不是一种硬模式，它是智能的，请参考<--delcon=>的定义，它决定了如何判断内容中是否含有关键词。

D. 二级关键词（只记录到日志而不拦截的关键词）

定义：

--Watchernotaccept=

默认值:

@新生网@新唐人@口交@天安门@共产主义@共产党@中共@反共@台独@达赖@反革命@反华@盗取
@绕过封锁@新疆独立@西藏独立@民运分子@打倒@推翻@多党执政@专制@国民党@成人小说@成
人电影@裸体@激情图片@激情电影@

说明:

对流入的内含有上面的关键词,当一级关键词 **speckey** 不为空时,只记录到日志中而不拦截。
当 **speckey** 为空时,且 **blockin=yes** 时,将执行拦截(本变量加上 **speckey** 的总长度必须小于 1K)。从 3.0 版本起分开一级与二级关键词的目标是,不采用一刀切的方法来处理流入服务器的内容,对于一级关键词有可能引起严重的后果的,例如邪教内容,应该马上拦截,对于一些中性内容共产党这样的词,可以将它放在二级关键词中,只记录而不拦截。

E. 是否拦截 SQL 关键词

定义:

--blocksql=

默认值:

yes

可选值:

no yes

说明:

此变量决定了是否拦截流入的含入 SQL 注入的内容。

当 **blocksql=no** 时, IIS 守门员只记录对方的 IP 地址, 访问地址, 时间等信息, 并不返回警告信息, 也不执行拦截。

F. 针对 HTTP 的 GET 操作中所分析的 SQL 关键词

定义:

-- SQLkeyGet=

默认值:

'@ or @ or@or @ and @ and@and @;and @;and @exec @exec @backup @backup
 @char@drop table@drop table@delete from@delete from@insert @insert
 @select @select @update @update @net user@net user@net localgroup@net
 localgroup@xp_cmdshell

可选值:

可以添加您所面要的关键词, 用;@;分隔开, 注意关键词必须小写。

说明:

此变量定义敏感的关键词, 用@分隔开, 您可以加入自己所要监控的关键字, 关键词决定了 IIS 守门员所关注的 HTTP 协议中的 GET 内容, 任何进入或流出的内容如果含有任何一个关键词都会被记录, 是否拦截将取决于<--blocksql=>这两个变量。您可以根据自己的需要, 随时调整关键词, 注意每次调整后要重启 IIS 才能生效的。

G. 针对 HTTP 的 POST 操作中所分析的 SQL 关键词

定义:

-- SQLkey=

默认值:

```
--SQLkey= or @ or@or @ and@and @;and @;and @exec @exec @backup @backup
@char@drop table@drop table@delete from@delete from@insert @insert
@select @select @update @update @net user@net user@net localgroup@net
localgroup@xp_cmdshell
```

可选值:

可以添加您所面要的关键词, 用;@;分隔开, 注意关键词必须小写。

说明:

此变量定义敏感的关键词, 用@分隔开, 您可以加入自己所要监控的关键字, 关键词决定了 IIS 守门员所关注的 HTTP 协议中的 POST 内容, 任何进入或流出的内容如果含有任何一个关键词都会被记录, 是否拦截将取决于<--blocksq1=>这两个变量。您可以根据自己的需要, 随时调整关键词, 注意每次调整后要重启 IIS 才能生效的。

H. 只对以下的本地的虚拟主机启用 SQL 拦截功能

定义:

```
--superonlyhost=
```

默认值:

空

说明:

当<--blocksq1=yes>时, 可以通过;--superonlyhost=来指定那一些域名才启用拦截功能, 示例: ;-- superonlyhost=www.abc.com|abc.com|, 注意域名必须小写。

H. 对以下的本地的虚拟主机不启用 SQL 拦截功能

定义:

```
--superfreehost=
```

默认值:

空

说明:

当<--blocksq1=yes>时, 可以通过;-- superfreehost=来指定那一些域名不启用拦截功能, 示例: ;-- superfreehost=www.abc.com|abc.com|, 注意域名必须小写。当 superonlyhost 和 superfreehost 都是空值时, 所有域名都启用些功能。

I. 超过以下大小的 POST 数据将被忽略(仅对 Windows 2003 IIS 默认内核模式有效)

定义:

```
--MaxbodyLen=
```

默认值:

512000

可选值:

256000

1024000

2048000

说明:

有时候, 访问者会通过网页 POST 上传一个大的文件(例如上传图片), 显然, 这些非常大的数据是无需分析的, 因此, 通过设置本值来忽略这类内容。超过指定大小的 POST 数据将忽略, 不作分析(单位是字节)。

J. IP 限制功能

定义:

--blockip=

默认值:

no (不启用本功能)

可选值:

no all post

说明:

IP 限制功能, 本系统从 2.1 版本起支持 IP 限制功能, 由于网上发布的大部分的反动信息, 如邪教等内容, 通常是从台湾或美国发布的, 本系统内建了一个完整的中国国内的 IP 地址表, 可以让服务器只接受国内的 IP 发布的信息。定义值可以是: no,all,post。no 表示不启用本功能, all 表示只能是国内 IP 才能访问本服务器, post 表示只允许国内 IP 地址在论坛或留言本发表。这项功能对抗反华组织是非常有效的!

K. IP 限制功能(添加另外允许的 IP 地址段)

定义:

--addip=

默认值:

127.0|192.168|10.1|

说明:

添加除了系统内建的国内 IP 段外的另外允许的 IP 地址段, 可以是多个段, 用|分隔, 例如 71.2|代表从 71.2.0.0-71.2.255.255 共 65025 个 IP 都被允许。

L. IP 限制功能(添加另外禁止的 IP 地址段)

定义:

--addblockip=

默认值:

127.0|192.168|10.1|

说明:

添加另外被禁止的 IP 地址段, 可以是多个段, 用|分隔, 例如 71.2|代表从 71.2.0.0-71.2.255.255 共 65025 个 IP 都被禁止。

;添加另外另外禁止的 IP 地址:

M. 是否记录相关流入服务器被拦截的信息到日志中

定义:

--logbip=

默认值:

yes

可选值:

no yes

说明:

此变量决定了是否在日志中记录流入服务器的内容中被拦截或被处理的信息。

N. 是否拦截输出服务器中含有关键词的内容

定义:

--blockout=

默认值:

no

可选值:

no yes

说明:

此变量决定了是否拦截输出的内容。当后面的 **anaout type** 不为 no 时, 系统会分析输出服务器的数据, 如果含有不允许的内容, 当 **blockout=yes** 时, IIS 守门员会执行拦截, 阻止数据发送给对方, 同时记录对方的 I P 地址, 访问地址, 时间等信息, IIS 守门员也会马上给对方返回警告信息, 同时, 会提醒用户是否关闭浏览器, 提示信息的格式如下:

一流信息监控系统提醒您: 很抱歉, 由于您提交的内容中或访问的内容中含有系统不允许的关键词或者您的 IP 受到了访问限制, 本次操作无效, 系统已记录您的 IP 及您提交的所有数据。请注意, 不要提交任何违反国家规定的内容! 本次拦截的相关信息为: 法轮! (这些提示信息可以在后面的设置中修改!)

当 **blockout=no** 时, IIS 守门员只记录对方的 I P 地址, 访问地址, 时间等信息, 并不返回警告信息。

O. 流出服务器的内容所拦截的关键词

定义:

--Watchernotacceptout=

默认值:

大法@法轮@新生网@新唐人@肉棍@阴户@强奸@阴唇@淫靡@淫水@阴茎@阴蒂@乱伦@手淫@做鸡@口交@李洪志@大纪元@真善忍@六合@天安门@共产主义@共产党@六四事件@江泽民@中共@反共@台独@达赖@反革命@反华@盗取@绕过封锁@新疆独立@西藏独立@胡锦涛@罗干@朱镕基@李鹏@民运分子@打倒@推翻@多党执政@专制@江主席@国民党@胡锦涛@温家宝@成人小说@成人电影@裸体@激情图片@激情电影@

说明:

此变量定义对流出服务器的内容所关注的敏感的关键词, 用@分隔开, 您可以加入自己所要监控的关键字, 关键词决定了 IIS 守门员所关注的内容, 任何进入或流出的内容如果含有任何一个关键词都会被记录, 是否拦截将取决于<--blockout=>这两个变量。您可以根据自己的需要, 随时调整关键词, 注意每次调整后要重启 IIS 才能生效的。IIS 守门员分析关键词时并不是一种硬模式, 它是智能的, 请参考<--delcon=>的定义, 它决定了如何判断内容中是否含有关键词。

P. 流出服务器的内容只记录不拦截的关键词

定义:

--Watchernotacceptout2=

默认值:

靖国神社@

说明:

此变量定义对流出服务器的内容所关注的敏感的关键词, 用@分隔开, 您可以加入自己所要监控的关键字, 关键词决定了 IIS 守门员所关注的内容, 任何流出的内容如果含有任何一个

关键词都会被记录，但不会拦截。

Q. 是否分析服务器所有 **text/html** 输出的数据

定义：

--anaouttype=

默认值：

onlydy

可选值：

no **alltext** **onlydy**

说明：

此变量决定了是否分析流出的数据的方式。当 **anaouttype=no** 时并不分析流出的数据。当 **anaouttype=alltext** 时服务器将分析所有流出的文本类内容，我们不建议设置为 **alltext**，因为对速度有一定的影响，**IIS 守门员从设计上应该只分析动态内容。**

当 **anaouttype=onlydy** 时，特定文件类型分析才生效，< **R.** 只分析指定文件结尾的文件> 才会起作用的。一般地，保持默认的 **onlydy** 值就行了。如果您有非常严格的要求，也可设置为 **alltext**，但由于系统需要大量的计算，我们仅建议在您的服务器流量不大或有强大的性能的才启用这个选项。例如流量在 30G/天,100000IP/天以下，CPU 在 2.0G 以上，您可以监控系统的消耗来决定是否使用这个选项。3.6 版本的 IIS 守门员已优化了 **alltext** 功能，现在起您可以放心使用它了。

R. 只分析指定文件结尾的文件

定义：

--anaoutdytype=

默认值：

.asp|.aspx|.php|

可选值：

.asp|.aspx|.jsp|.php|.htm|.html|.txt|

说明：

此变量决定了当< **L.** 是否分析服务器所有 **text/html** 输出的数据>的值 **anaouttype=onlydy** 时，系统将分析哪些类型的文件。您可以输入自己需要类型，如动态输出文件 **asp,aspx** 等，用|作分隔，如果您的服务器只支持 ASP，可以设为我们的建议值：**.asp|.aspx**，这种情况下。IIS 守门员将有最高的处理速度，其它类型的文件可以交给| 首席文件检查官| 来检查。

S. 是否记录相关**流出**服务器被拦截的信息到日志中

定义：

--logout=

默认值：

yes

可选值：

no **yes**

说明：

此变量决定了是否在日志中记录流出服务器的内容中被拦截或被处理的信息。

T. 修改拦截时的提示信息(大小在 2K 以内) (3.0 版本新增功能)

定义:

--blockinfo=

默认值:

一流信息监控系统提醒您: 很抱歉, 由于您提交的内容中或访问的内容中含有系统不允许的关键词或者您的 IP 受到了访问限制, 本次操作无效, 系统已记录您的 IP 及您提交的所有数据。请注意, 不要提交任何违反国家规定的内容! 本次拦截的相关信息为:

可选值:

您可以修改为您自己定义的内容!

U. 修改拦截时的提示信息对应的 URL 网址 (3.0 版本新增功能)

定义:

--blockinfourl=

默认值:

<http://7i24.com/safe/>

可选值:

您可以修改为您自己定义的网址!

V. 指定不启用拦截功能的虚拟主机

定义:

--freehost=

默认值: (为空值)

说明:

一些虚拟主机提供商的服务器上运行着政府网站, 对于这些网站, 一般是无需处理的, 本功能是可以特别指定那些虚拟主机不拦截。例如对 www.abc.com 与 abc.com 这两个虚拟主机不拦截, 可以修改的配置为 **--freehost=www.abc.com|abc.com|**

W. 拦截所有 Gzip 加密的信息: (3.6 版本新增功能)

定义:

--blockgzip=

默认值: no

no

可选值:

no yes

说明:

对于 PHP 的网站, 在启用 PHP 自带的 GZIP 压缩的情况下, 文字内容就会无法分析, 为了防止这类网站发布不良内容而无法检查, 您可以启用本功能, 一旦本功能被启动, 所有 PHP 类的 GZIP 站将无法运行, 这类虚拟主机只能自己关闭程序 GZIP 后才能运行。

X. 网址中含有以下内容, 无条件拦截: (3.6 版本新增功能)

定义:

--blockdir=

默认值: (为空值)

no

说明:

本功能为网址拦截, 对于这样的一个网址 <http://xxxx.xxx.com/bbs/index.asp>, <http://xxxx.xxx.com/forumdisplay.php>, 如您要拦截这样的网址访问, 您可以设置;--blockdir=/bbs/@forumdisplay.php@

Y. 网址中含有以下内容, 无条件不拦截: (3.6 版本新增功能)

定义:

;--freedir=

默认值: (为空值)

no

说明:

本功能允许设置指定的网址不拦截, 对于这样的 一个 网址 <http://xxxx.xxx.com/adm/index.asp>, <http://xxxx.xxx.com/admincp.php>, 如您不想拦截这样的网址, 您可以设置;--freedir=admincp.php@/admin/@

Z. 拦截摘要中如果包含这样的词就不拦截, 用@分开多个词(3.6 版本新增功能)

定义:

;--freekey=

默认值: (为空值)

no

说明:

本功能用来解决误拦截的问题, 如一篇文章中含有;安装 24 口交换机;的内容, 会被软件认为是含有; 口交; 这个关键词而被拦截, 因此, 您可以设置;--freekey=口交换机@就可以防止误拦截这个内容了。

ZZ. 分析特点

定义:

;--delcon=

默认值:

AI

可选值:

no delnotnormal delnotchinese AI

说明:

为了有最好的监控效果, 软件设计了几种可选的分析方式: no(代表不进行特殊处理), delnotnormal(删除空格, 忽略大小写后再分析), delnotchinese(删除所有非中文字符后再分析, 此选项在关键词为全部是中文时可以提高识别率), AI(智能分析, 这是 2.15 版本后的新功能)。

对于以下的一段内容:

xxxx 法 轮 功 xxxx

当关键词有中; 法轮功; 这个词, 如果您设置 delcon=no, 这段内容是合法的, 因为原文中

有空格，因此不会被记录，也不会被拦截，如果您设置 delcon= delnotnormal 或 delcon= delnotchinese 或 delcon= delnotchinese=AI 时，这段内容是非法的，它会被记录，也会被拦截。对于以下的一段内容：

xxxx 法\$\$\$\$\$dfdf\$\$\$\$\$gsdfg\$\$\$\$\$轮\$\$tgfg\$\$\$\$\$e\$\$\$\$\$功 xxxx

当关键词有中j 法轮功j 这个词，只有设置 delcon= delnotchinese 或 AI 时，这段内容才是非法的，它才会被记录，也会被拦截。在这种设置下，任何被分隔开的中文内容一样会被识别。当设置为 AI 时，软件会进行全面的分析，这种情况下，软件的识别率是最高的。如果您的关键词中包含有类似这样的：j fa 轮功j 的关键词，请设置成 AI 或 delnotnural 才能处理。关键词中不能含有特殊符号，例如：j.j，如果您想拦截jminghui.orgj 这样的内容，可以将关键词直接设置成jminghuiorgj。您可以根据需要自行添加或删除关键词。

2.3 查看监控的日志文件

可以用以下方式在线访问日志：

<http://服务器任何一个正在运行虚拟主机的域名/infosafe/访问密码>

访问密码及登陆密码可以在"一流信息监控拦截系统"中的"管理软件"中直接修改，重启 IIS 后就会生效。

日志文件是位于安装目录中的一个名为 infosafelog.htm 的文本文件。它的默认位置在：

C:\Program Files\LIWEIWENSOFT\iissafe\log\infosafelog.htm,

示例的监控的日志文件如下：

●一流信息安全监控系统，当前版本：3.5 商用正式版

当前的系统设置：
◇分析流入服务器的数据：分析流入的必要动态内容 [拦截流入含有关键词的内容]
◇分析流出服务器的数据：只分析指定结尾的文件的流出内容：.asp|.aspx|.php| [不拦截流出含有关键词的内容]
◇分析特点：智能分析 [关键词全部是中文 (流入)] [关键词全部是中文 (流出)]
◇启用了SQL防注入功能：GET部分：'@ or @ or@or @ and @ and@and @;and @;and @exec @exec @backup @backup @char@drop table@drop table@delete from@delete from@insert @insert @select @select @update @update @net user@net user@net localgroup@net localgroup@xp_cmdshell@
POST部分： or @ or@or @ and@and @;and @;and @exec @exec @backup @backup @char@drop table@drop table@delete from@delete from@insert @insert @select @select @update @update @net user@net user@net localgroup@net localgroup@xp_cmdshell@
启动信息：
◇拦截关键词 (流入)：大法@法轮@李洪志@大纪元@真善忍@新唐人@六合@阴唇@肉棍@阴尸@强奸@淫靡@淫水@阴茎@阴蒂@乱伦@手淫@做鸡@六四事件@江泽民@胡锦涛@罗干@朱镕基@李鹏@江主席@温家宝@迷药@迷魂药
◇只记录不拦截的关键词的设置 (流入)： @新生网@口交@天安门@共产主义@共产党@中共@反共@台独@达赖@反革命@反华@盗取@绕过封锁@新疆独立@西藏独立@民运分子@打倒@推翻@多党执政@专制@国民党@成人小说@成人电影@裸体@激情图片@激情电影@
◇拦截关键词的设置 (流出)：大法@法轮@新生网@新唐人@肉棍@阴尸@强奸@阴唇@淫靡@淫水@阴茎@阴蒂@乱伦@手淫@做鸡@口交@李洪志@大纪元@真善忍@六合@天安门@共产主义@共产党@六四事件@江泽民@中共@反共@台独@达赖@反革命@反华@盗取@绕过封锁@新疆独立@西藏独立@胡锦涛@罗干@朱镕基@李鹏@民运分子@打倒@推翻@多党执政@专制@江主席@国民党@胡锦涛@温家宝@成人小说@成人电影@裸体@激情图片@激情电影@迷药@迷魂药
◇只记录不拦截关键词的设置 (流出)：台湾@马英九@
◇IP限制：不启用IP限制功能 [记录被拦截的IP]
◇不拦截的虚拟主机：

2007-01-13 13:45:40 成功启动 清空日志 (Web访问时才有效) 静态文件及图片监控日志>>

时间	IP地址	分类	操作	访问的网址	关键词	找到的相关内容摘要
2007-01-13 19:10:57	127.0.0.1	[out]	[GET]	http://127.0.0.1:8080/addini.asp	[大法]	以加入自己所要监控的关键词含有以下的词时当时将执行拦截大法法轮李洪志大纪元真善忍新唐人六合阴唇肉棍
2007-01-13 19:10:57	127.0.0.1	[out]	[GET]	http://127.0.0.1:8080/addini.asp	[中共]	膊 族中共反共台独达赖反革命反华盗取绕过封锁新疆独立西藏独立民运分子打倒推翻多党执政专制国民党成人小?/td>

系统记录了以下内容：

时间：事件发生的时间，是服务器的时间，GMT 第八时区（中国）的时间。

IP 地址：指的是访问者的 IP 地址。

分类: [in]表示此访问者提交的内容被分析有含有关键词, [out]表示从服务器流出的内容被分析有含有关键词。

操作: [GET]表示访问者是通过 HTTP 命令的 GET 方式来与服务器交互的, [POST]表示访问者是通过 HTTP 命令的 POST 方式来与服务器交互的, 往往提交入服务器的数据, 例如 B B S, 是通过 POST 的方式进行的, 您可以清晰看到它的操作方式。

访问的网址: 指的是访问者所访问的网址。

关键词: IIS 守门员分析出流入或流出的数据中含有的关键词。

相关的内容摘要: 为了方便管理员分析, IIS 守门员将关键词附近的内容摘录了下来, 让管理员判断它是否合法。

[执行拦截]: 软件执行了拦截这次操作。这由 **blockin=yes** 及 **blockout=yes** 所定义。

2.4 重新启动 IIS

每次修改配置文件后, 您可以通过在"开始菜单"中的"IIS 守门员"中的"重新启动 IIS"来使改动生效。

您也可以打开 Internet 服务管理器 (可以在开始菜单--程序--管理工具中找到), 用鼠标右键点击左栏的计算机图标, 选择 **重新启动 IIS** 并 **确定** 后来启动 IIS。

请注意! 重新启动 IIS 会暂时造成您的服务器两分钟不能访问! 如果一次重启 IIS 失败, 可以再次重新启动它。

2.5 错误处理

注意软件需要获得运行许可证后才能正常加载的。因此请确保您已获得了有效的运行许可证。

- A. 如果监控的日志文件在成功安装后, 并且重新启动 IIS 后仍然是空白, 请检查您是否获得了有效的运行许可证。
- B. 如果已获得了有效的运行许可证, 以前也曾成功启动过, 请检查您的 IP 是否变更, 或您的网络是否连通, 因为一个运行许可证只能绑定在一个 IP 上的。
- C. 如果您修改配置文件后软件就无法启动, 表明您修改的一些重要参数出错了, 我们建议您恢复到原来的设置, 再重新启动 IIS。
- D. 任何时候您都可以检查软件是否正确加载, 您也可以打开 Internet 服务管理器 (可以在开始菜单--程序--管理工具中找到), 用鼠标右键点击左栏的计算机图标, 选择属性, 选择 **网站** (注意是全局网站, 不是单个网站), 再点击选项卡中的"ISAPI 筛选器", 看看最下面的一个 **INFOSAFE**, 如果它已正确加载, 应该有一个绿色的向上的箭头在它的前面, 如果它没有成功加载, 会是一个红色的向下的箭头。
- E. 对于只有日志但没有拦截的情况, 请您检查是否启用了拦截功能, 也可以检查有没有成功加载拦截模块, 请点击 IIS6 中, 其中一个网站的属性, 点主目录选项卡, 点配置, 正常情况下, 您可以在 **通配符影射** 中, 看到 **INFOSAFE** 的信息。
- F. 如果软件成功加载, 但没有分析出任何内容, 请检查您的配置文件是否正确。

3、首席文件检查官与 IIS 健康检查官

3.1 概述

全国首创的文件监控功能，将政治或黄色问题完美解决！此功能是空间提供商或 ICP 为了配合通信管理局、公安部门对使用服务器的用户进行关键字监控，无论是通过 FTP 方式上传或 web 方式上传的文件都可以准确监控，将不法用户的行为记录在案，同时可以在线检查，让您高枕无忧。

它由以下部分组成：

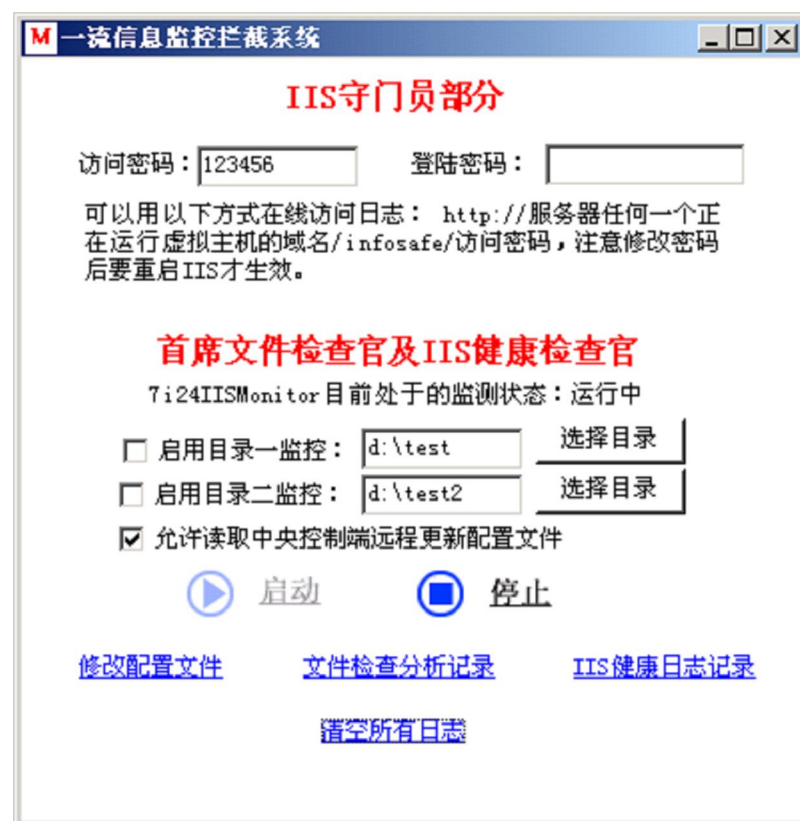
[首席文件检查官]负责监控用户上传的静态文件内容及**图片**/SWF 视频等内容，同时可以阻止用户上传影响稳定的程序，例如电影文件，江湖等游戏。

[IIS 健康检查]随时监控系统的状态，可以让网管不再需要 24 小时值班了！

本软件是基于 Microsoft .Net2.0 架构的软件，它需要 .Net 2.0 CLR 才能运行的。

3.2 管理与设置

安装完成后的，您可以在"开始菜单"中的"一流信息监控拦截系统"中的"管理软件"来打开它的管理程序，程序的界面如下：



安装完成后，默认地，它会处于停止状态的。请先修改它的配置文件符合您的服务器的要求，如何修改请参考<3.3 配置文件> 一节，修改完成后可以点击启动按钮，启动"首席文件检查官与 IIS 健康检查官"，注意，"首席文件检查官与 IIS 健康检查官"会每次在 windows 启动时自动加载的。

每次修改配置文件，请停止"首席文件检查官与 IIS 健康检查官"后，再启动它，这样您的修改才会生效的。

3.3 配置文件

"首席文件检查官与 IIS 健康检查官"的所有特性由配置文件决定，您可以 管理与设置；修改检查官的配置文件；来打开它，它是位于安装目录中的一个名为 `infosafe.ini` 的文本文件。它的默认安装位置在：

`C:\Program Files\LIWEI WENSOFT\iisafe\infosafe.ini`，

您也可以用任何文本文件编辑器来修改它的。我们建议您修改配置文件前先备份它。

"首席文件检查官与 IIS 健康检查官"会在每次启动时读取配置文件的信息，因此每次修改配置文件后要重新启动它才能生效。注意 **2.1** 版本后，首席文件检查官会在您启动本软件后自动等待 **20** 秒才正式进入启动状态。

配置文件由一节一节的内容组成，有效的变量由 `；--；` 为开始。下面详细说明配置文件的每一项内容：

文件监控部分功能的配置：

此功能是一般的 ICP 为了配合通信管理局或公安部门对使用服务器的用户进行关键字监控，无论是通过 FTP 方式上传或 web 方式上传的文件都可以准确监控，将不法用户的行为记录在案，同时可以在线检查，防止有非法内容。

A. 文件监控功能所分析的文件类型

定义：

；--Watchertype=

默认值：

`.htm|.html|.asp|.aspx|.jsp|.php|.txt|.js|.log|` 或 * 代表全部类型

可选值：

您可以添加新的文件类型，或减少一些没有必要的类型。

说明：

此变量决定了文件监控功能所分析的文件类型，这由文件的结尾来决定的，例如网页文件可以由以下来定义：`.htm|`，您可以根据自己的需要来调整。

B. 文件监控功能所分析的文件的大小上限

定义：(单位是 byte，字节)

；--Watcheranali m=

默认值：(100k)

102400

说明：

此变量决定了文件监控功能所分析的文件的大小上限，如果一个文件的大小大于这个值，它将不会被分析，这个值的意义在于，我们可以指定文件监控功能例如 `.asp|` 这类型文件，有一些 BBS，所用的小型 ACCESS 数据库，为了安全，也把 ACCESS 数据库改为 `.asp` 结尾，如果未定义本值，文件监控功能将分析 ACCESS 数据库，这种分析是没有意义的，因为数据已加密，同时会消耗大量的资源，ACCESS 数据库的大小通常比较大，因此定义本值来防止分析 ACCESS 数据库。您不必担心这些内容会被监控漏掉，它由 IIS 守门员来最后把关的。

C. 指定的目录允许最大的上传的文件

定义: (单位是 byte, 字节)

--WatcherLimbig=

默认值: (1000M)

102400000

说明:

文件监控功能将监控指定目录, 如果发现任何试图写入本目录的文件, 例如是用户上传的文件的大小超过了上面定义的值, 此文件将被删除, 此功能可以有效防止用户上传侵权的电影文件, 音乐文件等。在没有这个功能前, 空间提供商常为用户上传上百 M 的 MPEG 电影而头痛, 它会令到空间提供商的服务器不胜重荷的, 现在您再也不用提心了。

C. 增强模块功能: 是否处理数据库文件 (.mdb, .asp, .asa) (yes 或 no) (no 代表就算 mdb 等文件超过上限都不处理)

定义:

--WatcherMDB=

默认值:

no

可选值:

no yes

说明:

有一些类型的文件, 例如 ACCESS 数据库, 有些用户希望无论它的大小如何都不处理它, 本功能让您可以选择对这类较特别的文件 (.mdb, .asp, .asa), 是否进行处理。

D. 增强模块功能: 是否对超过了最大允许上传文件上限的 .mdb, .asp, .asa 这类 ASP 数据库文件不直接删除而只是重新命名

定义:

--WatcherAUTORENAME=

默认值:

yes

可选值:

no yes

说明:

(注意只有当 --WatcherMDB=yes 本选项才有效) 对于超过 WatcherLimbig= 大小的文件, 您可以让系统直接删除它, 但有一些类型的文件, 例如 ACCESS 数据库, 如果直接删除用户上传的内容, 会引起抗议, 本功能让您可以选择对这类较特别的文件, 采用重命名的形式, 让它暂时不法使用。最典型的问题的, 一些用户在虚拟主机有采用自行上传的 BBS, 它采用 ASP+ACCESS 数据库的形式来运行, 一些热门的 BBS 有几千个贴子, 结果是 ACCESS 数据库变得很大, 有可能有 10M, 会严重影响服务器的性能, 这儿定义的值, 让系统自动判断, 当 ACCESS 数据库大于 WatcherLimbig= 的值时, 并 WatcherAUTORENAME=yes 时, ACCESS 数据库将自动被重命名为j 由于超出上限被自动重命名 XXXXX.mdbj, 防止 ACCESS 数据库过大影响服务器的速度, 保障了空间提供商的利益。空间提供商可以要求用户压缩这个 ACCESS 数据库, 提供整体的速度。

E. 只记录不删除的关键词

定义:

--Watchernotaccept=

默认值:

肉棍@阴户@强奸@阴唇@淫靡@淫水@阴茎@阴蒂@乱伦@手淫@嫖@做鸡@口交@法轮功@法轮大法@李洪志@大法弟子@大纪元@真善忍@六合@天安门@共产主义@共产党@六四事件@江泽民@中共@反共@台独@达赖@反革命@反华@盗取@绕过封锁@新疆独立@西藏独立@胡锦涛@罗干@朱镕基@李鹏@民运分子@打倒@推翻@多党执政@专制@江主席@国民党@十六大@第十六届

说明:

此变量定义敏感的关键词或字,用@分隔开,您可以加入自己所要监控的关键字,关键词决定了首席文件检查官所关注的内容,任何在试图写入指定目录的特定类型的文件(由<D.文件监控功能所分析的文件类型所定义>),如果它的内容含有任何一个关键词都会被记录。您可以根据自己的需要,随时调整关键词,注意每次调整后要重启本软件才能生效的。首席文件检查官分析关键词时并不是一种硬模式,它是智能的,请参考<--delcon=>的定义,它决定了如何判断内容中是否含有关键词。

注意!您可以加入;聊天;与;江湖;这些关键词来判断用户是否上传了这类影响服务器稳定的程序的,大大方便了空间提供商的管理。

E. 记录并且删除的关键词

定义:

-- speckeyA=

默认值:

@Shell.Application@WScript.Shell@093ff999@f935dc26@0d43fe01@

说明:

此变量定义敏感的关键词或字,用@分隔开,您可以加入自己所要监控的关键字,关键词决定了首席文件检查官所关注的内容,任何在试图写入指定目录的特定类型的文件(由<D.文件监控功能所分析的文件类型所定义>),如果它的内容含有任何一个关键词都会被记录**并且删除**。您可以根据自己的需要,随时调整关键词,注意每次调整后要重启本软件才能生效的。首席文件检查官分析关键词时并不是一种硬模式,它是智能的,请参考<--delcon=>的定义,它决定了如何判断内容中是否含有关键词。(对付网页木马最有效!注意所有关键词中不应该含用特殊字符应该只是字母及数字)。

F. 分析特点

定义:

--delcon=

默认值:

smart

可选值:

no smart

说明:

为了有最好的监控效果,软件设计了几种可选的分析方式: no(代表不进行特殊处理), smart (删除所有非中文字符后再分析,此选项在关键词为全部是中文时可以极大地提高识别率)。

对于以下的一段内容:

xxxx 法\$\$\$\$\$dfdf\$\$\$fgsdfg\$\$\$\$\$\$轮\$\$tgfg\$\$\$e\$\$\$\$\$\$\$\$\$\$\$功 xxxx

当关键词有中*法轮功*这个词，只有设置 **delcon=smart** 时，这段内容才是非法的，它才会被记录。在这种设置下，任何被分隔开的中文内容一样会被识别。

G. 删除以下的格式的文件

定义：

-- Deltype=

默认值：

空

可选值：

.rm|.wmv|.rmvb|

说明：

为了有防止用户上传电影或下载类内容占用资源，可以启用本功能，只要用户一上传此类格式的文件，马上就会被删除。

H. 删除以下的格式的文件

定义：

-- Listtype=

默认值：

.htm|.txt|.jpg|.gif|.png|.swf|.rm|.wmv|.rmvb|.wma|

可选值：

任何您需要关注的格式

说明：

为了有防止用户上传色情图片，请在这个指定所有的图片格式，文件检查官会每天生成这些文件的更新情况，您可以在 Web 界面上，远程快速查看这台服务器上所有今天更新的图片等内容，谁上传了不良图片可以一目了然。

I. 日志的保存间隔

定义：

--Logtype=

默认值：

d 代表每天一个文件

可选值：

每月一个文件为 m,每小时一个文件为 h

说明：

日志的间隔一般不需要调整。

J. 扫描历史功能

本功能可以扫描安装一流信息监控系统前的硬盘上的旧内容(静态内容)，检查是否存在不良信息，您可以在首次使用软件时将旧的内容让软件在后台扫描一次。

注意，为了令到对系统的影响降到最低，对于一台有上百万的文件，会需要 3-10 小时，请在系统空闲时间进行，请在这段时间内不要重启服务器，扫描结束时会产生结束记录，您就可以关闭本功能，以免下次再次扫描。本功能生成的扫描日志的文件保存位置在安装目录的 log 目录中，文件名为：scanlog.htm，具体的设置可以直接参考配置文件上的说明。

J.

IIS 健康检查官的配置:

i IIS 健康检查官i 将自动定时访问指定的 URL，判断 IIS 是否正常，如果不正常，将自动执行恢复命令，令到 IIS 恢复了良好的状态。

A.每次启动后延迟指定的时间后才开始监控

定义: (单位是 ms,毫秒)

;-StartDelaytime=

默认值: (600 秒, 10 分钟)

600000

说明:

因为有一些服务器在启动后要几分钟才能完成数据库重新启动，在此期间，IIS 是不正常的，因此i IIS 健康检查官i 需要等待一些时间后才进行检查，我们建议延迟时间为 3 分钟以上。

B.时间间隔

定义:

;-IniInterval=

默认值: (180 秒, 3 分钟), 就是说每三分钟检查一次 IIS 是否正常。

180000

说明:

此变量指明每隔多少的时间就进行访问指定页面,i IIS 健康检查官i 将根据这个时间间隔来定时访问指定的 URL。

C.出错后的延迟时间

定义:

;-IniIntervalnext=

默认值: (1200 秒, 20 分钟)

1200000

说明:

i IIS 健康检查官i 检查出错误，将执行指定的恢复操作，然后过了由 IniIntervalnext=所定义的时间后再次检查 IIS 是否正常。

D.监控的 URL

定义:

**;\$7i24IISMonitorCompare= 7i24IISMonitorUrl= 7i24IISMonitorValue=
7i24IISMonitorCommand=**

默认值: (仅为测试用, 请修改为您的服务器的值)

\$7i24IISMonitorCompare>equals 7i24IISMonitorUrl=http://localhost/iistest.asp

7i24IISMonitorValue=ok 7i24IISMonitorCommand=NULL

说明:

这儿定义的是i IIS 健康检查官i 定时访问的 URL 与恢复命令。每一个变量的定义如下:

比较格式: 可选值: "equals" (是否相等的意思) indexof" (是否包含)

7i24IISMonitorCompare=

监视 URL

7i24IISMonitorUrl=

返回值

7i24IISMonitorValue=

出错所执行的命令

7i24IISMonitorCommand=

i IIS 健康检查官 i 将会用 IniIntervalnext= 所指定的时间间隔用 http 的方式访问 i 7i24IISMonitorUrl=i 所定义的 URL, 可以是本服务器的 URL, 也可以是别的服务器的 URL。然后会自动将访问返回的结果用 i 7i24IISMonitorCompare=i 所定义的方式进行比较, 比较的内容由 i 7i24IISMonitorValue=i 所定义。例如你可以定义是 i OK i, 如果比较最后的结果出现错误, 例如 IIS 出现 500 错误, 403 等错误, 本程式将自动执行由 7i24IISMonitorCommand= 所定义的程序, 例如重新启动 IIS 的 IISRESET, 这样可以确保任何 IIS 的出错在极短的时间间隔内恢复可以访问。程式内置了三个命令: "A", 它的意思是: "重启 IIS 必要时可以重启服务器"与"B", 它的意思是"仅重启 IIS", 还有"NULL", 它的意思是不执行任何操作, 您可以直接用这三个命令。

示例如下:

```
;$7i24IISMonitorCompare>equals 7i24IISMonitorUrl=http://域名或主机名/目录名/测试页的文件名 7i24IISMonitorValue=ok 7i24IISMonitorCommand=重启 IIS
```

这是最常用的方式, 您可以写一个名字叫 iitest.asp 的文件, 内容可以直接是 <%= "ok"%>, 本程式会定时比较 7i24IISMonitorValue, 是否相等, 否则就执行相关命令, 示例文件 iitest.asp 可以在安装目录中找到。

例如:

```
;$7i24IISMonitorCompare>equals 7i24IISMonitorUrl=http://localhost/iitest.asp
```

```
7i24IISMonitorValue=ok 7i24IISMonitorCommand=A
```

```
;$7i24IISMonitorCompare>equals 7i24IISMonitorUrl=http://localhost/iitest2.asp
```

```
7i24IISMonitorValue=ok 7i24IISMonitorCommand=B
```

```
;$7i24IISMonitorCompare>equals 7i24IISMonitorUrl=http://localhost/iitest3.asp
```

```
7i24IISMonitorValue=ok 7i24IISMonitorCommand="C:\test.exe"
```

```
;$7i24IISMonitorCompare>equals 7i24IISMonitorUrl=http://localhost/iitest4.asp
```

```
7i24IISMonitorValue=ok 7i24IISMonitorCommand="C:\test.bat"
```

关于 iitest.asp, 您可以在安装目录中找到, 默认地, 它位于:

C:\ Program Files\LIWEIWENSOFT\iissafe\iitest.asp,

另外, 一流信息监控拦截系统默认已安装了 wakeuipis.exe 及 wakemysql.exe 可以调用, 它们使用说明可以参考: <http://7i24.com/hsp/104201336206.htm> 来了解。

3.4 文件检查分析记录

文件检查分析记录文件可以通过以下查看:

<http://服务器任何一个正在运行虚拟主机的域名/infosafe/访问密码>

访问密码及登陆密码可以在"一流信息监控拦截系统"中的"管理软件"中直接修改, 重启 IIS 后就会生效。

●一流信息安全监控系统，当前版本：3.5 商用正式版

当前的系统设置：

- ◇分析流入服务器的数据：分析流入的必要动态内容 [拦截流入含有关键词的内容]
- ◇分析流出服务器的数据：只分析指定结尾的文件流出内容：.asp|.aspx|.php [不拦截流出含有关键词的内容]
- ◇分析特点：智能分析 [关键词全部是中文(流入)] [关键词全部是中文(流出)]
- ◇启用了SQL防注入功能：GET部分：' @ or @ or@or @ and @and @, and @; and @exec @exec @backup @backup @char@drop table@drop table@delete from@delete from@insert @insert @select @select @update @update @net user@net user@net localgroup@net localgroup@xp_cmdshell@

POST部分： or @ or@or @ and@and @, and @; and @exec @exec @backup @backup @char@drop table@drop table@delete from@delete from@insert @insert @select @select @update @update @net user@net user@net localgroup@net localgroup@xp_cmdshell@

启动信息：

- ◇拦截关键词(流入)：大法@法轮@李洪志@大纪元@真善忍@新疆人@六合@阴曆@肉棍@阴尸@强奸@淫靡@淫水@阴茎@阴蒂@乱伦@手淫@做鸡@六四事件@江泽民@胡锦涛@罗干@朱镕基@李鹏@江主席@温家宝@迷药@迷魂药
- ◇只记录不拦截的关键词的设置(流入)：@新生网@口交@天安门@共产主义@共产党@中共@反共@台独@达赖@反革命@反华@盗取@绕过封锁@新疆独立@西藏独立@民运分子@打倒@推翻@多党执政@专制@国民党@成人小说@成人电影@裸体@激情图片@激情电影@
- ◇拦截关键词的设置(流出)：大法@法轮@新生网@新疆人@肉棍@阴尸@强奸@阴曆@淫靡@淫水@阴茎@阴蒂@乱伦@手淫@做鸡@口交@李洪志@大纪元@真善忍@六合@天安门@共产主义@共产党@六四事件@江泽民@中共@反共@台独@达赖@反革命@反华@盗取@绕过封锁@新疆独立@西藏独立@胡锦涛@罗干@朱镕基@李鹏@民运分子@打倒@推翻@多党执政@专制@江主席@国民党@胡锦涛@温家宝@成人小说@成人电影@裸体@激情图片@激情电影@迷药@迷魂药
- ◇只记录不拦截关键词的设置(流出)：台湾@马英九@
- ◇IP限制：不启用IP限制功能 [记录被拦截的IP]
- ◇不拦截的虚拟主机：

时间	IP地址	分类	操作	访问的网址	关键词	找到的相关内容摘要
2007-01-13 19:10:57	127.0.0.1	[out]	[GET]	http://127.0.0.1:8080/addini.asp		[大法] 以加入自己所要监控的关键词含有以下的词时当时将执行拦截 大法 法轮李洪志大纪元真善忍新唐人六合阴屠肉棍阴
2007-01-13 19:10:57	127.0.0.1	[out]	[GET]	http://127.0.0.1:8080/addini.asp		[中共] 膊 侯中共反共台独达赖反革命反华盗取经过封锁新疆独立西藏独立民主分子打倒推翻多党执政专制国民党成人小?<t/d

欢迎使用一流信息安全监控系统(文件检查官及IIS健康检查官部分)

●一流信息安全监控系统，当前版本：3.5，[商用正式版]

当前的系统设置：

- ◇监控的目录：[d:\freehost](#)
- ◇分析的文件类型：[|.htm|.html|.asp|.aspx|.jsp|.php|.txt|.js|.log](#)
- ◇最大文件上限：102400000字节
- ◇内容分析特点：智能分析
- ◇关键词的设置：[聊天@江湖@蒋彦永@新唐人@腐败@人祸@禁书@无界浏览器@六合@特码@江湖消息@天安门@共产主义@共产党@六四事件@法轮功@法轮大法@李洪志@大法弟子@大纪元@真善忍@六合@大纪元@真善忍@新生网@灭绝罪@大揭露@修炼大法轮功@法轮@洪志@公审@突破封锁@绕过封锁@腐败@人祸@无界浏览器@中共@反共@台独@达赖@反革命@反华@盗取@疆独立@达赖@藏独立@国民党@民运分子@打倒@推翻@多党执政@专制@江泽民@胡锦涛@罗干@榕基@李鹏@江主席@江泽民@温家宝@温家宝@天安门@共产主义@共产党@六四@中共@江胡内斗@胡江内斗@民运@多党执政@专制@国民党@玉清团@家自拍@成人片@成人电影@裸体@激情图片@激情电影@成人小说@肉棍@阴尸@乳房@阴唇@淫水@阴茎@阴蒂@乱伦@手淫@露妓@黑鸡@幼女@第十六次代表@人权@江氏@小穴@淫荡@强奸@强暴@强奸@换妻@性骚扰@淫魔@淫女@三级片@素女@淫靡@做鸡@口交](#)
- ◇全部更新列表：[点击访问>>>](#)
- ◇图片更新列表：[点击访问>>>](#)
- ◇Flash等更新列表：[点击访问>>>](#)
- ◇htm更新列表：[点击访问>>>](#)

*另一个目录的监控记录(如果已启动监控)：[点击访问>>>](#)

返回上一頁(IIS守门员日志)：[>>>>](#)

[illegible]

系统记录了以下的内容：

时间：事件发生的时间，是服务器的时间，GMT 第八时区（中国）的时间。

被检查的文件：文件检查官会自动检查指定目录中内容修改了的文件。

网络访问：可以通过修改配置文件及 IIS，令到管理员在线检查此文件。

关键词：文件检查官分析指定的文件所含有的关键词。

相关的内容摘要：为了方便管理员分析，文件检查官将关键词附近的内容摘录了下来，让管理员判断它是否合法。

点击 [◇ 图片更新列表](#)： [点击访问>>>](#)；

您可以看到今天的图片更新的内容：

d:\freehost\testss\web\ameli04a014.jpg



通过快速浏览，您可以知道那个用户上传到不良图片在那个目录中。

常见问题：

A. 为什么我没有看到一个图片？原因是您没有启用文件检查官，默认安装后它的状态是停止的。另一个可能是，您的用户还今天还没有上传新文件。

B. 为什么我的图片全部都显示不出来？

在 I E 中查看文件检查官的图片日志时，它是使用 `应用程序池的运行用户` 来访问图片文件的，这个用户默认是 `网络服务(Service)用户`；如果这个用户没有权限读取图片，图片就会无法显示。为了解决这个问题，您可以按以下操作：

建立一个网站是运行在 `system` 用户下，然后用 IE 访问这个网站上的 IIS 医生，就可以

重启。

可以在 IIS6 管理器中，建立一个池，如"testpool"，将池的运行标识改成"本地系统"。然后，建立一个新的虚拟主机，分配一个新的域名(如: iis.test.com),主目录可以设置在任何一个目录,如:c:\test, 并且,将这个虚拟主机的运行池设为运行在"本地系统"下的池(如 testpool)。

这样设置好以后,访问 <http://iis.test.com/infosafe/123456>,就可以正常查看图片的监控记录了。为了安全,你可以进一步设置这个虚拟主机的"目录安全性",在"IP 地址和域名限制",选择"拒绝访问",那么,没有任何 IP 可以直接访问这个虚拟主机上的内容。只有一流信息监控拦截系统可以在这个主机上运行。

C. 我想看昨天的监控信息,我如何才能在 IE 中查看旧的图片监控日志?

使用以下的格式查看:

http://服务器任何一个正在运行虚拟主机的域名/infosafe/访问密码/年_月_日_类型_目录编号.htm

例如查看监控目录一的 2007-1-13 静态文件的检查日志:

http://sys.test.com/infosafe/123456/showfilecon/2007_1_13_ana_1.htm

例如查看监控目录一的图片的检查日志:

http://sys.abc.com/infosafe/123456/showfilecon/2007_1_13_photo_1.htm

例如查看监控目录二的 2007-1-13 静态文件的检查日志:

http://sys.test.com/infosafe/123456/showfilecon/2007_1_13_ana_2.htm

例如查看监控目录二的图片的检查日志:

http://sys.abc.com/infosafe/123456/showfilecon/2007_1_13_photo_2.htm

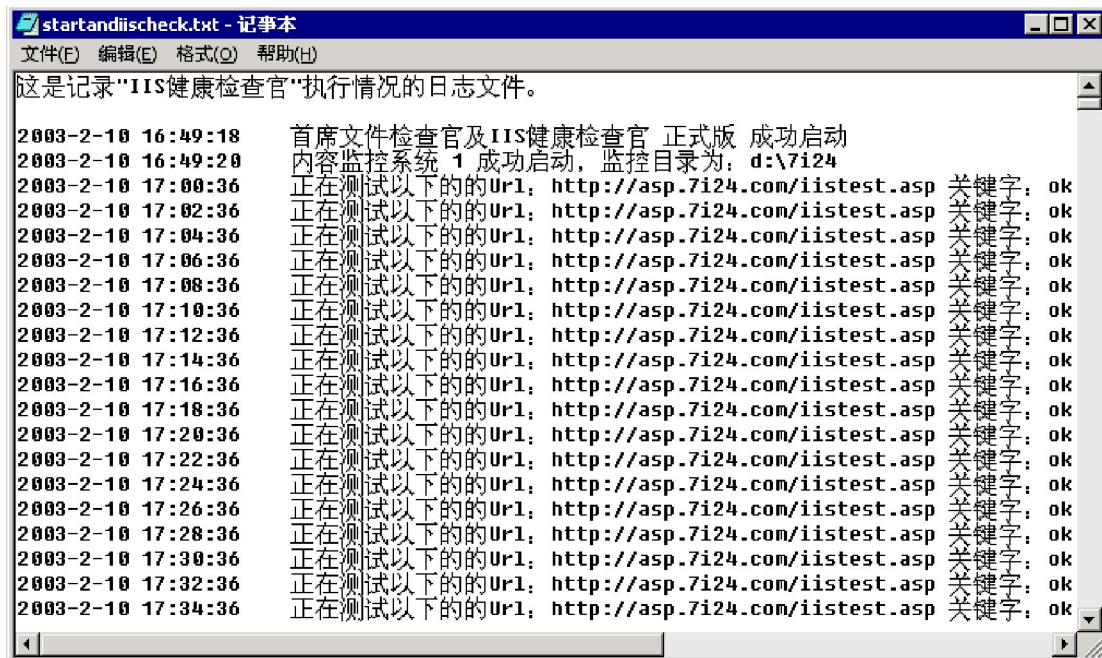
3.5 IIS 健康日志记录

IIS 健康日志文件可以通过以下方式查看:

您可以打开"开始菜单"中的"一流信息监控拦截系统"中的"管理与设置",并点击 i IIS 健康日志记录 j, 这样就可以从记事本中打开它。

它是位于安装目录中的一个名为 startandiischeck.txt 的文本文件。它的默认位置在:
C:\ Program Files\LIWEIWENSOFT\iissafe\log\startandiischeck.txt

示例文件如下:



IIS 健康日志记录描述了系统执行的情况，它会记录启动信息，IIS 的定时检查结果，出错信息，命令执行的情况等，您可以通过这个文件完全了解服务器的 IIS 的情况。

3.6 查看事件记录

"首席文件检查官与 IIS 健康检查官"除了写入以上的日志外，还会将一些重要的信息写入 windows 的事件记录中，您可以在 `管理工具` 中的 `事件查看器` 中的 `应用程序日志` 中看到它。

来源于 `7i24IISMonitor` 的事件就是由"首席文件检查官与 IIS 健康检查官"生成的，您可以查看它了解本软件的运行情况。

3.7 错误处理

注意软件需要获得运行许可证后才能正常加载的。因此请确保您已获得了有效的运行许可证。

- A. 如果监控的日志文件在成功安装后，并且重新本软件后仍然是空白，请检查您是否获得了有效的运行许可证。
- B. 如果已获得了有效的运行许可证，以前也曾成功启动过，请检查您的 IP 是否变更，或您的网络是否连通，因为一个运行许可证只能绑定在一个 IP 上的。
- C. 如果您修改守配置文件后软件就无法启动，表明您修改的一些重要参数出错了，我们建议您恢复到原来的设置，再重新启动本软件。

错误信息：

如果您在 `应用程序日志` 中看到以下内容：

`警告！首席文件检查官及 IIS 健康检查官启动不成功，注册表读取出错！请访问 http://7i24.com，请与 tec@7i24.com 联系；`

表明软件读取注册表初始化时失败，建议您重新安装本软件。

如果您在 i 应用程序日志 i 中看到以下内容：
i 注意！由于日志文件大于 20M，已被清除并重新开始记录。 i
表明软件将重新初始化 i IIS 健康日志文件 i。

如果您在 i 应用程序日志 i 中看到以下内容：
i 警告！首席文件检查官及 IIS 健康检查官启动不成功，不能建立日志文件！请访问
<http://7i24.com>，请与 tec@7i24.com 联系 i
表明软件建立日志失败，请检查：
相关的文件是否被删除，或是否有写的权限，默认的安装位置在：
C:\ Program Files\LIWEIWENSOFT\ iissafe\log\

如果您在 i 应用程序日志 i 及 i IIS 健康日志文件 i 中看到以下内容：
i 首席文件检查官及 IIS 健康检查官初始化失败！读取 infosafe.ini 发生错误，请检查此文
件！ i
表明软件读取配置文件失败，请检查位于安装目录中的一个名为 infosafe.ini 的文本文件。
它的默认安装位置在：
C:\ Program Files\LIWEIWENSOFT\ iissafe \infosafe.ini

如果您在 i 应用程序日志 i 及 i IIS 健康日志文件 i 中看到以下内容：
i 首席文件检查官(内容监控系统)初始化失败！启动过程中发生错误，请检查配置文件是否
正确！ i
表明软件配置文件中的监控目录不正确，有可能是指定的监控目录并不存在，请检查配置文
件中的 i WatcherDir= i 部分定义是否正确。

如果您在 i 应用程序日志 i 及 i IIS 健康日志文件 i 中看到以下内容：
i 语法不正确 XXXxx i
表明软件配置文件相关配置不正确，请检查并修正它。

4、爱国者智能 COM 组件

4.1 概述

此组件由 7i24.com 开发，目的是实现网站的 BBS 及新闻系统对政治及色情等不良内容的过滤。已实现了智能过滤，例如；#江##泽##民##；等分隔开的词一样能检测。

一些服务器提供商，例如一些 ICP，它所发布的信息，或论坛内容的是由自己的技术人员开发的，但并不是所有的公司的技术人员都有编写象；爱国者智能 COM 组件；这样的能力的，我们这个产品让您开发的程序可以直接调用本组件来实现智能过滤。示例代码可以在安装目录中找到，默认地，它位于：

C:\Program Files\LIWEIWENSOF\iissafe\example.asp

4.2 示例用法

以下是一段使用本组件的典型的 ASP 程序：

```
<%'  
str="    中    国    中    国    人    中    国    人    #    江    ##    泽  
##XXXXXXXXXXXXXXXXXXXXXIXXXXXXXXXXXXXXXXXXXXXXXXXX 民##"  
word="天安门@love@江泽民"  
Set icpcom = Server.CreateObject("FreeICP")  
icpcom.key=word '设置关键词  
icpcom.smart=1 '设置是否启用智能分析,1 代表启用，0 代表不启用，默认值是 1  
temp=icpcom.check(str)  
if temp<>"" then  
response.write "要检查的内容 ""&str&"" 含有非法关键词: "&temp '输出检查结果  
response.write "<br><br><br>"  
else  
response.write "要检查的内容 "&str&" 内容合法" '输出检查结果  
response.write "<br><br><br>"  
end if  
response.write icpcom.about '输出版权及其他信息  
set icpcom=nothing  
%>
```

生成组件的实例：

```
Set icpcom = Server.CreateObject("FreeICP")  
设置本组件所用的关键词  
icpcom.key="天安门@love@江泽民"  
设置是否启用智能分析,1 代表启用，0 代表不启用，默认值是 1  
icpcom.smart=1  
执行内容检查与分析  
temp=icpcom.check(我是中国人 XXX 江 erere 泽 sf 民 ZXXsd)
```

如果分析结果含有关键词，icpcom.check 会返回这个关键词，如果不含有任何关键词，icpcom.check 的返回值会是空的。

您可以通过这点来分析内容的合法性：

```

if temp<>"" then
response.write "要检查的内容 ""&str&"" 含有非法关键词: "&temp 输出检查结果
response.write "<br><br><br>"
else
response.write "要检查的内容 "&str&" 内容合法" '输出检查结果
response.write "<br><br><br>"
end if

```

关于智能分析:

当组件的属性: smart=1 时, 无论汉字中有任何特殊分隔它都可以找出来的, 例如这样:

dfajsklfjkjfkjasdfsdffsd 法 4358742dd,390584095ddafdkfld 轮 4059i4ti@#####功,,,,,
将一样被分析出来!

我们已经成功地将本组件应用在大量的大型的 BBS 论坛与新闻发布系统, 它让管理员完成放心了。它是一个完全符合 COM 规范的组件, 因此您可以在任何编程语言中使用它的, 例如 ASP,ASP.Net,VC++,VB,BCj .等。

4.3 错误处理

A. 错误信息:

服务器对象 错误 'ASP 0177 : 80020004' Server.CreateObject 失败 找不到参数。

原因: 有可能本组件未成功安装, 可以重新安装它。

B. 错误信息:

服务器对象 错误 'ASP 0177 : 80070057' Server.CreateObject 失败 一个或数个参数无效

原因: 未获得运行许可证, 请确保您已获得了有效的运行许可证。

C. 错误信息

Microsoft VBScript 运行时错误 错误 '800a0005' 无效的过程调用或参数: 'icpcom.check'

原因: 有可能本组件未成功安装, 可以重新安装它。另一可能是未获得运行许可证, 请确保您已获得了有效的运行许可证。

5、中央控制网站使用说明

5.1 概述

对于有多台服务器的用户，由于管理上的需要，监控的关键词会经常性调整，如果一台台地登陆服务器来手工修改关键词会消耗大量的时间，在星外科技全国的用户中，有一部分用户的服务器量达到 300 台服务器，为了增加一个关键词就要登陆 300 台服务器，显然处理效率非常低，针对这种情况，为了方便用户，星外科技在 3.6 版本的一流信息监控拦截系统正式推出了自动更新多台服务器配置文件的中央控制网站，让您可以同时自动更新上千台服务器的配置文件！从这个版本起您非常轻松地随时随地地调整多台服务器的一流信息监控拦截系统参数。

5.2 下载中央控制网站包

目前中央控制网站包免费提供给服务器超过 10 台的用户，详细的下载地址请您直接联系星外科技的技术支持 QQ 来获得。

5.3 安装中央控制网站

中央控制网站是一个标准的使用 ACCESS 数据库的 ASP 类的网站，因此，安装是很容易的。请您将 [www.rar 解压缩](#)，直接上传到一个支持 ASP+ACCESS 的虚拟主机中，马上就可以使用了。注意尽可能情况下不要将中央控制网站放在装了一流信息监控的服务器上，因为配置文件中大量的关键词，可能会被拦截而造成更新配置失败。

5.4 访问中央控制网站

访问您所上传的虚拟主机的网址，可以看到以下的界面：



5.5 注册管理员

请您点注册，然后按提示信息完成注册。

5.6 首次登陆

使用您注册好的用户名及密码，登陆管理系统后，您会看到以下内容：

登陆信息：登陆时间：2007-1-13 19:04:13 IP：127.0.0.1

设置本网站的域名： (如test.abc.com)

受控的服务器将通过这个域名来下载配置文件。

请您先设置好这个虚拟主机的访问用的域名，受中央控制端控制的每一台服务器，都会通过这个域名来下载配置文件，因此，请您确保每台受控的服务器，都能正常访问中央控制端网站。

5.7 添加配置模板

点击添加配置模板后，您可以看到以下内容：

自助管理

模板列表为空，请您先添加模板

定义配置模板：

名称： 录入人：星外科技

IIS守门员部分 (v3.5商用正式版支持中央集成/UTF-

请您输入自己定的这个模板名称如j 一号模板j，然后根据自己的情况调整配置文件中的内容，再点添加。您可以添加多个模板，从而根据自己的需要随时调用。

5.7 管理服务器

点击管理服务器后，您可以看到以下内容：

服务器列表为空，请您先添加服务器。

定义服务器：

录入人：星外科技 录入时间：2007-1-13 19:18:44 发布配置时间：

服务器名称： 服务器IP：

IIS守门员网址：

IIS守门员密码： (如：7i24.com)

设置这台服务器上不拦截的域名：

设置IIS健康检查的监控内容：

(如：\$7i24IISMonitorCompare>equals 7i24IISMonitorUrl=http://www.test.com/ii:

选择配置文件的模板：

请您先一台台地添加服务器的信息，服务器名称您可以自定，如; 电信一号; 服务器，服务器 IP 您可以自由输入，这儿输入的 IP 信息并不会影响一流信息监控拦截系统的运行，IP 信息只是方便您识别这台服务器，然后您可以输入 IIS 守门员的网址及 IIS 守门员的密码。中央控制端网站根据 IIS 守门员的网址及 IIS 守门员的密码来发布更新配置文件及重启 IIS 的指令。

由于每台服务器上的网站都不一样，您可以在定义服务器这儿，单独设置这台服务器上 IIS 守门员不拦截的域名，当然，您也可以不输入这儿的内容。

由于每台服务器上的 IIS 健康检查官监控的网站都不一样，您可以在定义服务器这儿，单独设置 IIS 健康检查官的配置信息，关于这方面配置的说明，请您参考本文档前面的配置文件说明部分来了解。

最后部分是选择这台服务器所使用的配置文件的模板。这个模板的内容，就是您在; 添加配置模板; 中所输入的内容。

点击; 添加; 后，您输入的服务器定义信息就会被保存下来，您可以输入无限多台服务器的信息。

5.8 发布配置文件给服务器

添加完服务器后，您可以看到以下内容：

发布当前配置给所有服务器>>> 重启所有服务器的IIS>>>

IP：192.168.0.8 配置文件发送时间：	修改	发布配置	重启IIS
IP：192.168.0.7 配置文件发送时间：	修改	发布配置	重启IIS

您可以点击发布配置，配置文件会马上发布给这台服务器，其中，; 文件检查官及 IIS 健康检查官; 会在这台服务器上生效，; IIS 守门员; 部分的配置会在下一次重启动 IIS 后生效，因此，您可以点 重启 IIS;，这样安装在服务器上的 7i24iismonitor.exe 服务，会用 System 用户的身份，调用重启 iisreset.exe 这个命令来重启服务器，一般几分钟内 IIS 会重启完成，新的配置文件也就生效了。

在点击发布配置文件后，几秒钟后，您可以刷新管理服务器这个网页，您可以看到; 配

置文件发送时间; 后面已填写上内容了, 表明配置文件已成功更新, 如果您没有看到; 配置文件发送时间; 后面有内容, 很可能是, 您这台服务器上, 没有允许远程更新配置文件, 请登陆这台受控服务器, 在; 一流信息监控拦截系统; ---管理软件中, 选中; 允许远程更新配置文件;。

在受控服务器上, 管理工具; 事件查看器中, 您可以看到相关的操作日志, 通过这些日志, 您也可以了解远程发布配置文件是否正常。

5.9 发布配置文件给多台服务器

定义好多台服务器的信息后, 您可以点击; 发布当前配置给所有服务器>>>; 及; 重启所有服务器的 IIS>>>;, 将配置文件发送给所有的服务器, 主控网站已经考虑到了各种可能, 就算其中的一些服务器不在线, 也不会影响正常服务器的更新。

5.10 安全方面的说明

为了安全, 您可以将主控网站放在机房的内部网中, 限制外面的 IP 访问, 主控网站只要受控服务器能访问, 它的所有功能就有效了。

5.11 常见问题的处理

配置文件无法更新的主要可能如下:

- A. 文件检查官服务没有启动, 请在; 一流信息监控拦截系统; ---管理软件中, 启动它。
- B. 受控服务器无法访问中央控制网站, 请检查域名有没有解析好, 网络是否正常。
- C. 重启 IIS 失败, 请检查 CMD.EXE, IISRESET.EXE 有没有 system 用户读与运行的权限。

6、性能报告

本报告将指出"一流信息监控拦截系统"在极限级的高负荷平台下的运行情况：

6.1 测试软件："IIS 守门员"

时间：一年

设备：位于中国电信机房的 INTEL IA 服务器

软件：windows 2000 server

硬件：CPU：PIII 1G 内存：512M 10000 转 SCSI 硬盘 36Gx2 RAID1 阵列

网络：中国电信 CHINANET 网络端 CISCO Catalyst 5500 交换机 客户端 100M 3Com 980C 服务器专用网卡

FTP 用户数 4100，真实用户，文件共有 1413,927(141 万)个 html 与图片等类型文件，用户数据共 32G。

访问量：26 万 IP/天

正常使用的情况下 html 文件只需"首席文件检查官"软件就可以用很小的 CPU 消耗来处理的，本次"IIS 守门员"软件的测试在真实使用是有可能有这么重的负荷的。本次测试是希望了解本软件在高负荷的状态下的速度与稳定性。

"IIS 守门员"在本次测试中设置如下：

- ◇分析流入服务器的数据：分析流入的必要动态内容 [不拦截流入含有关键词的内容]
- ◇分析流出服务器的数据：只分析指定结尾的文件的流出内容：.asp|.aspx|.jsp|.php|.html|.htm|.txt| [不拦截流出含有关键词的内容]
- ◇分析特点：删除特殊字符后再分析
- ◇关键词的设置：肉棍@阴户@强奸@阴唇@淫靡@淫水@阴茎@小穴@阴蒂@乱伦@手淫@嫖@做鸡@口交@他妈的@法轮功@法轮大法@李洪志@太比力克@大法弟子@大纪元@真善忍@六合@天安门@共产主义@共产党@紫阳@胡耀@六四事件@江泽民@中共@反共@台独@藏独@达赖@游行@反革命@反华@学运@公安@盗取@绕过封锁@政府@东突@新疆分裂主义@新疆独立@西藏独立@分裂国家@胡锦涛@朱镕基@李鹏@学运分子@民运分子@打倒@推翻@多党执政@专制@毛泽东@小平@毛主席@江主席@国民党@十六大@党代@第十六届@第十六届@第拾陆届@十六次@

经过三个月的连续使用，"IIS 守门员"稳定可靠，生成的分析日志共有 90M，帮助管理员查找出不少色情与政治内容。

网络的平均流量有 2236KB/秒，20MBPS/秒，峰值有 3573K/秒,32MBPS/秒，可以达到中国电信分配给服务器的最高带宽。IIS 的请求次数达 300 次/秒，几乎是新浪网站的流量级，一般国内可以达到这样流量的网站非常罕见。可以看出，用户完全不需要担心"IIS 守门员"对性能的影响！

CPU 平均值为 70%，比不安装本软件增加 2%(2.2 版本)，注意，真正使用时 CPU 是不可能

有这么高的负荷的，因为 html 文件应该用"首席文件检查官"软件来检查，而不是用"IIS 守门员"来检查。

性能监测的截图如下：



6.2 测试软件： "文件检查官及 IIS 健康检查官"

时间：一年

设备：位于中国电信机房的 INTEL IA 服务器

软件：windows 2000 server

硬件：CPU：PIII 1G 内存： 512M 10000 转 SCSI 硬盘 36Gx2 RAID1 阵列

网络：中国电信 CHINANET 网络端 CISCO Catalyst 5500 交换机 客户端 100M 3Com 980C 服务器专用网卡

FTP 用户数 4100，真实用户，文件共有 1413,927(141 万)个 html 与图片等类型文件，用户数据共 32G。

访问量：26 万 IP/天

这是一个真实的高负荷使用环境，在 4100 个的 FTP 用户下，用户可以通过 FTP 方式上传文件，也可以通过 web 方式在线上传。"首席文件检查官"分析监控 141 万个用户文件，实时查找里面的非常内容。本次测试是希望了解本软件在高负荷的状态下的速度与稳定性。 经过一个月的连续使用，"首席文件检查官及 IIS 健康检查官"稳定可靠，生成的分析日志共有 3M(一个月)，帮助管理员查找出不少色情与政治内容。

CPU 消耗平均值：1% 峰值 3%

性能监测的截图如下：7i24IISMonitor 是进程名：

7i24IISMonitor.	672	00	0:47:11	20,964 K
iomgr.exe	696	00	0:00:02	2,732 K
svchost.exe	720	00	0:00:04	7,420 K
LLSSRV.EXE	744	00	0:00:00	2,408 K
portserv.exe	776	00	0:00:00	1,776 K
regsvc.exe	836	00	0:00:00	1,100 K
mstask.exe	856	00	0:00:01	5,060 K
WinMmt.exe	920	00	0:00:13	208 K

☒ 显示所有用户的进程 (S) 结束进程 (E)

进程数: 36 CPU 使用: 22% 内存使用: 328120K / 2009664K

6.3 测试软件: "爱国者 COM 安全组件"

时间: 一年

设备: 位于中国电信机房的 INTEL IA 服务器

软件: windows 2000 ADVANCE Server, SQL 7 DATABASE

硬件: CPU: P4 2G 内存: 2G 10000 转 SCSI 硬盘 36Gx2 RAID1 阵列

网络: 中国电信 CHINANET 网络端 CISCO Catalyst 5500 交换机 客户端 100M INTEL Server 服务器专用网卡

大型社区 120 万注册用户, 发帖数 10213 篇/天, 内部留言 7200 条/天, 其它发布信息 2170 条/天。

访问量: 18 万 IP/天

这是一个真实的高负荷使用环境, "爱国者 COM 安全组件"在三个月的实际使用中, 每天过滤 20,000 次用户提交的内容, 实时分析用户发表的文章是否含有非法内容, 成功拦截 700 多次政治与色情内容, 大大减轻了管理员的工作。本次测试是希望了解本软件在高负荷的状态下的速度与稳定性。

我们通过以下的方法分析它的功能与效率:

本组件可以正确识别 江#####泽####民 这样的分隔开的内容。由于用 VC++ ATL 写成, 效率非常高。

我们通过在 ASP 中生成此组件 10000 次来分析一段 100K 的文章, 另一个对比是用 ASP 写成的同类算法, 结果发现, "爱国者 COM 安全组件"比由单纯 ASP 写成的同样功能的代码快 120 倍! 而且准确识别出所有的非法内容!

7、案例研究

7.1 对象：虚拟主机提供商/空间提供商

空间提供商常在一台服务器中放置大量的用户，并为用户开通 FTP 权限，让用户可以自行上行内容。这样，空间提供商就面临一个严峻的管理问题。因为服务器随时有可能有非法内容，例如法轮功，反党内容，色情内容，六合彩等，让提供商提心吊胆，因为公安部门接到举报后会马上警告空间提供商，多次出现此类问题有可能被公安部门停止服务。

一流信息监控拦截系统首先是为解决这个问题而开发的。它还解决了一个让空间提供商头痛的死角---空间用户自行上传的 社区/BBS/留言本/聊天室 的管理问题，一些提供商提供支持 ASP,PHP,CGI 的虚拟主机，不少空间用户自行上行了论坛或留言本，经常是一两个月都不管理，让访问者有机可乘，反表了反动信息，空间提供商根本不知道，也无法管理，最后是公安部门的网监处打电话警告空间提供商有非法信息！空间提供商就处于非常被动的状态。

一流信息监控拦截系统可以成功分析记录并可以拦截非法内容，在反动信息根本无法通过，也没有可能进入空间用户的虚拟主机中。对于空间用 ASP 读取数据库或其他方式动态生成的内容，一流信息监控拦截系统同样可以分析拦截，让空间用户完全处于受控状态，这部分工作由"IIS 守门员"软件来完成。

为了有最高的检查效率，静态内容，例如 html,txt 等内容，由于这此内容并不经常更新，我们采用 i 首席文件检查官 i 软件来监控，空间提供商只需看看它生成的报表就可以知道自己的用户上传了什么内容是敏感的或非法的，我们的测试结果表明这个软件仅用平均 2%的 CPU 消耗就可以监控 200 万个用户文件。

i 首席文件检查官 i 同样可以帮助空间提供商查找谁上传了聊天室，江湖，电影文件，音乐文件等影响稳定的内容，并可以自动删除，保证了系统的稳定。

"IIS 健康检查"模块让空间提供商可以无需人工值班监控服务器的状态，实行自动监控，出问题时可以用短信通知空间提供商，并自动恢复服务器回到优良状态。

应用实例：

7i24.com

7i24 为最终用户提供空间服务，空间的用户可以用 FTP 方式上传自己设计的内容，其中包括论坛，每台服务器通过 100M 带宽连接 ChinaNet。一台服务器的文件达 110 万个，有静态的 html 文件，也有动态的 ASP 内容。从十六大召开前两个月开始，为了保障信息的可控性，7i24 启用了"一流信息监控拦截系统"，经过长时间的使用，效果非常明显，管理人员可以轻松监控所有的用户上传的内容，可以监控拦截所有用户的 BBS 与留言本，大大减小的经营风险。同时每天可以分析出是否有用户上传聊天室，维护了每台服务器的稳定。

7.2 对象：ICP/内容提供商/政府网站/企业网站

ICP 与政府网站或企业网站，在自己发布内容前需要进行审查，例如通过 FTP 发布或自己的新闻系统发布，机器预审是必不可少，在机器预审方面，一流信息监控拦截系统完美地解决这个问题，在这个系统的监控下，CIO 完全可以放心，领先的智能过滤技术，例如j #江##泽##民##j 等分隔开的词一样能检测。用户可以直接用"IIS 守门员"来预审所有内容，如果有自己的新闻发布系统，可以在系统中调用"爱国者智能 COM 组件"，利用它高效地来分析调动文章内容，将非法内容拦在外面。

如果 ICP 与政府网站或企业网站用自己的 社区/BBS/留言本/聊天室，按以往的方式，需要人工监控，但有了"一流信息监控拦截系统"，您完全可以将监控工作交给它来代替，再也不需要工作人员 24 小时轮班了。

应用实例：

大型社区 BBS

大型社区 120 万注册用户，发帖数 10213 篇/天，内部留言 7200 条/天，其它发布信息 2170 条/天。访问量：18 万 IP/天。从十六大召开前两个月开始，为了保障信息的可控性，启用"一流信息监控拦截系统"，经过长时间的使用，效果非常明显，非法内容再也无法出现在文章，聊天室中了！大大减小的经营风险。

8、获得技术支持

您可以通过访问 <http://7i24.com> 中的相关栏目来获得技术支持，也可以发信给：
tec@7i24.com 获得技术支持，请注意，来信中请附上您的用户名，所用的软件的版本号，操作系统的环境以帮助我们迅速为您解决问题。

本软件出售给最终用户后，我们会在一个月内提供免费的电话技术支持，同时我们会在一年内为您提供免费的 Email 技术支持。

正版用户可以登陆客服中心在线提交问题，也可以联系在线技术 QQ 为您提供技术支持。

9、如何购买本公司的产品

请与我们的销售人员联系：

市场部

020-86001418/86001448/86001468

邮箱：mart@7i24.com

所有信件我们会在工作时间 9:00AM--24:00PM 回应。