InforGuard V5.2.5 使用手册

中创软件商用中间件股份有限公司

地　　址：山东省济南市千佛山东路41-1　号
服务热线：400-618-6180
传　　真：0531-81753668
邮　　编：250014

http://www.inforbus.com/index.jsp

第 1 章 安装部署

1.1. 产品综述

1.1.1. 概述

InforGuard 由以下几部分组成：InforGuard MA,InforGuard SA,InforGuard MC。

InforGuard MA 是 InforGuard 的监控代理，部署于网站服务器，负责实时监控保护网站文件，发现篡改企图或篡改操作实时发送恢复请求，并及时提交告警信息。

InforGuard SA 是 InforGuard 的同步代理，部署于同步服务器，负责实时监控备份文件变更，以及监控代理提交的恢复请求， 并根据请求执行向网站服务器的文件同步。注：同步服务器通常情况下是指 CMS 服务器或 FTP 服务器。

InforGuard MC 是 InforGuard 的管理中心，逻辑上部署于管理服务器，作为用户与系统之间的接口， 负责将操作指令传达给监控代理和同步代理；同时，负责实时接收来自代理端的各种告警信息并及时通知用户。

1.1.2. 产品支持的环境

当前版本支持的平台环境如下：

InforGuard 支持的操作系统：Windows 2003、Windows 2008、Linux RedHat9i、Linux RedHat AS3、Linux RedHat AS4、Linux RedHat AS5。

InforGuard 支持的应用服务器：Apache、IIS、JEE（Tomcat、Websphere、weblogic)。

1.2. 产品安装和卸载

1.2.1. 安装准备

1. 最低配置

组件	要求
CPU	CPU 2.8GMHz 的处理能力以上
物理内存	512MB 以上

硬盘	系统盘可用空间 800MB 以上
操作系统	Microsoft Windows 2003
浏览器	Microsoft Internet Explorer 7、6.x

2．推荐配置

组件	要求
CPU	CPU 2.8GMHz 的处理能力以上
物理内存	1GB 以上
硬盘	系统盘可用空间 1GB 以上
操作系统	Microsoft Windows 2003
浏览器	Microsoft Internet Explorer 7、6.x

1.2.2. InforGuard MA 的安装

1.2.2.1. Windows 上 InforGuard MA 的安装

InforGuard MA 在 Windows 上的安装过程如下:

1．双击安装程序。

2．稍后会启动安装向导，并提示用户选择安装向导的提示语言种类。以下的步骤以简体中文语言为例说明。

3．稍后会出现安装提示界面如下，安装程序将指导您完成 InforGuard MA 的安装，如图 1-1：

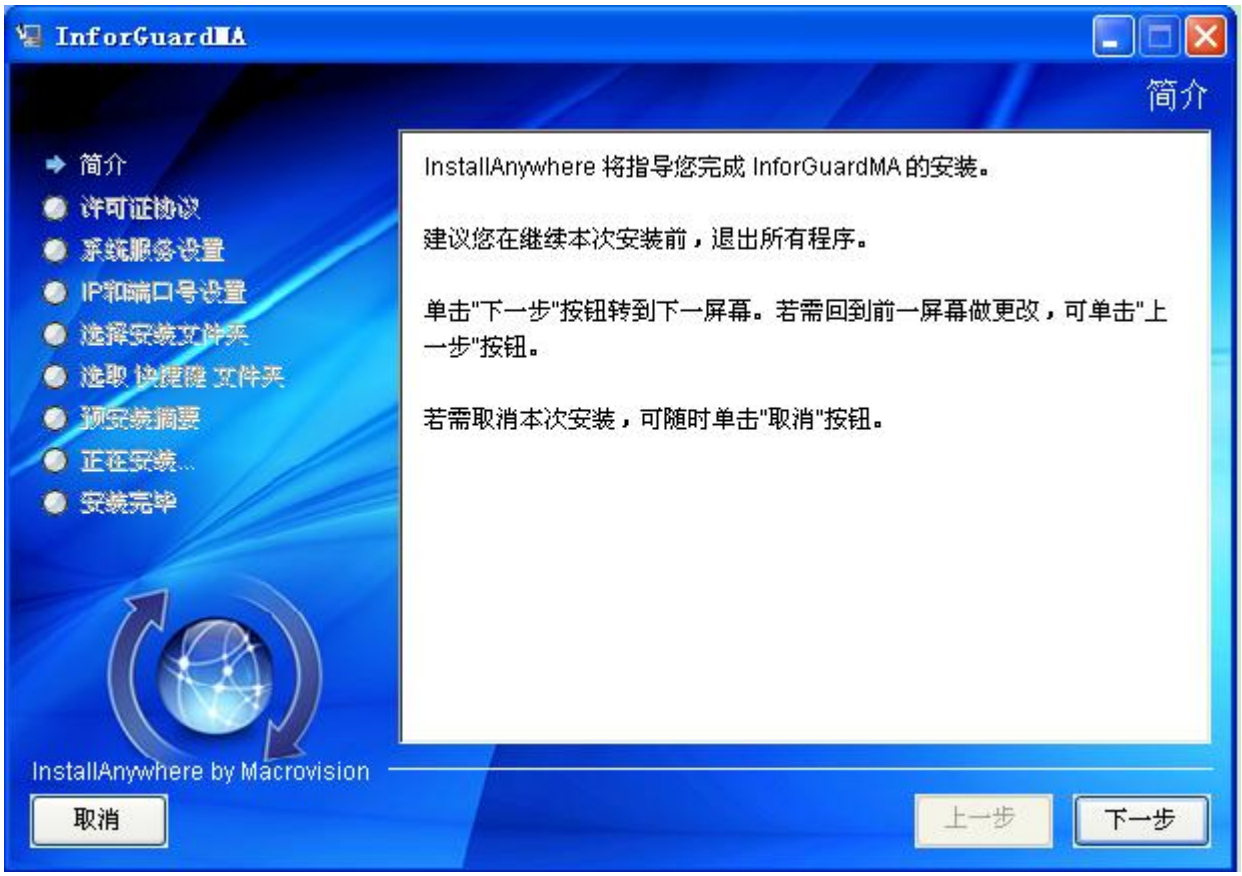


图 1-1

4. 接受 InforGuard 的 License 后，安装程序会提示您是否将 InforGuard MA 设置成为系统服务。如果选择“是”， InforGuard MA 将会被安装为一项系统服务，在每次系统启动时自动启动。选择设置为系统服务后，安装后您可以 通过 Windows 的控制面板->管理工具->服务来管理 InforGuard MA 的启动和停止。如果您想每次都手动控制 InforGuard MA 的启动和停止，请选择“否”，如图 1-2：

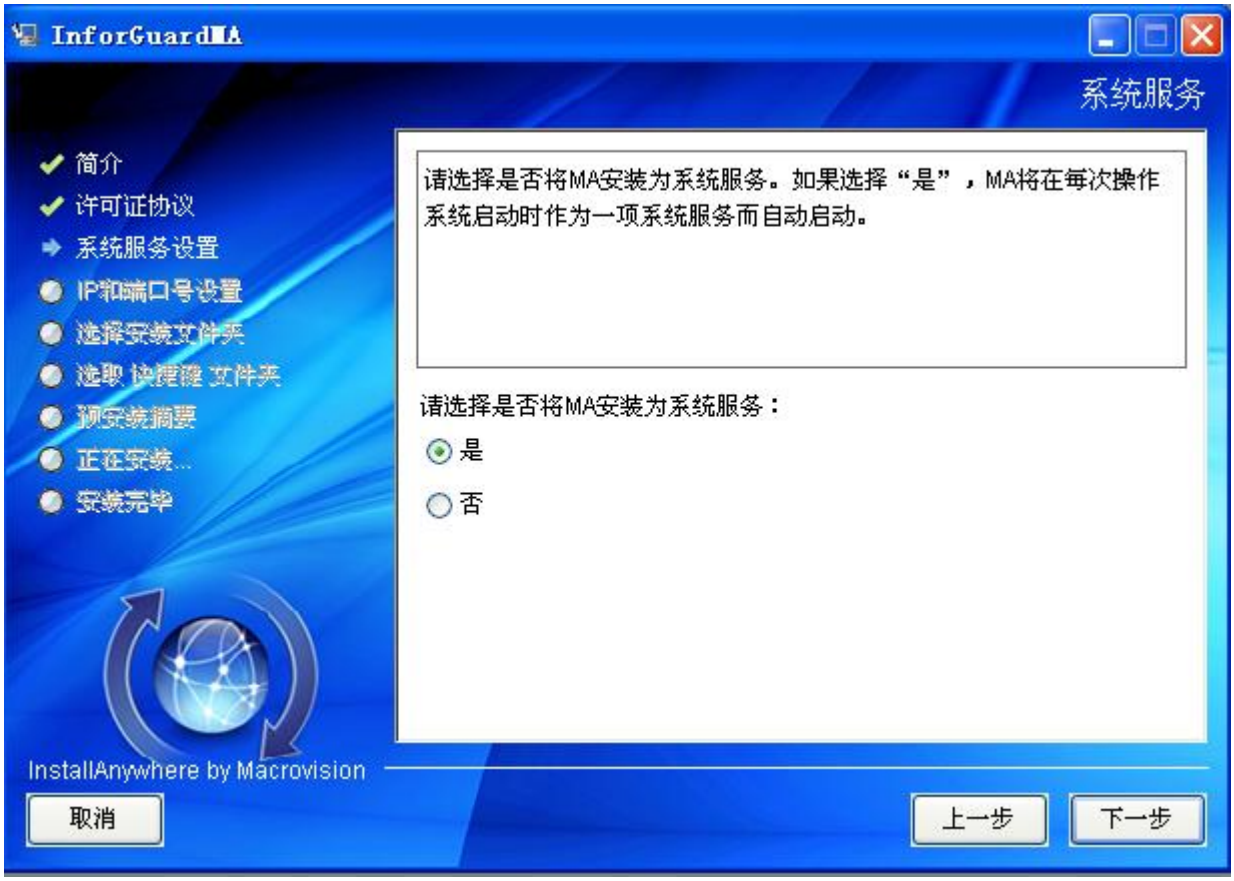


图 1-2

5. 之后安装程序将提示您设置 InforGuard MA 所使用的 IP 地址和端口。在此界面的 IP 地址下拉列表中，会列出您的机器 当前的所有 IP 地址。请选择一项和 InforGuard MC、InforGuard SA 在同一网段内的 IP 地址。InforGuard MA 将使用此 IP 地址 和 InforGuard MC、InforGuard SA 进行通讯。InforGuard MA 默认是用的端口号为 10002，请确认此端口没有被占用。如果此 端口已经被占用，请输入其他的端口号，如图 1-3:

图 1-3

如果在安装后您想修改 InforGuard MA 所使用的 IP 地址和端口号，可以直接修改 MA 的配置文件 cfg\ma.xml。 里面的 app 节点的 localip 属性和 localport 属性对应这里输入的 IP 地址和端口。

6. 下一步安装程序提示您输入要安装的路径。请注意不要选择有中文和空格的路径地址。

7. 在选择快捷方式后，如果您对之前输入的项没有疑问，点击"预安装摘要"的下一步后安装程序会将 InforGuard MA 装入您的计算机中。

1.2.2.2. Linux 上 InforGuard MA 的安装

InforGuard MA 在 Linux 上的安装过程如下:

1、选择安装 MA 的用户，可以是 ROOT 用户也可以是普通用户，所选的用户应当对希望保护的网站有读写和执行的权限。

2、用上述选定的用户登陆 Linux 系统，拷贝安装包到本用户的目录。

3、若安装包为压缩格式，请先解压。解压后为目录，其中包含 install 文件。

4、执行上述目录下的文件 install（即执行./install），随后系统会显示版权信息，计算机 CPU 类型信息和产品版本信息，并提示用户是否继续安装。

注：若程序 install 不能够运行，一般是文件权限的问题，请改变这两个文件的权限为可执行/可读权限。然后继续执行 install。

5、输入字符 y，之后敲回车键确认安装。

6、安装程序将提示输入安装全路径，MA 将安装到该目录下。如输入 /usr/local，则 MA 安装后的目录为/usr/local/InforGuardMA。输入路径并回车。

7、修改 MA 安装目录中的配置文件。例如：vi /usr/local/InforGuardMA/cfg/ma.xml。找到 localip="127.0.0.1"，把 ip 地址改为 MA 进程希望绑定的本机 IP 地址。

8、MA 启动：在 MA 的 bin 目录下执行./mactl start

9、MA 停止：在 MA 的 bin 目录下执行./mactl stop

1.2.3. InforGuard SA 的安装

1.2.3.1. Windows 上 InforGuard SA 的安装

InforGuard SA 的安装同 InforGuard MA 基本相同，具体步骤介绍如下:

1．双击安装程序。

2．稍后会启动安装向导，并提示用户选择安装向导的提示语言种类。以下的步骤以简体中文语言为例说明。

3．稍后会出现安装提示界面，安装程序将指导您完成 InforGuard SA 的安装，如图 1-4:

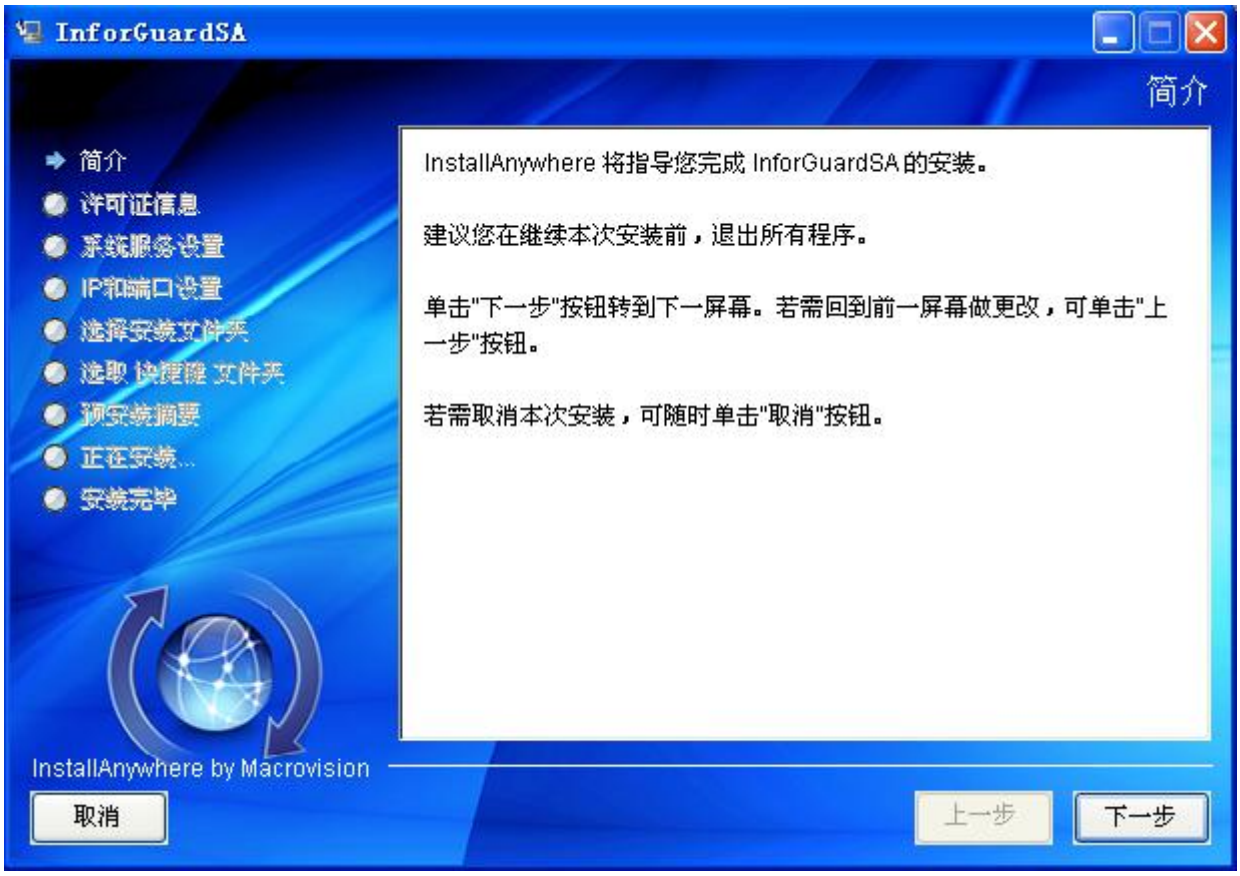


图 1-4

4. 接受 InforGuard 的 License 后，安装程序会提示您是否将 InforGuard SA 设置成为系统服务。如果选择“是”， InforGuard SA 将会被安装为一项系统服务，在每次系统启动时自动启动。选择设置为系统服务后，安装后您可以通过 Windows 的控制面板->管理工具->服务来管理 InforGuard SA 的启动和停止。如果您想每次都手动控制 InforGuard SA 的启动和停止，请选择“否”，如图 1-5:

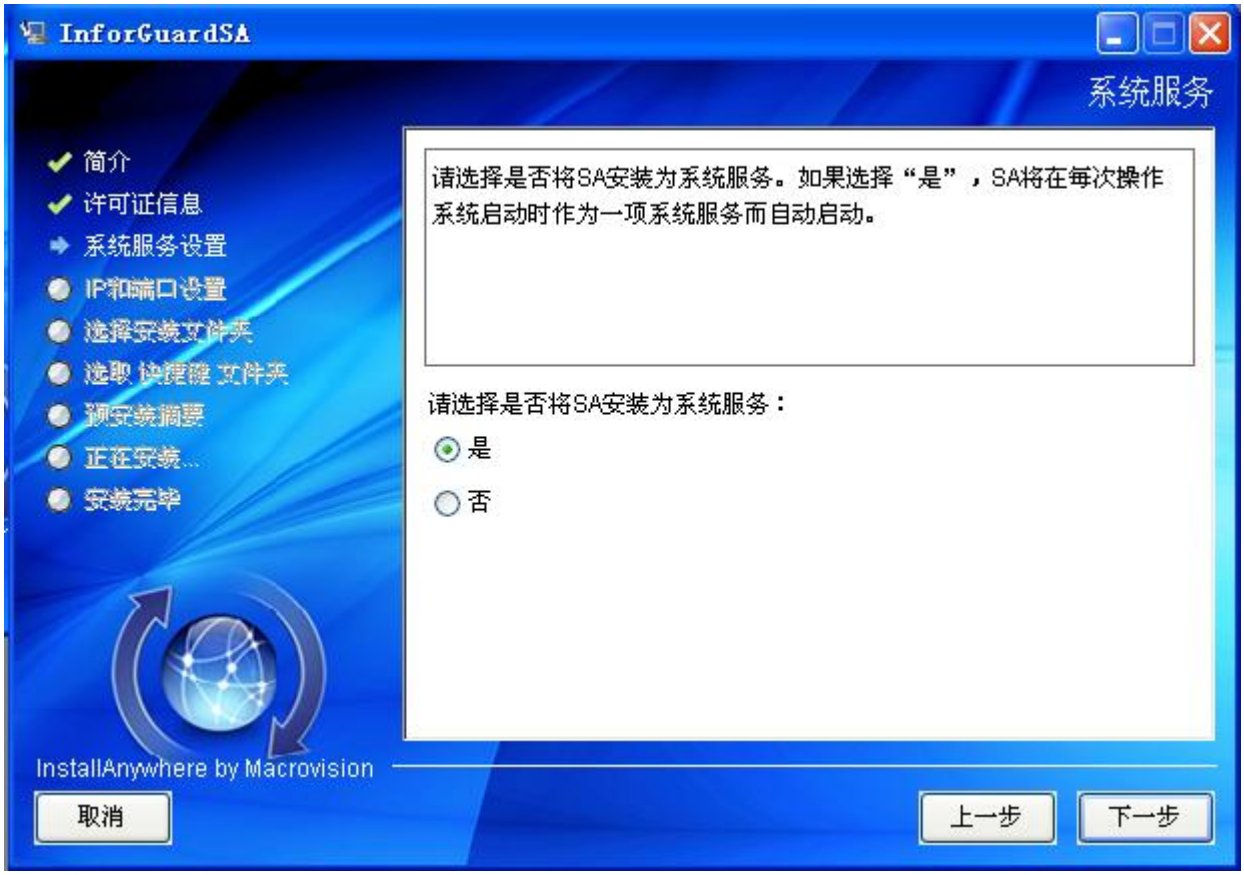


图 1-5

5. 之后安装程序将提示您设置 InforGuard SA 所使用的 IP 地址和端口。在此界面的 IP 地址下拉列表中，会列出您的机器 当前的所有 IP 地址。请选择一项和 InforGuard MC、InforGuard MA 在同一网段内的 IP 地址。InforGuard SA 将使用此 IP 地址 和 InforGuard MC、InforGuard MA 进行通讯。InforGuard SA 默认是用的端口号为 10003，请确认此端口没有被占用。如果此 端口已经被占用，请输入其他的端口号，如图 1-6:

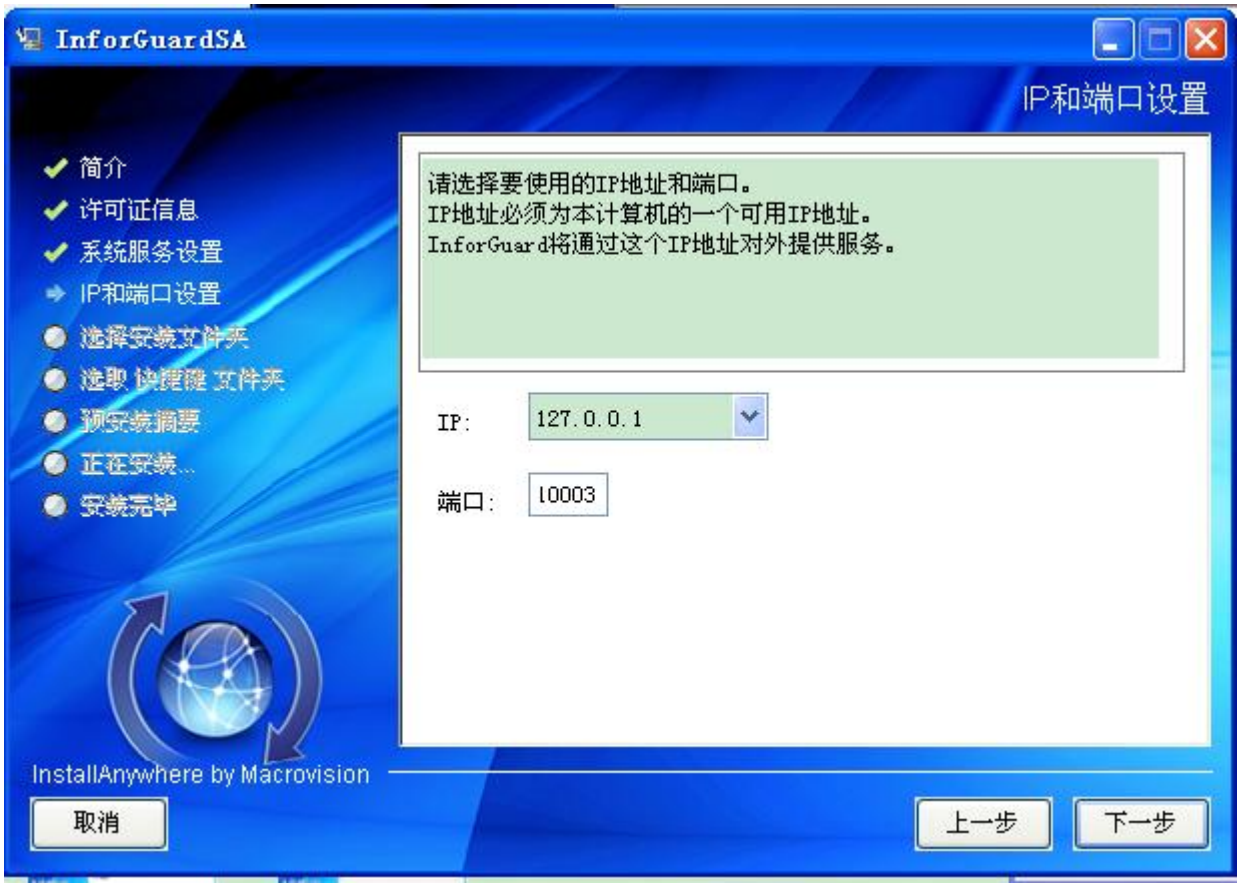


图 1-6

如果在安装后您想修改 InforGuard SA 所使用的 IP 地址和端口号，可以直接修改 SA 的配置文件 cfg\sa.xml。 里面的 app 节点的 localip 属性和 localport 属性对应这里输入的 IP 地址和端口号。

6. 下一步安装程序提示您输入要安装的路径。请注意不要选择有中文和空格的路径地址。

7. 在选择快捷方式后，如果您对之前输入的项没有疑问，点击"预安装摘要"的下一步后安装程序会将 InforGuard SA 装入您的计算机中。

1.2.3.2. Linux 上 InforGuard SA 的安装

InforGuard SA 在 Linux 上的安装过程如下:

1、选择安装 SA 的用户，可以是 ROOT 用户也可以是普通用户。

2、用上述选定的用户登陆 Linux 系统，拷贝安装包到本用户的目录。

3、若安装包为压缩格式，请先解压。解压后为目录，其中包含 install 文件。

4、执行上述目录下的文件 install（即执行./install），随后系统会显示版权信息，计算机 CPU 类型信息和产品版本信息，并提示用户是否继续安装。

注：若程序 install 不能够运行，一般是文件权限的问题，请改变这两个文件的权限为可执行/可读权限。然后继续执行 install。

5、输入字符 y ，之后敲回车键确认安装。

6、安装程序将提示输入安装全路径，SA 将安装到该目录下。如输入/usr/local，则 SA 安装后的目录为/usr/local/InforGuardSA。输入路径并回车。

7、修改 SA 安装目录中的配置文件。例如：vi /usr/local/InforGuardSA/cfg/sa.conf。找到 localip="127.0.0.1"，把 ip 地址改为 SA 进程希望绑定的本机 IP 地址。

8、SA 启动：在 SA 的 bin 目录下执行./sactl start

9、SA 停止：在 SA 的 bin 目录下执行./sactl stop

1.2.4. InforGuard MC 的安装

1.2.4.1. Windows 上 InforGuard MC 的安装

InforGuard MC 在 Windows 上的安装过程如下:

1．双击安装程序。

2．稍后会启动安装向导，并提示用户选择安装向导的提示语言种类。以下的步骤以简体中文语言为例说明。

3．稍后会出现安装提示界面，安装程序将指导您完成 InforGuard MC 的安装，如图 1-7:

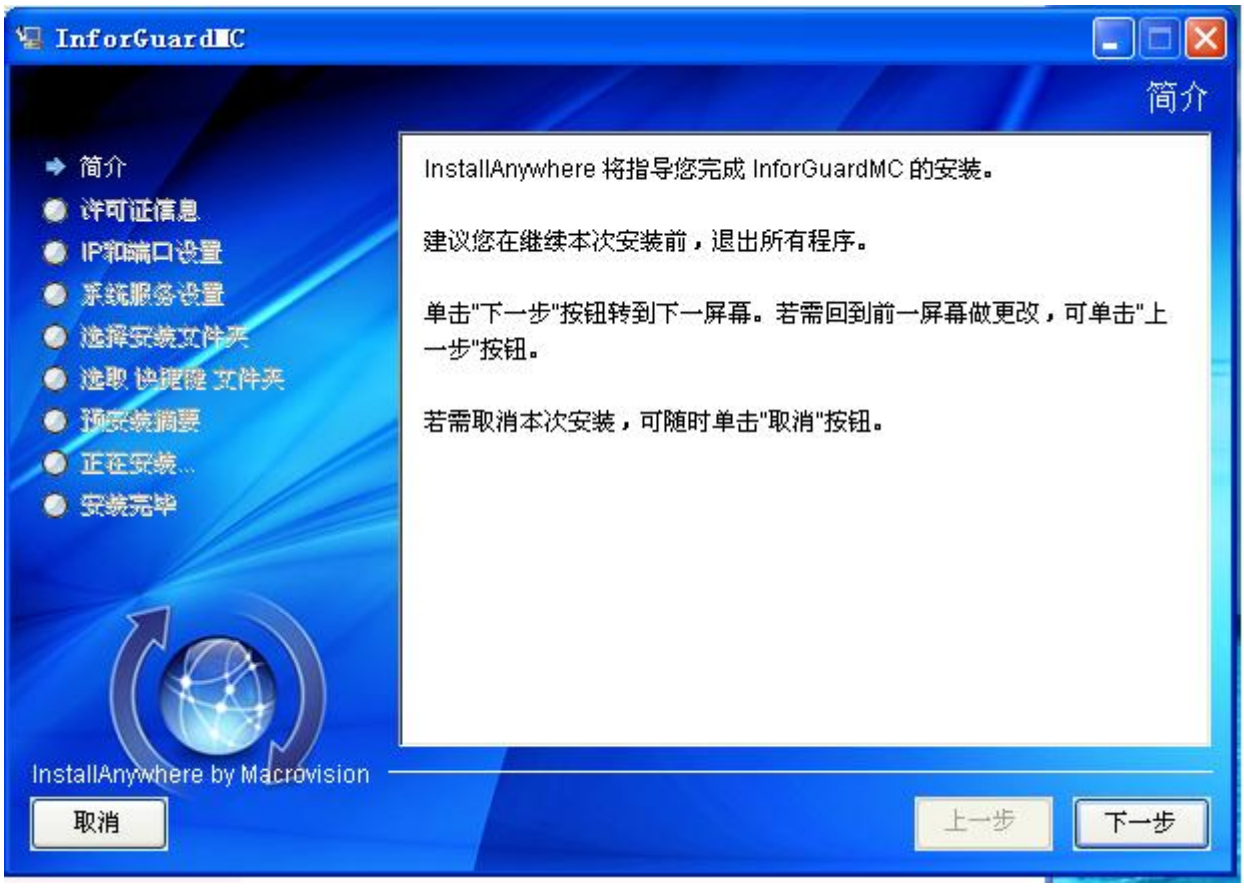


图 1-7

4. 接受 InforGuard 的 License 后，安装程序会提示您设置 MC 的 IP 地址和端口号，在此界面的 IP 地址下拉列表中，会列出您的 机器当前的所有 IP 地址。请选择一项和 InforGuard MA、InforGuard SA 在同一网段内的 IP 地址。InforGuard MC 将 使用此 IP 地址和 InforGuard MA、InforGuard SA 进行通讯。InforGuard MC 默认是用的端口号为 10004，请确认此 端口没有被占用。如果此端口已经被占用，请输入其他的端口号如图 1-8:

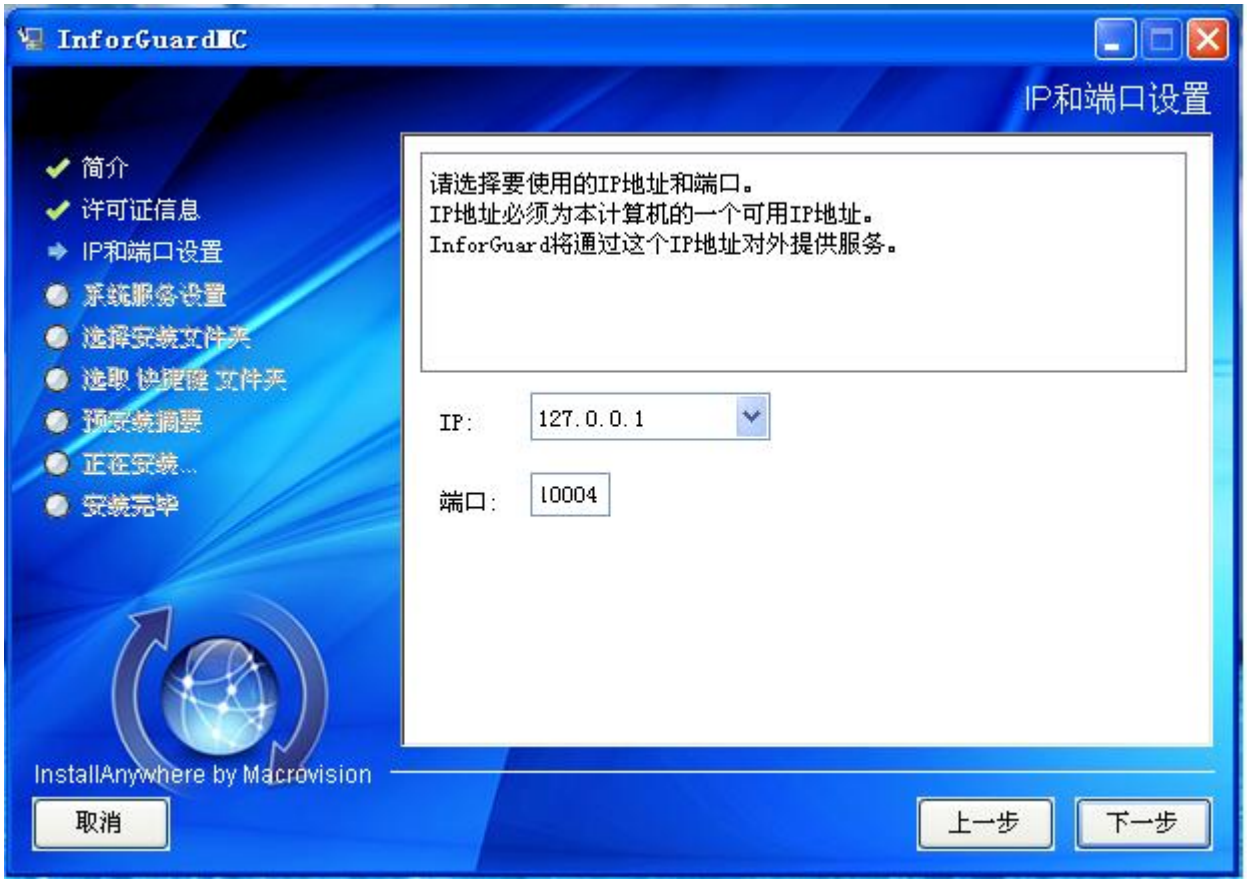


图 1-8

5. 下一步会提示是否将 InforGuard MC 设置为系统服务。选择设置为系统服务后，安装后您可以通过 Windows 的控制面板->管理工具->服务来管理 InforGuard MC 的启动和停止。如果您想每次都手动 控制 InforGuard MC 的启动和停止，请选择“否”，如图 1-9:

图 1-9

如果在安装后您想修改 InforGuard MC 所使用的 IP 地址和端口号，可以直接修改 MC 的配置文件 var\inforguard\managerConsole.xml。 里面的 mc 节点的 localip 属性和 localport 属性对应这里输入的 IP 地址和端口。

6. 下一步安装程序提示您输入要安装的路径。请注意不要选择有中文和空格的路径地址。

7. 在选择快捷方式后，如果您对之前输入的项没有疑问，点击"预安装摘要"的下一步后安装程序会将 InforGuard MC 装入您的计算机中。

1.2.4.2. Linux 上 InforGuard MC 的安装

要求 InforGuard MC 在安装时必须使用 root 用户安装，否则将不能正常使用。

InforGuard MC 在 Linux 上的安装有图形界面安装和命令行安装两种模式。

界面安装模式：

1．为安装文件增加可执行权限。使用 chmod +x InforGuardMC.bin 命令。

2．在图形界面下双击安装文件，运行此安装文件。注意：在某些 Linux 上，可能不允许文件后缀名为.bin 的文件的执行， 如果出现此问题您可以通过将后缀名改为.sh 来运行此文件。

3．此后的安装步骤同 Windows 上的安装。

命令行安装模式：

在 Linux 上，您还可以通过命令行方式来安装 InforGuard MC。方法如下：

1．在命令行终端下进入安装目录

2．为安装文件增加可执行权限。使用 chmod +x InforGuardMC.bin 命令。

3．在执行文件时增加 -i console 参数。执行./InforGuardMC.bin -i console

4．之后的安装步骤同图形界面相一致，只是将界面改为了字符提示方式,需要注意的是 Linux 上安装输入错误是不允许修改的, 所以用户在选择安装的产品时要保证输入信息的正确。

1.2.4.3. Linux 上 InforGuard MC jar 包的安装

要求 InforGuard MC 在安装时必须使用 root 用户安装，否则将不能正常使用。

InforGuard MC 在 Linux 上的安装有图形界面安装和命令行安装两种模式。

图形界面安装模式：

1．进入放置安装包的目录，解开安装包。

2．进入解开的安装包中，执行命令./install。

3．进入安装界面，此后的安装步骤同 Windows 上的安装。

命令行安装模式：

在 Linux 上，您还可以通过命令行方式来安装 InforGuard MC。方法如下：

1．进入放置安装包的目录，解开安装包。

2．进入解开的安装包中，执行命令./install -i console 。

3．之后的安装步骤同图形界面相一致，只是将界面改为了字符提示方式,需要注意的是 Linux 上安装输入错误是不允许修改的, 所以用户在选择安装的产品时要保证输入信息的正确。

1.2.4.4. Linux 上安装 InforGuard MC 的注意事项

InforGuard 要求 InforGuard MC 在安装时必须使用 root 用户安装，否则将不能正常使用。

1、为了工作方便，InforGuard MC 内置了一个管理用户 system(口令：manager)。为了系统的安全， InforGuard 用户应该尽快修改内置管理用户的口令。

2、在 Linux 上安装 InforGuard MC 时，有时会发现用户须知和许可协议显示为乱码。这是因为某些 Linux 默认的编码方式没有采用 GBK 的原因。将编码方式改为 GBK 后就可以看到正常汉字了。比如在 RedHat Linux 上可以使用 以下命令设置当前 Shell 的编码方式为 GBK：

export LANG=zh_CN.GBK

export LC_ALL=zh_CN.GBK：

3、 如果使用命令行方式安装时使用上一步的设置后仍然不能显示汉字，可能和当前使用的命令行终端的 编码设置有关。如 RedHat Linux 上图形界面终端可以通过菜单"终端->设置字符编码"来改变当前编码设置，改变为 GBK 后就可以正常显示汉字了。

4、在 Linux 上如果您将之前安装的 InforGuard MC 删除后又马上在另外一个位置安装了 InforGuard MC， 启动时可能还会找旧的 InforGuard MC 的目录造成启动失败。这是由于新装的 InforGuard MC 的环境变量还没有生效造成的。 通常情况下您只需注销一下即可正常启动 InforGuard MC 了。

5、在 SUSE Linux Enterprise Server10、Ubuntu7 等较新的 Linux 发行版里，直接执行安装程序可能会报错如下：

awk: error while loading shared libraries: libdl.so.2: cannot open shared object file: No such file or directory.....

这是因为 InstallAnyWhere 制作的安装包不支持这些 Linux 最新的线程库。如果遇到这种情况，您可以用以下方法来启动安装过程：

1. 将下面的内容保存为 InforGuardMC.sh 文件,并把它和安装包放置在同一目录下。

```
if [ 'uname -s' = "Linux" ];
 then
      if [ 'uname -m' != "ia64" ];
      then
                    'sed -i[.bak] -e 's/export LD_ASSUME_KERNEL/#xport LD_ASSUME_KERNEL/' $1'
      fi
 fi
 sh ./$1 $2 $3 $4 $5 $6 $7
```

2. 执行命令./InforGuardMC.sh InforGuardMC.bin 来启动安装进程。

3. 如果需要在命令行下安装，可以执行./InforGuardMC.sh InforGuardMC.bin -i console

1.2.5. 产品卸载

您可以通过两种方式来卸载 InforGuard。一种方法为，在 Windows 的控制面板->添加删除程序中， 找到 InforGuard 对应的程序项，如 InforGuard MA 等。通过它来卸载 InforGuard。也可以通过您安装时建立的卸载的快捷方式来卸载它。

请注意：

卸载 InforGuard 后只会删除在安装以后没有修改过的文件。这样可能在 InforGuard 的安装目录下 还残留了一些文件，如果您确定这些文件没有作用了，可以手工将其删除。如果有些安装后没有被修改的 文件在卸载时因为某些原因无法被删除，安装程序会提示您重启机器，在重启后自动删除这些文件。

1.3. 产品注册

1.3.1. 正式版产品注册授权

安装了 InforGuard 后，您需要进行产品注册授权，使 InforGuard 成为正式授权的产品，以保证 InforGuard 正常运行和获取正式的产品技术支持服务。

产品注册授权的流程如下：

1. 安装软件产品时，同意双方所履行的责任，通过后完成安装过程。

2. 通过邮件或其他方式将 InforGuardMC 下的 license.infor 发回中创软件商用中间件股份有限公司的版权控制部门， 版权部门制作一个正式版的 license.infor 文件返回。

3. 用户获取到版权控制人员发送来的 license 文件 license.infor 后，覆盖 InforGuardMC 的安装目录下的 linces.infor 文件即可。

1.3.2. 试用版升级到正式版注册授权

试用版升级为正式版的授权流程，请参照正式版的授权流程。

1.3.3. 产品升级注册授权

在产品升级时，将升级后的正式版授权文件覆盖 InforGuardMC 目录下授权文件即可。

1.4. 产品启停

1.4.1. 启动、停止 MA

1、Windows 上启停 MA：

安装 InforGuard MA 后，您可以通过安装时建立的快捷方式来启动。

启动后，将弹出一个 Cmd 窗口来显示启动的信息，如果您想停止 InforGuard MA, 在此窗口下键入 Ctrl+c 即可。如果您在安装时选择了设置为系统服务，那 InforGuard MA 将会在系统每次启动时自动启动，也可以通过 Windows 的控制面板->管理工具->服务中找到 InforGuardMA 的服务项，通过它来控制 InforGuard MA 的启动停止。

2、在 Linux 上启停 MA：

进入 MA 安装目录的 bin 目录下，执行命令./mactl start 启动 MA，执行命令./mactl stop 停止 MA。

1.4.2. 启动、停止 SA

1、在 Windows 上启停 SA：

安装 InforGuard SA 后，您可以通过您安装时建立的快捷方式来启动。

启动后，将弹出一个 Cmd 窗口来显示启动的信息，如果您想停止 InforGuard SA, 在此窗口下键入 Ctrl+c 即可。如果您在安装时选择了设置为系统服务，那 InforGuard SA 将会在系统每次启动时自动启动，也可以通过 Windows 的控制面板->管理工具->服务中找到 InforGuard SA 的服务项，通过它来控制 InforGuard SA 的启动停止。

2、在 Linux 上启停 SA：

进入 SA 安装目录的 bin 目录下，执行命令./sactl start 启动 MA，执行命令./sactl stop 停止 MA。

1.4.3. 启动、停止 MC

您可以通过您安装时建立的快捷方式来启动。如果您在安装时选择了设置为系统服务，那 InforGuard MC 将会在系统每次启动时自动启动， 也可以通过 Windows 的控制面板->管理工具->服务中找到 InforGuard MC 的服务项，通过它来控制 InforGuard MC 的启动停止。

InforGuard MC 启动结束后，可以使用快捷方式中的“访问 InforGuard 管理工具”来管理 InforGuard。

在 Linux 上，您可以通过执行 bin 目录下的 startup.sh 来启动 MC，通过执行 bin 目录下的 shutdown.sh 来停止 MC。

在 Linux 上，停止 MC 时会提示有如下操作：

1.提示输入用户名，输入 system 后回车

2.提示输入密码，输入 manager 后回车

3.提示输入端口，输入 1099 后回车

1.5. 访问管理工具及用户手册

1、访问管理工具

在浏览器地址栏中输入以下格式的ＵＲＬ地址：

http://安装 MC 的 IP:9090/inforguard

按回车即可链接到管理工具的登陆页面。

2、查看用户手册

在浏览器地址栏中输入以下格式的ＵＲＬ地址：

http://安装 MC 的 IP:9090/inforguard/help/index.html

按回车即可链接到用户手册的页面。

第 2 章 产品配置

2.1. Windows 上过滤器配置

2.1.1. Windows 上 Apache 过滤器的配置

第一步：修改配置文件

源文件：conf\httpd.conf

在 LoadModule 区域的最前面添加如下内容：

防篡改过滤器：LoadModule guard_module modules\mod_guard_xx.so

防注入过滤器：LoadModule guard_module_sql modules\mod_guard_sql_xx.so

mod_guard_xx.so 中的 xx 表示加载过滤器的 apache 的版本系列，如果 apache 是 2.0 系列的，xx 值为 2.0，若 apache 为 2.2 系列的， 则 xx 值为 2.2。

第二步：复制模块文件

32 位防篡改过滤器：源文件：filter\apache\bit32\mod_guard_xx.so，目标文件：modules\mod_guard_xx.so

64 位防篡改过滤器：源文件：filter\apache\bit64\mod_guard_xx.so，目标文件：modules\mod_guard_xx.so

32 位防注入过滤器：源文件：filter\apache\bit32\mod_guard_sql_xx.so，目标文件：modules\mod_guard_sql_xx.so

64 位防注入过滤器：源文件：filter\apache\bit64\mod_guard_sql_xx.so，目标文件：modules\mod_guard_sql_xx.so

第三步：修改环境变量

打开 Windows 系统的“环境变量”管理界面，编辑系统变量中的 Path 项，在其中增加 InforGuard MA 安装目录下的 bin 目录，即如下内容：

```
32 位过滤器：X:\CVICSE\InforGuardMA\bin
64 位过滤器：X:\CVICSE\InforGuardMA\bin\bit64
```

具体内容与安装路径一致

此时启动 Apache，如果没有看到错误信息，则表示过滤器配置正确。

说明一：过滤器版本不匹配错误

如果在 Apache 启动时，界面显示以下错误信息，则表示过滤器版本不匹配。

Syntax error on line 135 of D:/Apache2.0.63/conf/httpd.conf:

API module structure 'guard_module_sql' in file D:/Apache2.0.63/modules/mod_guard_sql.so is garbled - expected signature 41503230 but saw 41503232 - perhaps this is not an Apache module DSO, or was compiled for a different Apache version?

由于 Apache 各个版本之间对过滤器的支持存在差异，需要针对不同的 Apache 版本提供相应版本的过滤器模块文件。

说明二：64 位 Apache 应用服务器

在 64 位操作系统上，可以运行 32 位的 Apache 应用服务器，也可以运行 64 位的 Apache 应用服务器。 如果是 64 位的 Apache 应用服务器，还要区分服务器的 CPU 架构：目前市面上的 CPU 主要分为两大阵营，一个是 Intel 系列 CPU， 另一个是 AMD 系列 CPU，通常将采用 Intel 处理器的服务器称为 IA(Intel Architec-ture)架构服务器；将采用 AMD 处理器的服务器称为 x86-64 架构。

以上差异需要在第二步复制模块文件和第三步修改环境变量时区别对待，对采用 IA 架构的 64 位 Apache，复制文件和修改环境变量时使用 X:\CVICSE\InforGuardMA\bin\bit64 目录，对采用 x86-64 架构的 64 位 Apache，使用 X:\CVICSE\InforGuardMA\bin\bit64 目录。

2.1.2. Windows 上 IIS 过滤器的配置

第一步：配置 IIS 筛选器

打开 IIS 管理器，在“网站”结点下，打开需要配置过滤器的网站属性，选择“ISAPI 筛选器”标签页，添加筛选器，名称自定义。

防篡改过滤器：选择文件 X:\CVICSE\InforGuard MA\bin\IISFilter.dll，然后确定退出。

防注入过滤器：选择文件 X:\CVICSE\InforGuard MA\bin\IISFilterSql.dll，然后确定退出。

第二步：修改环境变量

打开 Windows 系统的“环境变量”管理界面，编辑系统变量中的 Path 项，在其中增加 InforGuardMA 安装目录下的 bin 目录，即如下内容：

```
X:\CVICSE\InforGuardMA\bin
```

具体内容与安装路径一致。

说明一：64 位 IIS 应用服务器

在 64 位操作系统上，需要区分服务器的 CPU 架构：目前市面上的 CPU 主要分为两大阵营，一个是 Intel 系列 CPU，另一个是 AMD 系列 CPU，通常将采用 Intel 处理器的服务器称为 IA(Intel Architec-ture)架构服务器；将采用 AMD 处理器的服务器称为 x86-64 架构。

以上差异需要在第二步复制模块文件和第三步修改环境变量时区别对待，对采用 IA 架构的 64 位 IIS，复制文件和修改环境变量时使用 X:\CVICSE\InforGuardMA\bin\IA64 目录，对采用 x86-64 架构的 64 位 IIS，使用 X:\CVICSE\InforGuardMA\bin\AMD64 目录。

2.1.3. Windows 上 Tomcat 过滤器的配置

第一步：修改配置文件

源文件：WEB-INF\web.xml

说明：需要对哪个应用进行保护，就要对该应用的 web.xml 文件进行修改，多个应用就修改多个文件。

修改方式：严格按照配置文件 web.xml 的标签顺序（<!ELEMENT web-app (icon?, display-name?, description?, distributable?, context-param*, filter*, filter-mapping*, listener*, servlet*, servlet-mapping*, session-config?, mime-mapping*, welcome-file-list?, error-page*, taglib*, resource-env-ref*, resource-ref*, security-constraint*, login-config?, security-role*, env-entry*, ejb-ref*, ejb-local-ref*)>）在合适的位置添加如下代码。

```
<filter>
  <filter-name>FilterName</filter-name>
  <filter-class>com.cvicse.inforguard.FilterName</filter-class>
  <init-param>
    <param-name>rootpathflag</param-name>
    <param-value>value</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>FilterName</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

在以上代码段中，若加载防篡改过滤器，则将代码中所有的 FilterName 替换为 InforGuardFilter，若加载防注入过滤器，则替换为 InforGuardFilterSql。value 的值默认为 1， 如果获取不到应用的路径，则将 value 值设置为 0。

第二步：复制类包文件

防篡改过滤器：源文件：filter\jee\InforGuardFilter.jar，目标文件：WEB-INF\lib\InforGuardFilter.jar

防注入过滤器：源文件：filter\jee\InforGuardFilterSql.jar，目标文件：WEB-INF\lib\InforGuardFilterSql.jar

说明：如果在 WEB-INF 目录下不存在 lib 目录，则手工创建后，再复制文件。

第三步：复制类包文件

Tomcat 5 系列：

防篡改过滤器：源文件：filter\jee\InforGuardValidator.jar，目标文件：common\lib\InforGuardValidator.jar

防注入过滤器：源文件：filter\jee\InforGuardValidatorSql.jar，目标文件：common\lib\InforGuardValidatorSql.jar

Tomcat 6 系列：

防篡改过滤器：源文件：filter\jee\InforGuardValidator.jar，目标文件：lib\InforGuardValidator.jar

防注入过滤器：源文件：filter\jee\InforGuardValidatorSql.jar，目标文件：lib\InforGuardValidatorSql.jar

说明：该 lib 目录是应用服务器总的 lib 目录，不是 WEB-INF 目录下的 lib 目录。

第四步：修改环境变量

打开 Windows 系统的“环境变量”管理界面，编辑系统变量中的 Path，在其中增加 InforGuardMA 安装目录下的 bin 目录，即如下内容：

```
X:\CVICSE\InforGuardMA\bin
```

具体内容与安装路径一致。

此时启动 Tomcat，如果没有看到错误信息，则表示过滤器配置正确。

2.1.4. Windows 上 WebLogic 过滤器的配置

第一步：修改配置文件

源文件：WEB-INF\web.xml

说明：需要对哪个应用进行保护，就要对该应用的 web.xml 文件进行修改，多个应用就修改多个文件。

修改方式：严格按照配置文件 web.xml 的标签顺序（<!ELEMENT web-app (icon?, display-name?, description?, distributable?, context-param*, filter*, filter-mapping*, listener*, servlet*, servlet-mapping*, session-config?, mime-mapping*, welcome-file-list?, error-page*, taglib*, resource-env-ref*, resource-ref*, security-constraint*, login-config?, security-role*, env-entry*, ejb-ref*, ejb-local-ref*)>） 在合适的位置添加如下代码。

```
<filter>
  <filter-name>FilterName</filter-name>
  <filter-class>com.cvicse.inforguard.FilterName</filter-class>
  <init-param>
```

```
    <param-name>rootpathflag</param-name>
    <param-value>value</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>FilterName</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

在以上代码段中，若加载防篡改过滤器，则将代码中所有的 FilterName 替换为 InforGuardFilter，若加载防注入过滤器，则替换为 InforGuardFilterSql。value 的值默认为 1， 如果获取不到应用的路径，则将 value 值设置为 0。

第二步：复制类包文件

防篡改过滤器：源文件：filter\jee\InforGuardFilter.jar 目标文件：WEB-INF\lib\InforGuardFilter.jar

防注入过滤器：源文件：filter\jee\InforGuardFilterSql.jar 目标文件：WEB-INF\lib\InforGuardFilterSql.jar

说明：如果在 WEB-INF 目录下不存在 lib 目录，则手工创建后，再复制文件。

第三步：复制类包文件

防篡改过滤器：源文件：filter\jee\InforGuardValidator.jar 目标文件：common\lib\InforGuardValidator.jar

防注入过滤器：源文件：filter\jee\InforGuardValidatorSql.jar 目标文件：common\lib\InforGuardValidatorSql.jar

说明：该 lib 目录是应用服务器总的 lib 目录，不是 WEB-INF 目录下的 lib 目录。

第四步：修改环境变量

修改启动脚本 startWebLogic.cmd，添加如下内容：

```
set INFORGUARD_AGENT_PATH=InforGuardMA 安装目录
set PATH=InforGuardMA 安装目录\bin;%PATH%
防篡改过滤器：set CLASSPATH=(weblogic 安装目
录)\weblogicx.x\common\lib\InforGuardValidator.jar;%CLASSPATH%
防注入过滤器：set CLASSPATH= (weblogic 安装目
录)\weblogicx.x\common\lib\InforGuardValidatorSql.jar;%CLASSPATH%
```

weblogicx.x 中的 x.x 表示 weblogic 的具体版本号，在设置 CLASSPATH 时，找到输出 CLASSPATH 的地方，在输出前一行添加以上设置 CLASSPATH 的语句，此时启动 Weblogic，如果没有看到错误信息，则表示过滤器配置正确。

2.1.5. Windows 上 Websphere 过滤器的配置

第一步：修改配置文件

源文件：WEB-INF\web.xml

说明：需要对哪个应用进行保护，就要对该应用的 web.xml 文件进行修改，多个应用就修改多个文件。

修改方式：严格按照配置文件 web.xml 的标签顺序（<!ELEMENT web-app (icon?, display-name?, description?, distributable?, context-param*, filter*, filter-mapping*, listener*, servlet*, servlet-mapping*, session-config?, mime-mapping*, welcome-file-list?, error-page*, taglib*, resource-env-ref*, resource-ref*, security-

constraint*, login-config?, security-role*, env-entry*, ejb-ref*, ejb-local-ref*)>） 在合适的位置添加如下代码。

```
<filter>
  <filter-name>FilterName</filter-name>
  <filter-class>com.cvicse.inforguard.FilterName</filter-class>
  <init-param>
    <param-name>rootpathflag</param-name>
    <param-value>value</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>FilterName</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

在以上代码段中，若加载防篡改过滤器，则将代码中所有的 FilterName 替换为 InforGuardFilter，若加载防注入过滤器，则替换为 InforGuardFilterSql。value 的值默认为 1， 如果获取不到应用的路径，则将 value 值设置为 0。

第二步：复制类包文件

防篡改过滤器：源文件：filter\jee\InforGuardFilter.jar 目标文件：WEB-INF\lib\InforGuardFilter.jar

防注入过滤器：源文件：filter\jee\InforGuardFilterSql.jar 目标文件：WEB-INF\lib\InforGuardFilterSql.jar

说明：如果在 WEB-INF 目录下不存在 lib 目录，则手工创建后，再复制文件。

第三步：复制类包文件

防篡改过滤器：源文件：filter\jee\InforGuardValidator.jar 目标文件：\WebSphere\AppServer\lib\InforGuardValidator.jar

防注入过滤器：源文件：filter\jee\InforGuardValidatorSql.jar 目标文件：\WebSphere\AppServer\lib\InforGuardValidatorSql.jar

说明：该 lib 目录是应用服务器总的 lib 目录，不是 WEB-INF 目录下的 lib 目录。

第四步：修改环境变量

修改启动脚本 startServer.bat，添加如下内容：

```
set INFORGUARD_AGENT_PATH=InforGuardMA 安装目录
set PATH=InforGuardMA 安装目录\bin;%PATH%
```

修改 setupCmdLine.bat，修改内容如下:

```
防篡改过滤器：
WAS_CLASSPATH=%WAS_HOME%\properties;%WAS_HOME%\lib\InforGuardValidator.jar;
防注入过滤器：
WAS_CLASSPATH=%WAS_HOME%\properties;%WAS_HOME%\lib\InforGuardValidatorSql.jar;
```

注：在修改 WEB-INF\web.xml 之后，如果不重新部署一下的话，过滤器不会起作用，因为 Websphere 缓存了 web.xml 的内容。

此时启动 Websphere，如果没有看到错误信息，则表示过滤器配置正确。

2.2. Linux/UNIX 过滤器的配置

2.2.1. Linux/UNIX 上 Apache 过滤器的配置

第一步：修改配置文件

源文件：conf/httpd.conf

在 LoadModule 区域的最前面添加如下内容：

防篡改过滤器：LoadModule guard_module modules/mod_guard_xx.so

防注入过滤器：LoadModule guard_module_sql modules/mod_guard_sql_xx.so

mod_guard_xx.so 中的 xx 表示加载过滤器的 apache 的版本系列，如果 apache 是 2.0 系列的，xx 值为 20，若 apache 为 2.2 系列的， 则 xx 值为 22。

第二步：复制模块文件

32 位防篡改过滤器：源文件：filter/apache/bit32/mod_guard_xx.so，目标文件：modules/mod_guard_xx.so

64 位防篡改过滤器：源文件：filter/apache/bit64/mod_guard_xx.so，目标文件：modules/mod_guard_xx.so

32 位防注入过滤器：源文件：filter/apache/bit32/mod_guard_sql_xx.so，目标文件：modules/mod_guard_sql_xx.so

64 位防注入过滤器：源文件：filter/apache/bit64/mod_guard_sql_xx.so，目标文件：modules/mod_guard_sql_xx.so

第三步：修改环境变量

打开 Apache 启动脚本文件 bin/apachectl，在其中增加 InforGuard MA 安装目录及其下的 bin 目录，即如下内容：

```
export INFORGUARD_AGENT_PATH=InforGuardMA 安装目录
32 位:export LD_LIBRARY_PATH=InforGuardMA 安装目录/bin:$LD_LIBRARY_PATH
64 位:export LD_LIBRARY_PATH=InforGuardMA 安装目录
/bin/bit64:$LD_LIBRARY_PATH
```

注意：LD_LIBRARY_PATH 在不同系统中名字有所区别：AIX 上为 LIBPATH，HP-UX 上为 SHLIB_PATH，Solaris 和 Linux 上为 LD_LIBRARY_PATH；此外在 HPPA 上如果还是找不到 mod_guard_sql-xx.so 文件，可以添加：export LD_PRELOAD=(apache 安装目录)/modules/模块名称 或 export LD_PRELOAD=/usr/lib/libpthread.sl :(apache 安装目录)/modules/模块名称。

具体内容与安装路径一致，位置尽量靠前（可以放在第一行）。

此时启动 Apache，如果没有看到错误信息，则表示过滤器配置正确。

2.2.2. Linux/UNIX 上 Tomcat 过滤器的配置

第一步：修改配置文件

源文件：WEB-INF/web.xml

说明：需要对哪个应用进行保护，就要对该应用的 web.xml 文件进行修改，多个应用就修改多个文件。

修改方式：严格按照配置文件 web.xml 的标签顺序（<!ELEMENT web-app (icon?, display-name?, description?, distributable?, context-param*, filter*, filter-mapping*, listener*, servlet*, servlet-mapping*, session-config?, mime-mapping*, welcome-file-list?, error-page*, taglib*, resource-env-ref*, resource-ref*, security-

constraint*, login-config?, security-role*, env-entry*, ejb-ref*, ejb-local-ref*)>） 在合适的位置添加如下代码。

```
<filter>
  <filter-name>FilterName</filter-name>
  <filter-class>com.cvicse.inforguard.FilterName</filter-class>
  <init-param>
    <param-name>rootpathflag</param-name>
    <param-value>value</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>FilterName</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

在以上代码段中，若加载防篡改过滤器，则将代码中所有的 FilterName 替换为 InforGuardFilter，若加载防注入过滤器，则替换为 InforGuardFilterSql。value 的值默认为 1， 如果获取不到应用的路径，则将 value 值设置为 0。

第二步：复制类包文件

防篡改过滤器：源文件：filter/jee/InforGuardFilter.jar 目标文件：WEB-INF/lib/InforGuardFilter.jar

防注入过滤器：源文件：filter/jee/InforGuardFilterSql.jar 目标文件：WEB-INF/lib/InforGuardFilterSql.jar

说明：如果在 WEB-INF 目录下不存在 lib 目录，则手工创建后，再复制文件。

第三步：复制类包文件

Tomcat 5 系列：

防篡改过滤器：源文件：filter/jee/InforGuardValidator.jar 目标文件：common/lib/InforGuardValidator.jar

防注入过滤器：源文件：filter/jee/InforGuardValidatorSql.jar 目标文件：common/lib/InforGuardValidatorSql.jar

Tomcat 6 系列：

防篡改过滤器：源文件：filter\jee\InforGuardValidator.jar，目标文件：lib\InforGuardValidator.jar

防注入过滤器：源文件：filter\jee\InforGuardValidatorSql.jar，目标文件：lib\InforGuardValidatorSql.jar

说明：该 lib 目录是应用服务器总的 lib 目录，不是 WEB-INF 目录下的 lib 目录。

第四步：修改环境变量

修改 Tomcat 的启动脚本 startup.sh 靠前的适当位置（或者第一行），加入 InforGuard MA 的环境变量，将 MA 安装路径的 bin 目录 (如/usr/InforGuardMA/bin) 加入到 LIBRARY_PATH 变量中，例如：

```
export INFORGUARD_AGENT_PATH=InforGuardMA 安装目录
export LD_LIBRARY_PATH=InforGuardMA 安装目录/bin:$LD_LIBRARY_PATH
```

注意：LD_LIBRARY_PATH 在不同系统中名字有所区别：AIX 上为 LIBPATH，HP-UX 上为 SHLIB_PATH，Solaris 和 Linux 上为 LD_LIBRARY_PATH； 此外在 HPPA 上如果还是找不到 mod_guard_sql-xx.so 文件，可以添加：export

LD_PRELOAD=(tomcat 安装目录)/../WEB—INF/lib/模块名称 或 export LD_PRELOAD=/usr/lib/libpthread.sl :(tomcat 安装目录)/../WEB—INF/lib/模块名称。

此时启动 Tomcat，如果没有看到错误信息，则表示过滤器配置正确。

2.2.3. Linux/UNIX 上 Websphere 过滤器的配置

第一步：修改配置文件

源文件：WEB-INF/web.xml

说明：需要对哪个应用进行保护，就要对该应用的 web.xml 文件进行修改，多个应用就修改多个文件。

修改方式：严格按照配置文件 web.xml 的标签顺序（<!ELEMENT web-app (icon?, display-name?, description?, distributable?, context-param*, filter*, filter-mapping*, listener*, servlet*, servlet-mapping*, session-config?, mime-mapping*, welcome-file-list?, error-page*, taglib*, resource-env-ref*, resource-ref*, security-constraint*, login-config?, security-role*, env-entry*, ejb-ref*, ejb-local-ref*)>） 在合适的位置添加如下代码。

```
<filter>
  <filter-name>FilterName</filter-name>
  <filter-class>com.cvicse.inforguard.FilterName</filter-class>
  <init-param>
    <param-name>rootpathflag</param-name>
    <param-value>value</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>FilterName</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

在以上代码段中，若加载防篡改过滤器，则将代码中所有的 FilterName 替换为 InforGuardFilter，若加载防注入过滤器，则替换为 InforGuardFilterSql。value 的值默认为 1， 如果获取不到应用的路径，则将 value 值设置为 0。

第二步：复制类包文件

防篡改过滤器：源文件：filter/jee/InforGuardFilter.jar 目标文件：WEB-INF/lib/InforGuardFilter.jar

防注入过滤器：源文件：filter/jee/InforGuardFilterSql.jar 目标文件：WEB-INF/lib/InforGuardFilterSql.jar

说明：如果在 WEB-INF 目录下不存在 lib 目录，则手工创建后，再复制文件。

第三步：复制类包文件

防篡改过滤器：源文件：filter/jee/InforGuardValidator.jar 目标文件：/WebSphere/AppServer/lib/InforGuardValidator.jar

防注入过滤器：源文件：filter/jee/InforGuardValidatorSql.jar 目标文件：/WebSphere/AppServer/lib/InforGuardValidatorSql.jar

说明：该 lib 目录是应用服务器总的 lib 目录，不是 WEB-INF 目录下的 lib 目录。

第四步：修改环境变量

修改启动脚本 startServer.sh，添加如下内容：

```
export INFORGUARD_AGENT_PATH=InforGuardMA 安装目录
export LD_LIBRARY_PATH=InforGuardMA 安装目录/bin:$LD_LIBRARY_PATH
```

注意：LD_LIBRARY_PATH 在不同系统中名字有所区别：AIX 上为 LIBPATH，HP-UX 上为 SHLIB_PATH，Solaris 和 Linux 上为 LD_LIBRARY_PATH； 此外在 HPPA 上如果还是找不到 mod_guard_sql-xx.so 文件，可以添加：export LD_PRELOAD=export LD_PRELOAD=(websphere 安装目录)/../WEB—INF/lib/模块名称 或 export LD_PRELOAD=/usr/lib/libpthread.sl :(websphere 安装目录)/../WEB—INF/lib/模块名称。

修改 setupCmdLine.sh，修改内容如下:

```
防篡改过滤器：
WAS_CLASSPATH="$WAS_HOME"/properties:"$WAS_HOME"/lib/InforGuardValidator.jar:
防注入过滤器：
WAS_CLASSPATH="$WAS_HOME"/properties:"$WAS_HOME"/lib/InforGuardValidatorSql.jar:
```

注：在修改 WEB-INF/web.xml 之后，如果不重新部署一下的话，过滤器不会起作用，因为 Websphere 缓存了 web.xml 的内容。

此时启动 Websphere，如果没有看到错误信息，则表示过滤器配置正确。

2.2.4. Linux/UNIX 上 WebLogic 过滤器的配置

第一步：修改配置文件

源文件：WEB-INF/web.xml

说明：需要对哪个应用进行保护，就要对该应用的 web.xml 文件进行修改，多个应用就修改多个文件。

修改方式：严格按照配置文件 web.xml 的标签顺序（<!ELEMENT web-app (icon?, display-name?, description?, distributable?, context-param*, filter*, filter-mapping*, listener*, servlet*, servlet-mapping*, session-config?, mime-mapping*, welcome-file-list?, error-page*, taglib*, resource-env-ref*, resource-ref*, security-constraint*, login-config?, security-role*, env-entry*, ejb-ref*, ejb-local-ref*)>） 在合适的位置添加如下代码。

```
<filter>
  <filter-name>FilterName</filter-name>
  <filter-class>com.cvicse.inforguard.FilterName</filter-class>
  <init-param>
    <param-name>rootpathflag</param-name>
    <param-value>value</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>FilterName</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

在以上代码段中，若加载防篡改过滤器，则将代码中所有的 FilterName 替换为 InforGuardFilter，若加载防注入过滤器，则替换为 InforGuardFilterSql。value 的值默认为 1， 如果获取不到应用的路径，则将 value 值设置为 0。

第二步：复制类包文件

防篡改过滤器：源文件：filter/jee/InforGuardFilter.jar 目标文件：WEB-INF/lib/InforGuardFilter.jar

防注入过滤器：源文件：filter/jee/InforGuardFilterSql.jar 目标文件：WEB-INF/lib/InforGuardFilterSql.jar

说明：如果在 WEB-INF 目录下不存在 lib 目录，则手工创建后，再复制文件。

第三步：复制类包文件

防篡改过滤器：源文件：filter/jee/InforGuardValidator.jar 目标文件：common/lib/InforGuardValidator.jar

防注入过滤器：源文件：filter/jee/InforGuardValidatorSql.jar 目标文件：common/lib/InforGuardValidatorSql.jar

说明：该 lib 目录是应用服务器总的 lib 目录，不是 WEB-INF 目录下的 lib 目录。

第四步：修改环境变量

修改启动脚本 startWebLogic.sh，添加如下内容：

```
export INFORGUARD_AGENT_PATH=InforGuardMA 安装目录
export LD_LIBRARY_PATH=InforGuardMA 安装目录/bin:$LD_LIBRARY_PATH
防篡改过滤器：export CLASSPATH= (weblogic 安装目
录)/weblogicx.x/common/lib/InforGuardValidator.jar:$CLASSPATH
防注入过滤器：export CLASSPATH= (weblogic 安装目
录)/weblogicx.x/common/lib/InforGuardValidatorSql.jar:$CLASSPATH
```

注意：weblogicx.x 中的 x.x 表示 weblogic 的具体版本号，LD_LIBRARY_PATH 在不同系统中名字有所区别：AIX 上为 LIBPATH，HP-UX 上为 SHLIB_PATH，Solaris 和 Linux 上为 LD_LIBRARY_PATH；此外在 HPPA 上如果还是找不到 mod_guard_sql-xx.so 文件，可以添加：export LD_PRELOAD=(weblogic 安装目录)/../WEB—INF/lib/ 模块名称 或 export LD_PRELOAD=/usr/lib/libpthread.sl :(weblogic 安装目录)/../WEB—INF/lib/模块名称。

此时启动 Weblogic，如果没有看到错误信息，则表示过滤器配置正确。

2.2.5. Linux/UNIX 上 OC4J 过滤器的配置

第一步：修改配置文件

源文件：WEB-INF/web.xml

说明：需要对哪个应用进行保护，就要对该应用的 web.xml 文件进行修改，多个应用就修改多个文件。

修改方式：严格按照配置文件 web.xml 的标签顺序（<!ELEMENT web-app (icon?, display-name?, description?, distributable?, context-param*, filter*, filter-mapping*, listener*, servlet*, servlet-mapping*, session-config?, mime-mapping*, welcome-file-list?, error-page*, taglib*, resource-env-ref*, resource-ref*, security-constraint*, login-config?, security-role*, env-entry*, ejb-ref*, ejb-local-ref*)>） 在合适的位置添加如下代码。

```
<filter>
  <filter-name>FilterName</filter-name>
  <filter-class>com.cvicse.inforguard.FilterName</filter-class>
  <init-param>
    <param-name>rootpathflag</param-name>
    <param-value>value</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>FilterName</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

在以上代码段中，若加载防篡改过滤器，则将代码中所有的 FilterName 替换为 InforGuardFilter，若加载防注入过滤器，则替换为 InforGuardFilterSql。value 的值默认为 1， 如果获取不到应用的路径，则将 value 值设置为 0。

第二步：复制类包文件

防篡改过滤器：源文件：filter/jee/InforGuardFilter.jar 目标文件：WEB-INF/lib/InforGuardFilter.jar

防注入过滤器：源文件：filter/jee/InforGuardFilterSql.jar 目标文件：WEB-INF/lib/InforGuardFilterSql.jar

说明：如果在 WEB-INF 目录下不存在 lib 目录，则手工创建后，再复制文件。

第三步：复制类包文件

防篡改过滤器：源文件：filter/jee/InforGuardValidator.jar 目标文件：j2EE/home/jsp/lib/taglib/InforGuardValidator.jar

防注入过滤器：源文件：filter/jee/InforGuardValidatorSql.jar 目标文件：j2EE/home/jsp/lib/taglib/InforGuardValidatorSql.jar

说明：该 lib 目录在应用服务器 oc4j 安装目录下，不是 WEB-INF 目录下的 lib 目录。

第四步：修改环境变量

在 oc4j 的 web 服务器里面加载我们环境变量，由于不是 oc4j 不采用外部加载环境变量的方式，而是采用变量传递的方式来加载环境变量； 因此环境变量要加载到 oc4j 安装目录下 opmn/conf/opmn.xml 里面

在 j2EE/home 下创建文件 start.sh(可以直接用命令 vi start.sh,则打开了一个名为 start.sh 的空文件)在此文件中添加如下内容：

```
<environment>
  <variable id="INFORGUARD_AGENT_PATH" value="InforGuardMA 的安装目录"
append="false"/>
  <variable id="LD_LIBRARY_PATH" value="InforGuardMA 安装目录/bin"
append="true"/>
</environment>
```

注意：LD_LIBRARY_PATH 在不同系统中名字有所区别：AIX 上为 LIBPATH，HP-UX 上为 SHLIB_PATH，Solaris 和 Linux 上为 LD_LIBRARY_PATH； 此外在 HPPA 上如果还是找不到 mod_guard_sql-xx.so 文件，可以添加：export LD_PRELOAD=(tomcat 安装目录)/../WEB—INF/lib/模块名称 或 export LD_PRELOAD=/usr/lib/libpthread.sl :(tomcat 安装目录)/../WEB—INF/lib/模块名称。

1.每个 ias-component 标签内只能出现一个 environment 标签;若要添的 ias-component 内已经存在了 environment 标签，则直接在其中增加我们的变量。否则要一起添加。

2.若 ias-component 标签的属性 status="disabled"，表示该标签已被禁用，在其中添加的环境变量不起作用。

3.若在 opmn.xml 文件中有-Djava.library.path=“xxx 路径”的内容，则要在其中添加“InforGuardMA 安装路径/bin”。

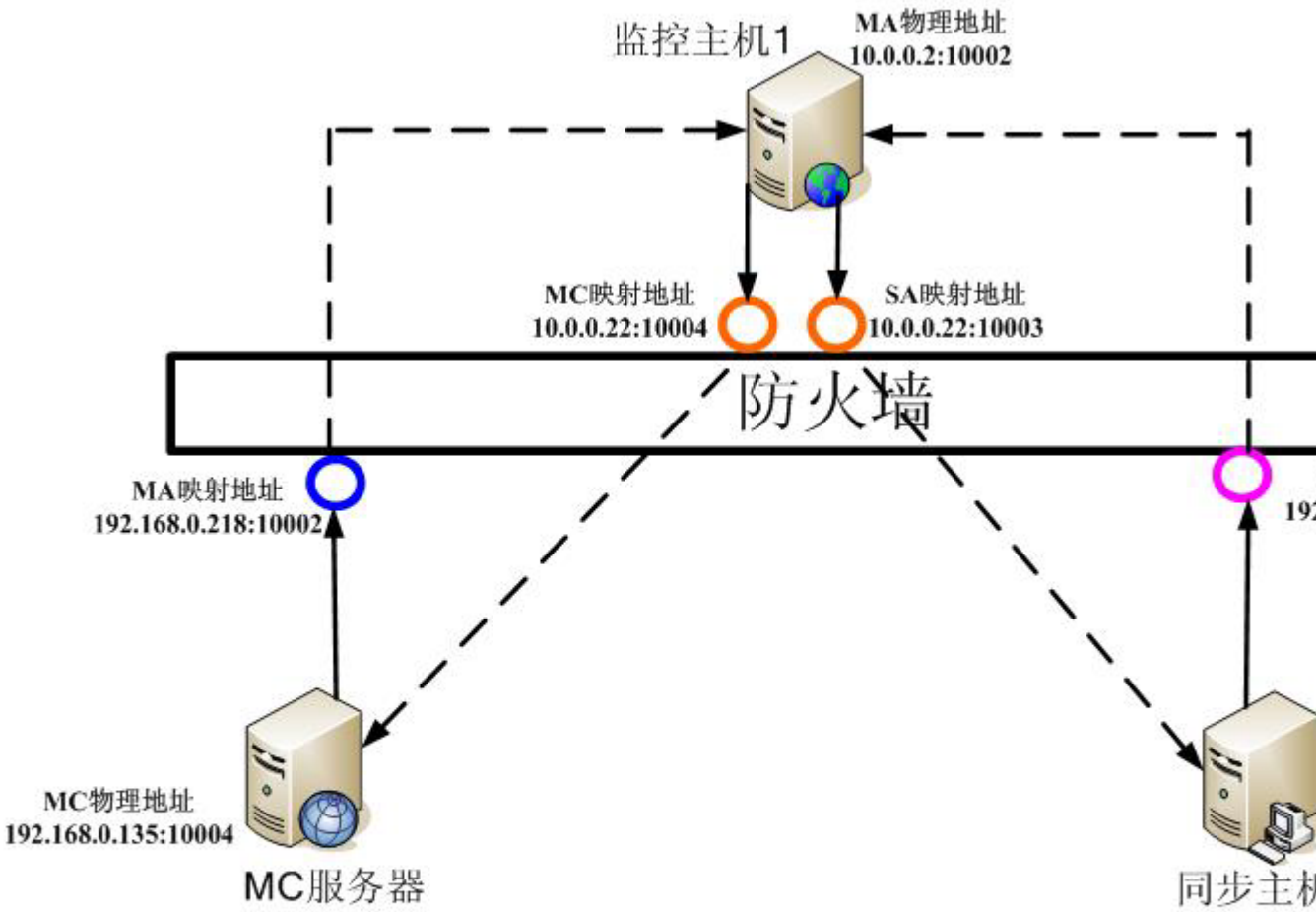
此时启动 OC4J，如果没有看到错误信息，则表示过滤器配置正确。

2.3. 防火墙的配置

2.3.1. 只有监控端有防火墙的配置

1、场景描述

以下以只有监控端有防火墙的情型为例进行描述，具体场景如图 2-1：



网站服务器位于独立区域，同步、管理服务器位于

原始场景

图 2-1

上图描述的场景是监控主机（即网站服务器），单独位于防火墙一侧；同步主机和 MC 管理服务器位于防火墙另一侧的情形。

此处假设防火墙配置为最复杂的情况，防火墙配置为默认双向禁止通信，即防火墙两边的主机物理 IP 互相不可见；实现双向通讯的方式是， 在防火墙配置 IP 和 Port 映射，通过访问映射的 IP 和 Port 可以访问到另一侧的应用。

通过图 2-1，可以得出如下地址映射表：

服务名	物理地址	映射地址	备注
MA	10.0.0.2:10002	192.168.0.218:10002	SA 和 MC 通过映射地址访问 MA
SA	192.168.0.135:10003	10.0.0.22:10003	MA 通过映射地址访问 SA； MC 通过物理地址访问 SA
MC	192.168.0.135:10004	10.0.0.22:10004	MA 通过映射地址访问 MC； SA 通过物理地址访问 MC

2、防火墙通讯验证

建议实际部署 InforGuard 之前，先使用测试程序验证防火墙配置是否已经满足 InforGuard 通讯需要。

测试程序 BusClient 和 BusServer 分别是客户方和服务方程序，其通讯机制与 InforGuard 通讯机制一致。BusClient 的启动命令格式： BusClient <目标 IP> <目标端口>；BusServer 的启动命令格式：BusServer <本地物理 IP> <监听端口>。

以上述情形为例，把测试程序放置在各主机上，分别验证 3 端应用、6 个链路的通信情况：

1.MC->MA：BusServer 模拟 MA，绑定物理地址 10.0.0.2:10002；BusClient 模拟 MC，访问 MA 的映射地址 192.168.0.218:10002

2.SA->MA：BusServer 模拟 MA，绑定物理地址 10.0.0.2:10002；BusClient 模拟 SA，访问 MA 的映射地址 192.168.0.218:10002

3.MC->SA：MC 和 SA 处于防火墙的同一侧，没有跨防火墙问题，本测试可略过。

4.MA->SA：BusServer 模拟 SA，绑定物理地址 192.168.0.135:10003；BusClient 模拟 MA，访问 SA 的映射地址 10.0.0.22:10003

5.MA->MC：BusServer 模拟 MC，绑定物理地址 192.168.0.135:10004；BusClient 模拟 MA，访问 MC 的映射地址 10.0.0.22:10004

6.SA->MC：SA 和 MC 处于防火墙的同一侧，没有跨防火墙问题，本测试可略过。

注：BusServer 不会自动退出，因此每次测试结束后，应当用 ctrl+c 强制关闭，以免造成端口冲突，影响其它的测试和后续实际环境的部署。

3、部署

通过浏览器使用“网站配置向导”部署时，各步骤与没有防火墙时一致，只有“添加监控主机”和“添加同步主机”这两步有差别。

a、添加监控主机

添加监控主机时的具体配置如图 2-2：

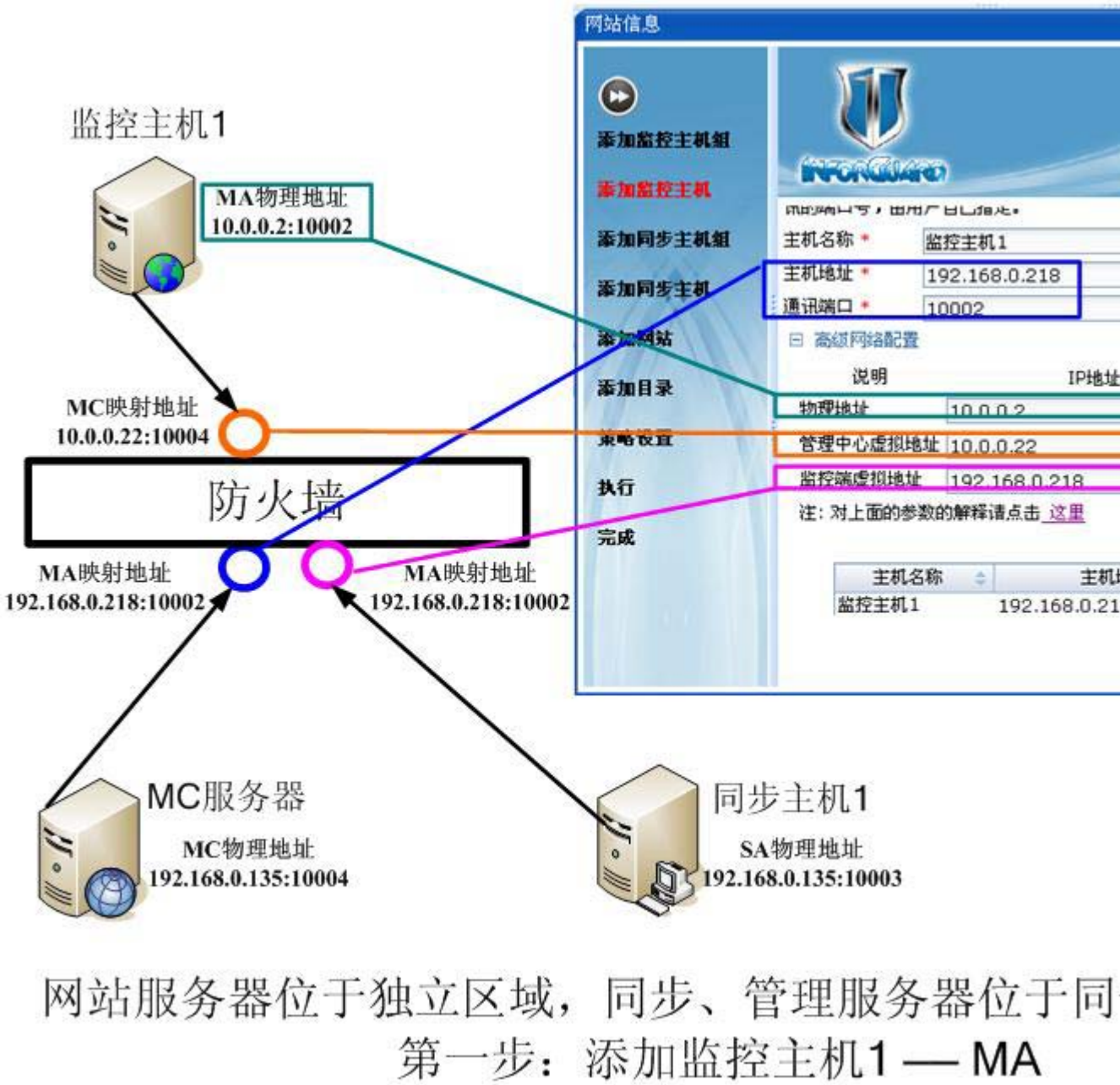


图 2-2

如上图，以上情形中配置“主机地址”和“通讯端口”是从 MC 所在主机看到的 MA 映射地址；“物理地址”是 MA 的物理地址；“管理中心虚拟地址”是从 MA 所在主机看到的 MC 映射地址；“监控端虚拟地址”是从 SA 所在主机看到的 MA 映射地址。

b、添加同步主机

添加同步主机时的具体配置如图 2-3：

图 2-3

如上图，以上情形中配置“主机地址”和“通讯端口”就是 SA 的物理地址（因为 MC 和 SA 不穿越防火墙）；“物理地址”是 SA 的物理地址；“管理中心虚拟地址”就是 MC 物理地址（因为 MC 和 SA 不穿越防火墙）；“同步端虚拟地址”是从 MA 所在主机看到的 SA 映射地址。

其他情形的防火墙配置，可参考此情形进行。

2.4. 系统参数配置

2.4.1. 系统内存大小的配置

系统默认的内存大小为 20M，如果网站文件数量很多，则生成水印时需要的内存大小可能会超过默认内存的大小，这时需要设置系统内存的大小值。

第一步：计算网站需要的内存大小

计算规则如下：

按 1 万个文件需要的内存为 1M，1 万个目录需要的内存为 1M，通过统计网站的文件数量和目录数量大致计算出系统需要的内存。如果需要的内存值 大于系统默认的内存值，则重新设置内存的大小。

第二步：修改内存值

源文件：InforGuard MA 安装目录/cfg/maoption.xml

```
<db dbtreesize="20480" dbtreesavecount="1024" dbtreesaveseconds="150" />
```

将配置文件中以上位置的 dbtreesize 的值设置为系统需要的内存大小值。重启 InforGuard MA

2.4.2. MA 水印控制的配置

在 Windows 上，如果需要使用过滤器机制，可以将 ma 的水印生成模块启用。

修改配置文件：

源文件：InforGuard MA 安装目录/cfg/maoption.xml

```
<db available="0"  />
```

将配置文件中以上位置的 available 的值设置 1，重启 InforGuard MA

第 3 章 产品使用说明

3.1. 产品介绍

3.1.1. 产品专用名词介绍

本节主要介绍一下产品中使用到的专用名词。

1、监控代理（Monitor Agent 简称 MA）

监控代理是一个独立进程。该进程运行在被保护的网站服务器上。监控端实时监视网站被保护文件（或被访问文件）的修改状态，当发现文件被篡改时，实时通知“备份服务”程序，对发生篡改的文件进行恢复。

2、同步代理（Synchronization Agent 简称 SA）

同步代理是一个独立进程。该进程运行在网站发布服务器上。SA 建立与监控端（简称 MA）的实时通讯，一方面，SA 为 MA 提供标准水印，供 MA 进行水印验证；另一方面，当 MA 发现被篡改的文件时，就会通过 SA 的文件传输服务，发起对篡改文件的恢复处理。

3、管理中心（Manager Center 简称 MC）

管理中心管理该中心下所有的网站和主机，记录该中心下所有主机和网站的各类日志，在有报警信息时，记录报警信息并将报警信息发送给指定的用户。

4、监控主机组

监控主机组就是对网站进行监控的一组主机，如果一个网站部署在多台监控主机上，那么这几台监控主机就组成了这个网站的监控主机组。如果一个网站只部署在一台监控主机上，那么这一台监控主机就组成这个网站的监控主机组。

5、备份主机组

备份主机组是对网站进行备份的一组主机，如果一个网站备份到多台备份主机上，那么这几台备份主机就组成了这个网站的备份主机组。如果一个网站只需要备份在一台备份主机上，那么这一台备份主机就组成这个网站的备份主机组。

6、监控主机

用于监控网站的一台主机，即一个监控代理（MA）。

7、同步主机

用于备份网站和同步网站的一台主机，即一个同步代理（SA）。

8、网站

用户对外发布的网站，即监控的内容。

9、逻辑目录

一个主机组中多台主机上内容相同的目录命名为一个逻辑目录。

10、物理目录

网站目录在磁盘上的路径。

3.1.2. 产品功能特点介绍

功能概述

支持多虚拟主机——自动实时监控多个网站或文件系统

支持多虚拟目录——自动实时监控多个文件目录

实时恢复——真正做到实时恢复被篡改的文件

实时报警——支持多种形式的报警模式

支持多终端——允许多终端远程协同对网站进行维护

安全通道——文件传输过程采用高强度加密传输

抗攻击功能——监控代理 MA 以安全服务的方式运行

自动更新——系统可以将 CMS 生成的网页文件自动、实时同步更新到网站服务器

支持复杂网站应用——基于独特的监控技术，支持各种复杂应用

支持动态网页——允许对动态网页文件进行监控保护

权限管理——支持完备的用户权限分配及管理

策略管理——支持用户自定义监控策略

查询审计——支持对监控信息的查询与审计功能

产品特点

四重防护

InforGuard 网页防篡改系统采用独有的四重防护技术，做到网站防御的滴水不漏，确保网站的安全性。四重防护依次是实时阻断（也称之为增强型事件触发）、事件触发、Web 服务器核心内嵌（简称核心内嵌）和防 SQL 注入。

一重防护——实时阻断

实时阻断是一种主动式的“防”篡改手段，其核心是文件驱动技术。操作系统在加载了我们专用的文件驱动后，可以实现进程级磁盘操作检测，能够判断企图进行磁盘操作的进程合法性，从而预先阻断非法进程对网站内容的篡改。

二重防护——事件触发

事件触发是 InforGuard 独有的文件系统监控技术，特点是主动、实时、低耗。它是以操作系统内核消息作为信息源，经过触发式文件变更检测引擎的分析形成事件，由于所有监控中心发布的文件操作指令都会在系统中进行授权注册，因此可以认定未经授权注册的操作为非法事件，从而进行恢复并报警。

三重防护——核心内嵌

核心内嵌是将篡改检测模块嵌入 Web 服务器或应用服务器软件内部，与服务器软件实现无缝结合，对服务器收到的所有 URL 请求所涉及的网页文件进行合法性验证（数字水印对比），从而能够在服务器对外发送网页之前，确保每个网页文件的真实性、合法性。

四重防护——防 SQL 注入

屏蔽网站恶意扫描，有效地抵御针对网站数据库资源的注入式攻击。对网络请求进行验证，自动阻止 SQL 注入攻击，发生 SQL 注入企图自动实时报警，支持 SQL

注入规则库自定义，支持用户查看过滤的请求与请求来源等信息，支持规则库定期升级更新，规则库采用正则表达式描述，规则扩展性高。

自动同步

高效的同步服务

InforGuard 网页防篡改系统具备高效的文件同步机制，能够将网站文件自动地同步到网站服务器上，且支持海量数据/文件同步（每天可以承载数十万文件量的发布）。同时，为了兼顾网站发布的效率，该系统还支持增量式同步和精确同步两种高级模式。

完善的容错机制

InforGuard 网页防篡改系统支持同步过程中的网络连接重试、失败重传、断点续传等完善的容错机制，从而能够确保各类网站的 7*24 小时连续正常运行，完全实现网站文件发布的无人值守和自动恢复。

支持复杂网站系统

InforGuard 网页防篡改系统支持集群、热备等复杂应用的自动同步，用户仅需要将网页文件发布到同步端，InforGuard 会根据网站部署的情况进行同步任务的分发，自动完成向集群或热备系统中多台服务器的文件同步，从而达到在保护网站的同时又降低用户工作量的效果。

无缝集成 CMS

InforGuard 网页防篡改系统支持内容管理系统 CMS 的无缝集成，InforGuard 的自动同步服务能够以旁路的方式知悉所有 CMS 发布的文件并自动实时进行网站服务器的同步，达到了既不影响原有发布系统，又能够准确高效地实现网站文件同步的目标。

3.2. 部署向导

点击导航条上的“网站配置向导”，进入网站部署界面。

1、添加监控主机组

选择“新建监控主机组”，输入主机组名称，输入的名称请遵守界面的提示；选择“使用已存在的监控主机组”， 选择一个已经存在的监控主机组，设置完成，点击“下一步”，进入添加监控主机的界面。

2、添加监控主机

输入要添加的主机名称，主机的 IP 地址和通讯端口，输入的内容请遵守界面的提示，设置完成后，点击“确定”添加该主机，若添加 成功，在信息框中会显示新添加的主机信息，按以上操作，可以添加多台主机。选中一个新添加的主机，点击信息框中的删除标志，则删除改主机。

设置完成，点击“下一步”，进入添加同步主机组界面。

3、添加同步主机组

添加同步主机组的操作同添加监控主机组的操作。

4、添加同步主机

添加同步主机的操作同添加监控主机。

5、添加网站

输入要添加的网站名称，输入的内容请遵守界面的提示，设置完成点击“下一步”，进入添加目录的界面。

6、添加目录

输入要添加的目录名称，然后在各个监控主机上选择相应的监控目录，在各个同步主机上选择相应的备份目录。点击“添加”添加 该目录，添加成功后在信息框中可以看到新添加的目录信息，按以上操作可添加多个目录。

选择某个添加的目录，点击删除标志，删除该目录。设置完成后点击“下一步”，进入策略设置界面。

7、策略设置

选择要设置的策略，进入该策略的设置界面，具体的设置操作请参考后面相应的章节。

8、执行

点击“执行”，保存设置的内容，点击取消不保存退出。

9、完成

配置完成后，进入完成界面，请在配置完成后先执行界面提示的操作，具体的操作请参考后面相应的章节。

3.3. 主机管理

3.3.1. 主机组管理

3.3.1.1. 添加主机组

在系统初次运行时，必须先添加主机组，只有添加了主机组，才能往组内添加主机和网站。 在新添加一个主机或网站时，若该主机或网站不属于现有的任何主机组，需要先添加这个主机组。

1. 添加监控主机组

点击导航条上的“主机管理”，进入主机管理界面，如图 3-1：

图 3-1

左侧为导航树，有两个并列的根节点，分别为监控主机组管理和同步主机组管理。默认为监控主机组管理。 选择“添加自定义的监控主机组”，弹出一个添加主机组的窗口，如图 3-2：

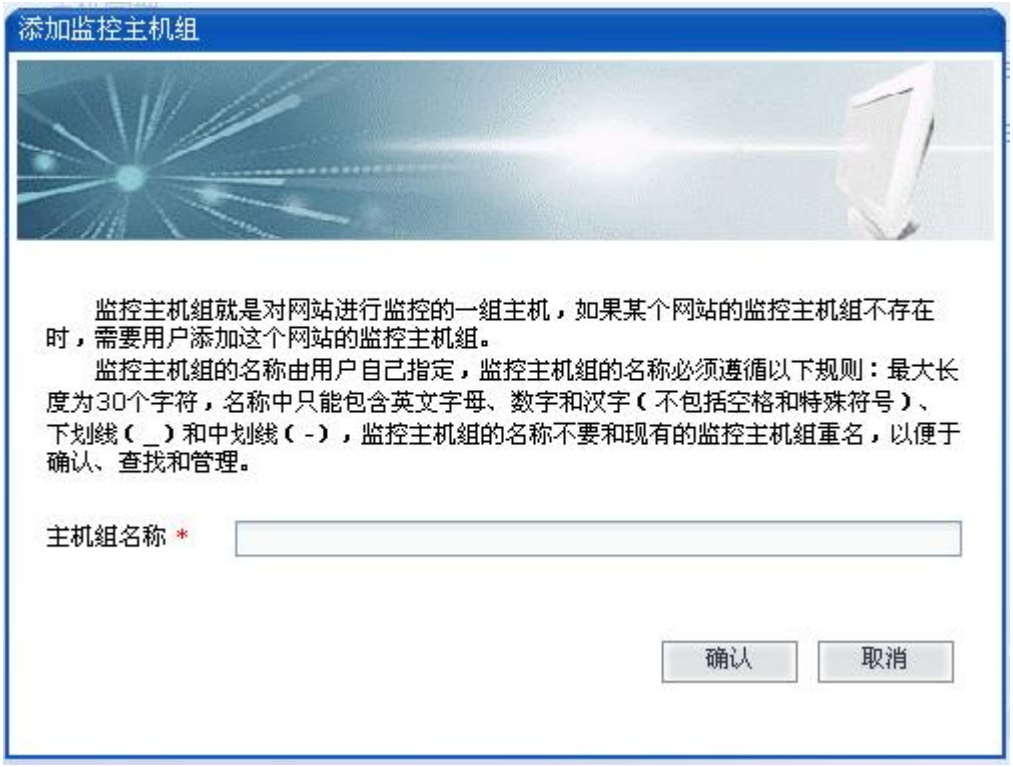


图 3-2

在窗口内填写主机组名称，点击“确认”添加主机组，点击“取消”，则取消添加主机组操作，如果添加成功，左侧导航树监控主机组管理节点下会出现新添加的主机组子节点。

2. 添加同步主机组

在左侧导航树上点击同步主机组管理，可添加同步主机组，操作同添加监控主机组。

3.3.1.2. 修改主机组属性

若需要修改某个主机组的名称，可以通过修改主机组的属性来完成。

1. 修改监控主机组属性

点击导航条上的“主机管理”，进入主机管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，选择要修改属性的主机组，进入如下界面，如图 3-3：

图 3-3

在“主机组属性”面板内，输入新的主机组名称，点击“保存”，保存新设置的内容，点击“重置”还原修改。

在“帮助”面板内显示了在修改主机组属性时需要注意的一些提示信息。

2. 修改同步主机组属性

修改同步主机组属性，操作同修改监控主机组属性。

3.3.1.3. 删除主机组

一个主机组中没有任何主机，或者一个主机组不再需要时，删除该主机组，在删除主机组前，若该主机组上有网站，需要先删除该主机组上的网站。 主机组被删除后，组内的所有主机也被删除。

1. 删除监控主机组

点击导航条上的“主机管理”，进入主机管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，选择要删除的主机组，进入如下界面，如图 3-4：

图 3-4

在“生命周期管理”面板内，选择删除主机组，弹出询问窗口，点击“确认”删除该主机组，点击“取消”，取消删除，若主机组被 网站引用时，给出提示，删除操作不成功。如果想成功删除该主机组，请进入网站管理界面，先删除引用该主机组的网站。当主机组未被网站引用时， 删除成功，左侧导航树中该主机组被删除。

2. 删除同步主机组

点击同步主机组管理前的按钮，可删除相应的同步主机组，操作同删除监控主机组。

3.3.2. 主机管理

3.3.2.1. 添加主机

添加主机时，要确保该主机所在的主机组已经建立，如果主机组没有建立，先添加该主机组。

1. 添加监控主机

点击导航条上的“主机管理”，进入主机管理界面。

点击“监控主机组管理”前的按钮，列出所有的监控主机组，选择要添加该主机的主机组，进入如下界面，如图 3-5：

图 3-5

在“生命周期管理”面板内，选择“向主机组内添加主机”， 弹出如下窗口，如图 3-6：

图 3-6

在窗口内填写主机名称、主机 IP 地址、通讯端口，点击“确认”添加主机，点击“取消”，取消添加主机组操作。 添加成功后，左侧导航树相应的监控主机组节点下会出现新添加的主机子节点。

2. 添加同步主机

添加一个同步主机，操作同添加监控主机。

3.3.2.2. 修改主机属性

修改主机属性即修改主机的名称，IP 地址和通讯端口。

1. 修改监控主机属性

点击导航条上的“主机管理”，进入主机管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组， 选择要修改属性的主机所在的主机组，列出所有的主机，选择要修改的主机，进入如下界面，如图 3-7：

图 3-7

在“主机属性”面板内，该主机没有被禁用时只能修改主机的名称。若想修改主机的 IP 地址和通讯端口， 需要先禁用该主机。修改完毕后请点击保存按钮保存设置。修改完成后，导航树中出现新修改的主机名。

在“帮助”面板内显示了在修改主机属性时需要注意的一些 提示信息。

2. 修改同步主机属性

修改一个同步主机属性，操作同修改监控主机属性。

3.3.2.3. 启用主机

一个主机被禁用后需要将该主机启用时，使用启用主机的功能。主机被启用后，恢复与其它主机的通讯，正常运行。

1. 启用监控主机

点击导航条上的“主机管理”，进入主机管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组， 选择要启用监控的主机所在的主机组，列出所有的主机，选择要启用的主机，进入如下界面，如图 3-8：

图 3-8

在“生命周期管理”面板内，选择“启用主机”，弹出询问窗口，点击“确认”启用该主机，点击“取消”，取消启用该主机。 启用成功后，则“删除主机”变成不可用状态。

2. 启用同步主机

启用一个同步主机，操作同启用监控主机。

3.3.2.4. 禁用主机

一个主机不需要对网站进行监控，或该主机被删除前，禁用该主机。主机被禁用后，其它主机不再和它进行通讯， 该主机也停止工作。

1. 禁用监控主机

点击导航条上的“主机管理”，进入主机管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组， 选择要禁用的主机所在的主机组，列出所有的主机，选择要禁用的主机，进入如下界面，如图 3-9：

图 3-9

在“生命周期管理”面板内，选择“禁用主机”，弹出询问窗口，点击“确认”禁用该主机，点击“取消”，取消禁用该主机。 禁用成功后，“删除主机”变成可用状态。

2. 禁用同步主机

禁用一个同步主机，操作同禁用监控主机。

3.3.2.5. 删除主机

一个主机不再属于某个组时，删除该主机，删除某个主机前，需要先禁用该主机。 删除组内的一个主机，不会影响组内其它的主机。

1. 删除监控主机

点击导航条上的“主机管理”，进入主机管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，选择要删除的主机所在的主机组， 列出所有的主机，选择要删除的主机，进入如下界面，如图 3-10：

图 3-10

在“生命周期管理”面板内，若“删除主机”不可用，请先选择“禁用主机”，主机被禁用后，再选择“删除主机”， 弹出询问窗口， 点击“确认”删除该主机，点击“取消”，取消删除该主机。删除成功后，左侧导航树中该主机被删除。

2. 删除同步主机

删除一个同步主机，操作同删除监控主机。

3.3.2.6. 查看主机状态

需要了解主机当前的运行状态时，查看主机的状态。主机组显示组内所有主机的运行状态，主机显示选择主机的运行状态。

1. 查看监控主机组的状态

点击导航条上的“主机管理”，进入主机管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组， 选择要查看的主机组，进入如下界面，如图 3-11：

图 3-11

在“状态信息”面板内显示组内所有主机的状态。

2. 查看同步主机组的状态

查看同步主机组的状态，操作同查看监控主机组的状态。

3. 查看监控主机状态

点击导航条上的主机管理，进入主机管理界面，点击“监控主机组管理”前的按钮，列出所有的监控 主机组，选择要查看的主机所在的主机组前的按钮，列出所有的主机，选择要查看的主机，进入如下界面，如图 3-12：

图 3-12

在“状态信息”面板内显示该主机当前的状态。

4 . 查看同步主机状态

查看同步主机状态，操作同查看监控主机状态。

3.4. 网站管理

3.4.1. 添加网站

添加网站前，必须确定要添加该网站的监控主机组和同步主机组已经建立，如果没有建立，请在主机管理中添加。

点击导航条上的“网站管理”，进入网站管理界面，点击”监控主机组管理“前的按钮，列出所有的监控主机组，点击要添加网站的主机组，进入如下界面，如图 3-13：

图 3-13

在“生命周期管理”面板内选择“向主机组内添加网站”，进入添加网站的界面，如图 3-14：

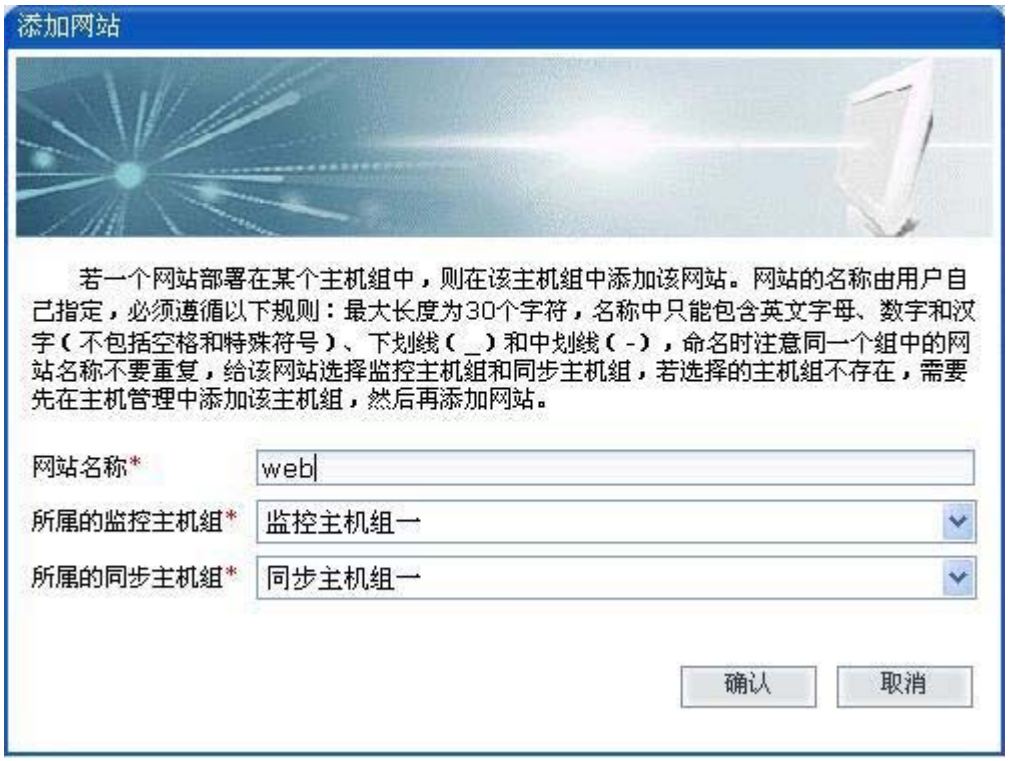


图 3-14

在界面内输入网站的名称，在下拉框中选择所属的监控主机组和同步主机组。输入网站名称时请遵守界面的提示。

点击“确定”添加网站，添加成功后，在左侧的导航树上出现新添加的网站，点击“取消”，取消添加网站。

3.4.2. 为网站添加目录

在添加目录前，添加目录的网站所在的主机组，组内所有的监控主机上已经部署了该网站，同步主机都建立了用于备份该网站的目录。 为网站添加了目录后，才能进行网站的备份和初始化。

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组， 点击要添加目录的网站所在的主机组，列出该组所有的网站，点击要添加目录的网站，进入如下界面，如图 3-15：

图 3-15

选择“生命周期管理”面板内的“添加目录”，弹出添加目录窗口，如图 3-16：

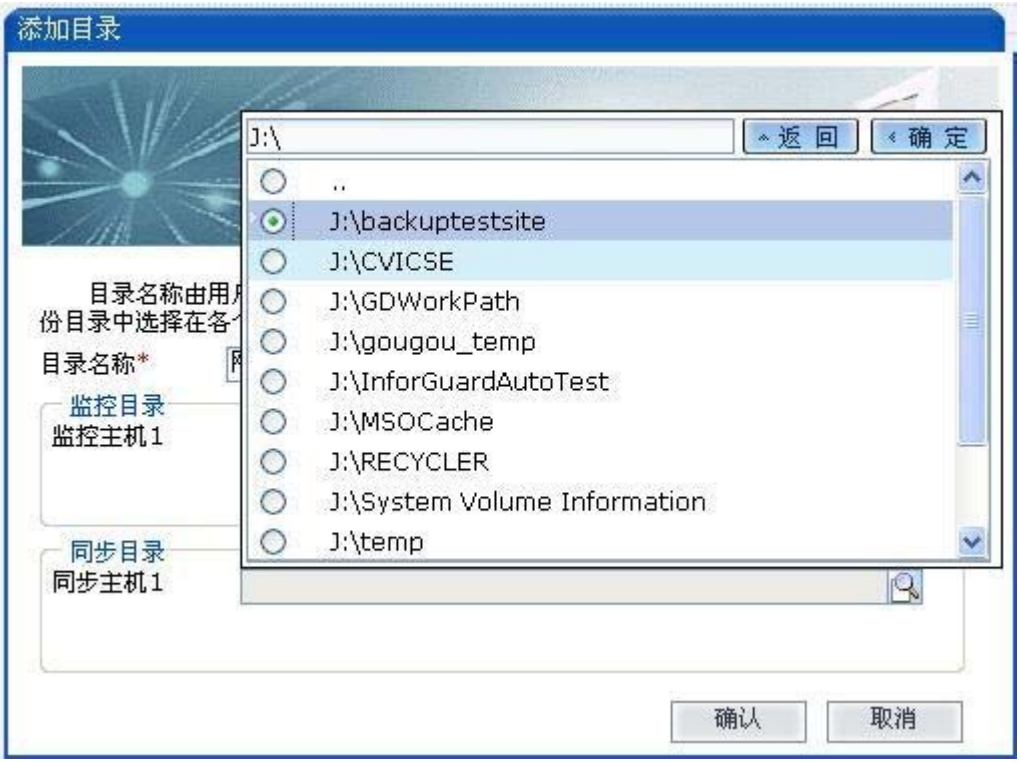


图 3-16

输入目录名称，点击目录选择图标，选择相应的监控目录和备份目录。“监控目录”列表列举了监控主机组下每一台主机的监控目录。 “备份目录”列表列举了同步主机组下每一台主机的备份目录。点击监控目录文本框（或者后面的按钮），出现目录选取窗口。“目录选取窗口”包含 “当前目录”文本框、“后退”按钮、“确认”按钮、“目录列表”。目录列表默认显示磁盘根目录。鼠标单击目录将进入它的子目录，文本框上显示选取的目录， 列表框上显示该目录的子目录。点击“后退”按钮返回该目录。选择目录前面的单选框，单击“确认”按钮完成选取监控目录的操作。选择备份目录和选择监控目录一样的操作。

点击“确定”，添加目录，点击“取消”，取消添加目录。添加成功后，在导航树中会看到新添加的目录。

3.4.3. 修改网站属性

点击导航条上的“网站管理”，进入网站管理界面。点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要修改属性的网站所在的主机组， 列出该组中所有的网站，点击要修改的网站，进入如下界面，如图 3-17：

图 3-17

在“网站属性信息”面板内，可以修改网站的名称，输入新的网站名称， 点击“保存”，保存新设置的属性，点击“重置”还原修改。保存成功后，导航树中出现新设置的网站名称。

在“帮助”面板内显示了在修改网站属性时需要注意的一些提示信息。

在同步主机组中选择网站，也可修改网站的属性。

3.4.4. 网站内容管理

3.4.4.1. 生成水印

生成水印是指不进行网站的备份或同步，而直接生成文件的水印，在进行网站初始化之前，必须设置好了监控目录和备份目录。 若网站内容比较多，建议先生成水印，然后将监控的内容直接拷贝到各个同步主机对应的备份目录下，若直接进行网站备份操作， 会花费较长的时间。若内容不是很多，可直接进行网站备份。

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要生成水印的网站所在的主机组， 列出该组中所有的网站，点击要生成水印的网站，进入如下界面，如图 3-18：

图 3-18

在“内容管理”面板内选择“生成水印”，弹出提示窗口，点击“是”生成水印，点击“否”取消操作。

3.4.4.2. 备份网站

在进行网站备份之前，必须设置好了监控目录和备份目录。网站备份前需要停止监控，备份完成后开启监控。

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要备份的网站所在的主机组， 列出该组中所有的网站，点击要备份的网站，进入如下界面，如图 3-19：

图 3-19

在“内容管理”面板内选择“备份网站”，弹出如下窗口，如图 3-20：

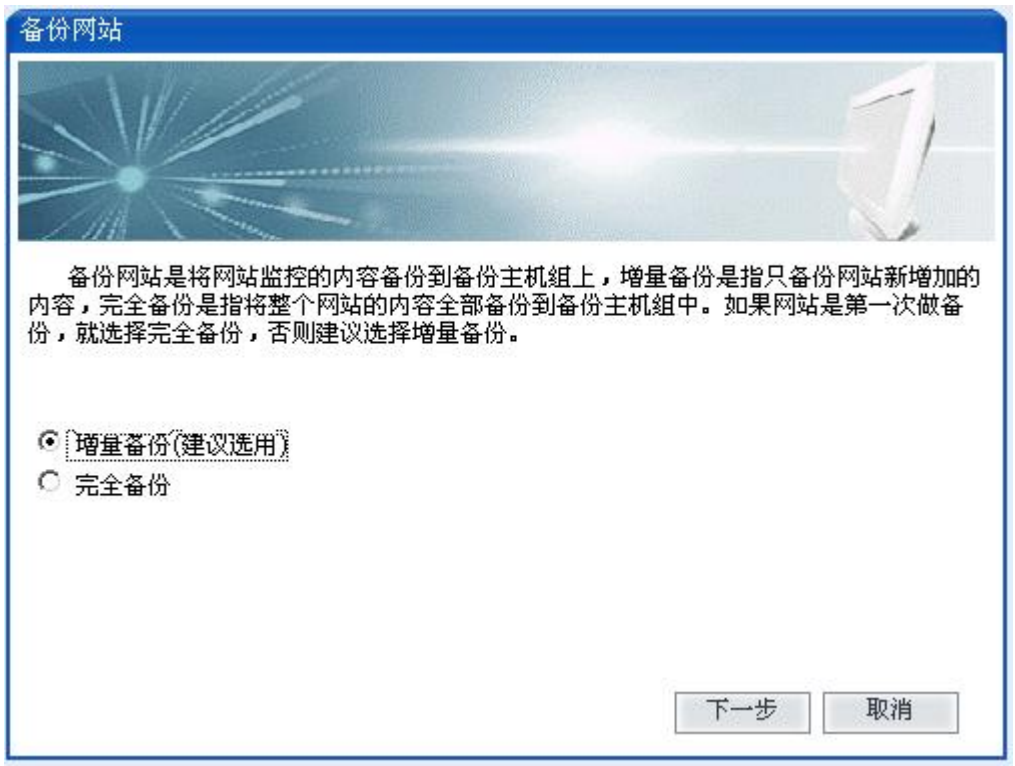


图 3-20

若备份的网站是第一次进行备份，则选择完全备份，否则建议选择增量备份，然后点击“下一步”按钮，进行备份，弹出如下窗口，点击“取消”按钮，取消备份，如图 3-21：

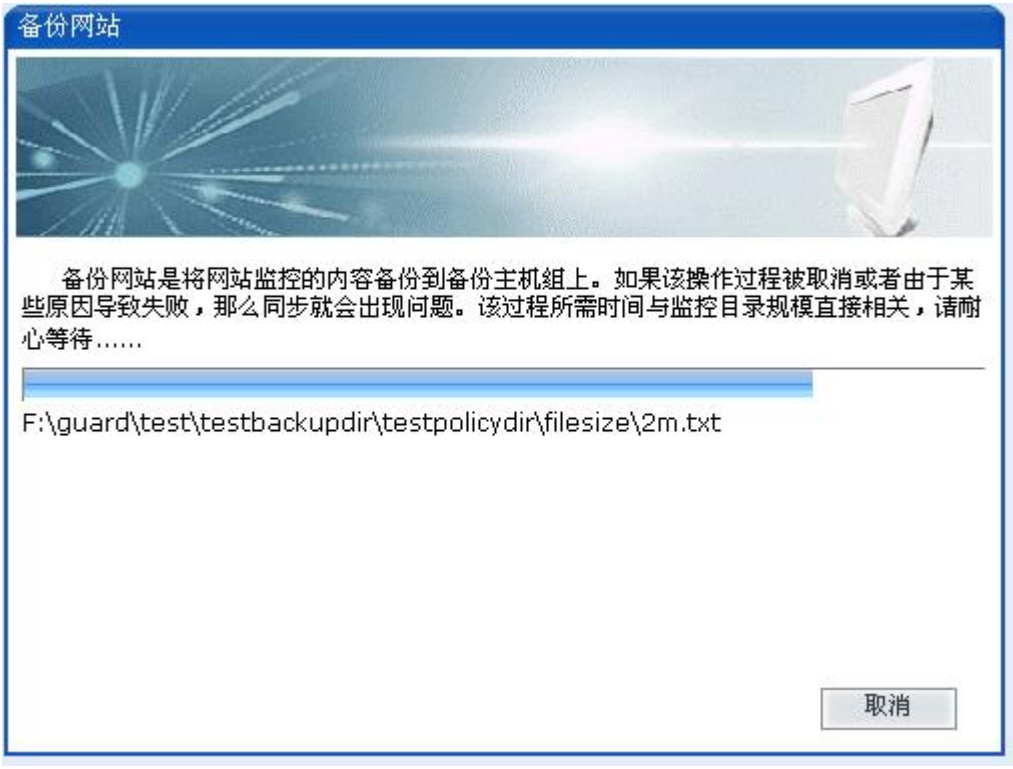


图 3-21

网站备份时界面显示网站备份的进度，此时点击“取消”会中断备份操作返回，备份完成后弹出如下窗口，如图 3-22：

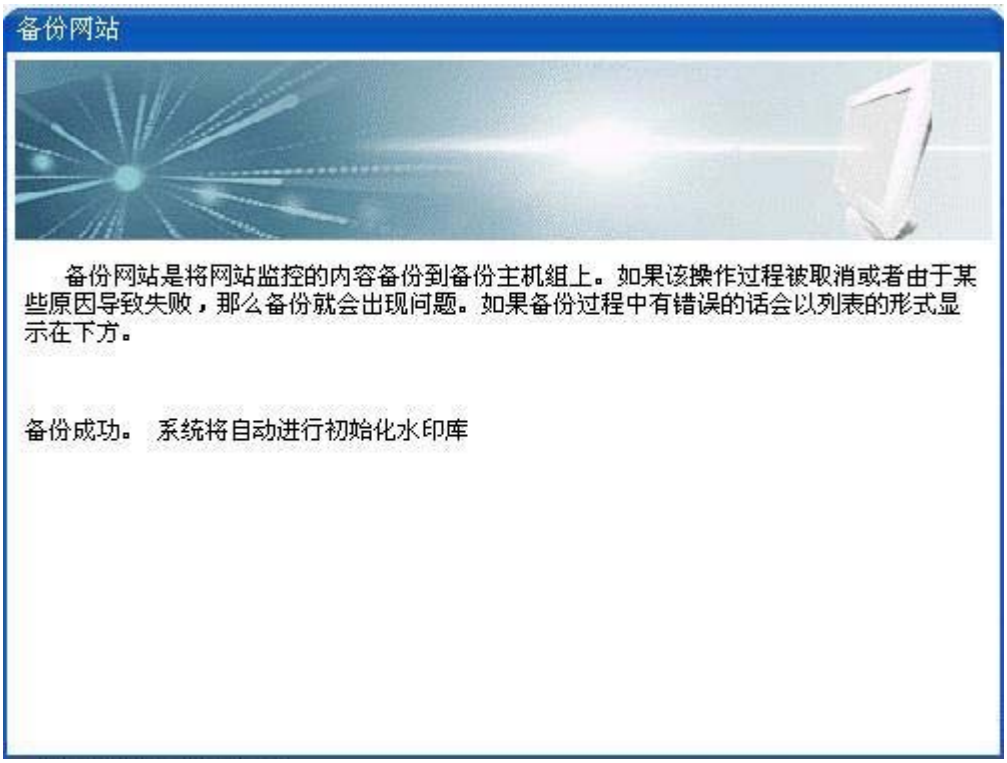


图 3-22

点击“完成”按钮完成备份操作。在同步主机组中选择网站，也可进行网站的备份。

3.4.4.3. 同步网站

同步网站是人工对网站进行同步，将同步端文件的变化同步到监控端，在进行网站同步之前，必须设置好了监控目录和备份目录。

点击导航条上的“网站管理”，进入网站管理界面，点击“同步主机组管理”前的按钮，列出所有的同步主机组，点击要同步的网站所在的主机组， 列出该组中所有的网站，点击要同步的网站，进入如下界面，如图 3-23：

图 3-23

在“内容管理”面板内选择“同步网站”，弹出窗口界面的具体操作同 2.4.4.2 备份网站.

3.4.5. 网站状态管理

3.4.5.1. 启用网站

一个网站被禁用之后启动该网站，使用启用网站的功能。在启用网站前，必须先停止该网站的监控。网站被启用后，重新被监控起来。

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要启动的网站所在的主机组， 列出该组中所有的网站，点击要启用的网站，进入如下界面，如图 3-24：

图 3-24

在“生命周期管理”面板内选择“启用网站”，弹出提示框，点击“确定”启用网站，点击“取消”，取消启用网站，启用成功后，“删除网站”和“启用网站”变成不可用状态，“禁用网站”变成可用状态。

在同步主机组中选择网站，也可进行启用网站的操作。

3.4.5.2. 禁用网站

一个网站暂时不需要被监控，或者一个网站被删除前，禁用该网站，在禁用一个网站前，必须先停止该网站的监控。

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要禁用的网站所在的主机组， 列出该组中所有的网站，点击要禁用的网站，进入如下界面，如图 3-25：

图 3-25

在“生命周期管理”面板内选择“禁用网站”，弹出如下框，点击“确定”禁用网站，点击“取消”，取消禁用网站，禁用成功后，“删除网站”和“启用网站”变成可用状态。

在同步主机组中选择网站，也可进行禁用网站的操作。

3.4.5.3. 删除网站

若一个网站不需要被监控，或该网站所在的主机组将被删除，删除该网站，删除某个网站前，需要先停止该网站的监控，然后禁用该网站。

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要删除的网站所在的主机组， 列出该组中所有的网站，点击要删除的网站，进入如下界面，如图 3-26：

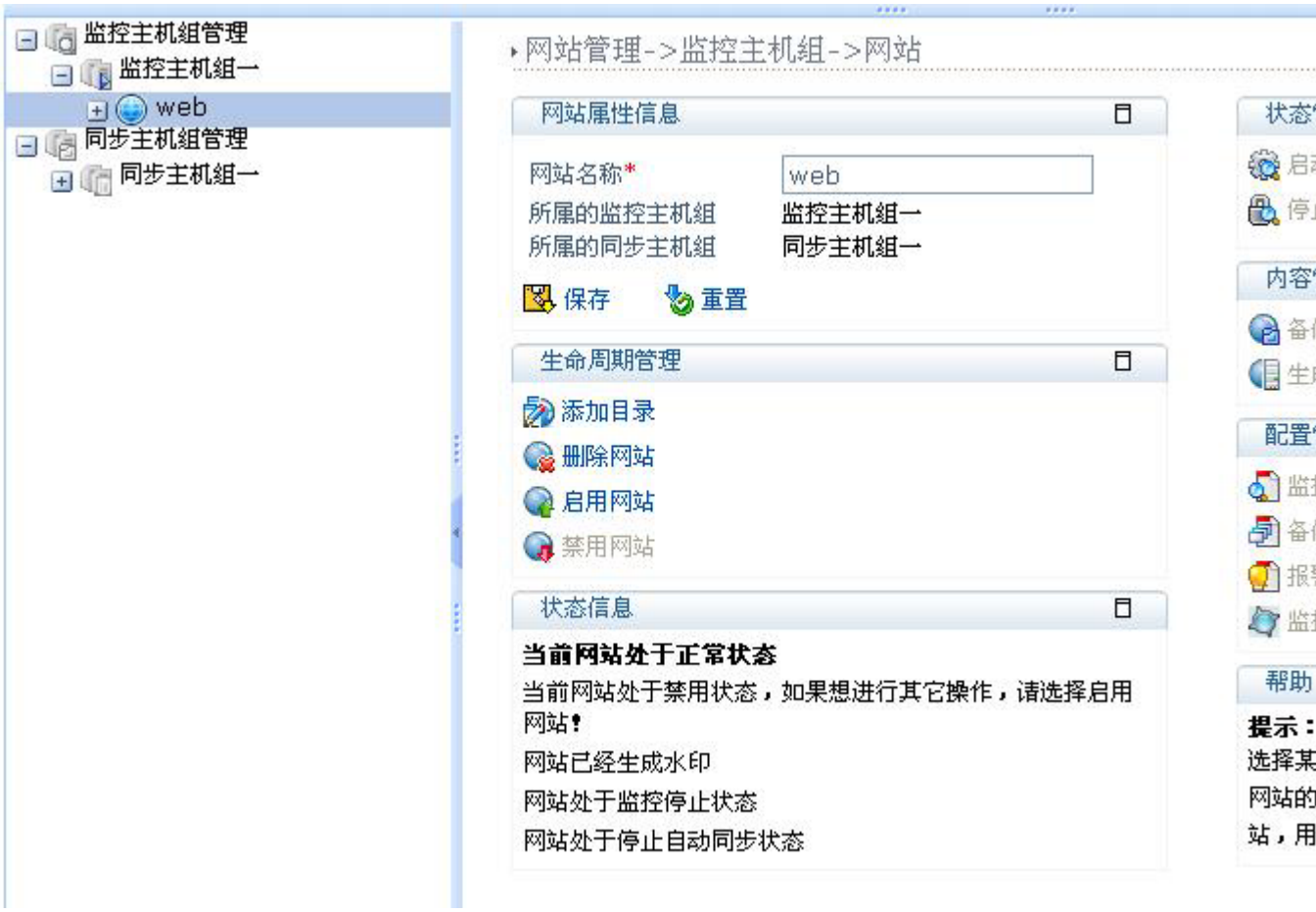


图 3-26

在“生命周期管理”面板内，如果“删除网站”不可用，请先禁用该网站，再选择“删除网站”，弹出提示框，点击“确定”删除网站，点击“取消”，取消删除网站，禁用成功后， 导航树中没有该网站。

在同步主机组中选择网站，也可进行网站的删除操作。

3.4.5.4. 启动监控

一个新添加的网站，只有在生成了网站水印或网站备份之后，才能启动对网站的监控，启动监控后，系统才能检测到篡改事件并自动恢复。

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要启动监控的网站所在的主机组， 列出该组中所有的网站，点击要启动监控的网站，进入如下界面，如图 3-27：

图 3-27

在“状态管理”面板内，若“启动监控”和“停止监控”都不可用，请先生成该网站的水印或备份该网站，然后再选择“启动监控”， 弹出提示框，点击“确定”启动监控，点击“取消”，取消启动监控，启动成功后，“停止监控”变成可用状态。“删除网站”、“启用网站”、“禁用网站”变成不可用状态。

3.4.5.5. 停止监控

一个网站停止监控后，系统将不再监控该网站，网站停止监控后，可以在监控端添加目录，备份后再启动监控， 只有停止了网站的监控，才能进行网站的其它操作。

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要停止监控的网站所在的主机组， 列出该组中所有的网站，点击要停止监控的网站，进入如下界面，如图 3-28：

图 3-28

在“状态管理”面板内，点击“停止监控”，弹出提示框，点击“确定”停止监控，点击“取消”，取消停止监控，停止成功后，“启动监控”变成可用状态，“停止监控”变成不可用状态。“删除网站”、“启用网站”、“禁用网站”中某一个变成可用状态。

3.4.5.6. 启动自动同步

一个新添加的网站，只有在生成了网站的水印或网站同步之后，才能启动网站的自动同步功能，启动网站的自动同步后， 若同步端有文件的变化，会自动同步到监控端。

点击导航条上的“网站管理”，进入网站管理界面，点击“同步主机组管理”前的按钮，列出所有的同步主机组，点击要启动自动同步的网站所在的主机组， 列出该组中所有的网站，点击要启动自动同步的网站，进入如下界面，如图 3-29：

图 3-29

在“状态管理”面板内，若“启动自动同步”和“停止自动同步”都不可用，请先生成该网站的水印或同步该网站，然后再 选择“启动自动同步”，弹出如下提示框，如图：

点击“确定”启动自动同步，点击“取消”，取消启动自动同步，启动成功后，“停止自动同步”变成可用状态。

3.4.5.7. 停止自动同步

停止自动同步后，同步端的文件变化不会自动同步到监控端。

点击导航条上的“网站管理”，进入网站管理界面，点击“同步主机组管理”前的按钮，列出所有的同步主机组，点击要停止自动同步的网站所在的主机组， 列出该组中所有的网站，点击要停止自动同步的网站，进入如下界面，如图 3-30：

图 3-30

在“状态管理”面板内，点击“停止自动同步”，弹出提示框，点击“确定”停止自动同步，点击“取消”，取消停止自动同步，停止成功后，“启动自动同步”变成可用状态，“停止自动同步”变成不可用状态。

3.4.5.8. 查看网站状态

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要查看的网站所在的主机组，列出该组中所有的网站，点击要查看的网站，进入如下界面，如图 3-31：

图 3-31

在“状态信息”面板内，显示该网站当前的状态。在同步主机组中选择网站，也可查看网站的状态。

3.4.6. 设置网站策略

3.4.6.1. 设置监控策略

若网站中的某些内容不需要进行监控时，通过策略设置，来排除这些不用监控的内容。这些排除的内容，在监控的过程中， 若有文件操作事件发生，系统不会视为篡改事件进行报警，也不会自动恢复。网站只有在启用的状态下，才可以设置策略。

点击导航条上的“网站管理”，进入网站管理界面点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要设置策略的网站所在的主机组， 列出该组中所有的网站，点击要设置策略的网站，进入如下界面，如图 3-32：

图 3-32

在“配置管理”面板内选择“监控策略”，弹出监控策略设置窗口，如图 3-33：

图 3-33

选择“启动以下策略”，各个设置的选择框变成可用状态。

1、排除目录列表

选择“排除目录列表后”，会出现一个“添加目录”的按钮，点击该按钮，会出现一个用于目录选择的目录框，

选择不需要进行监控的目录，点击右边的按钮确定选定的目录。在“排除目录列表”框里会出现选择的目录，若是第一次 添加排除监控的目录，则在“添加目录”按钮旁边会出现一个“删除”的按钮。若要删除一个目录，在“排除目录列表”框里选择该目录， 点击“删除”按钮，删除该目录，若所有的排除目录都被删除了，则“删除”按钮被隐藏。

2、排除文件列表

选择“排除文件列表后”，会出现一个“添加文件”的按钮，点击该按钮，会出现一个用于文件选择的目录框，

选择不需要进行监控的文件，点击右边的按钮确定选定的文件。在“排除文件列表”框里会出现选择的文件，若是第一次添加排除监控的文件， 则在“添加文件”按钮旁边会出现一个“删除”的按钮。若要删除一个文件，在“排除文件列表”框里选择该文件， 点击“删除”按钮，删除该文件，若所有的排除文件都被删除了，则“删除”按钮被隐藏。

3、排除类型列表

选择“排除类型列表”，在列表中输入要排除监控的文件类型，如 html，txt 等类型，同类信息之间以|分隔，排除类型支持模糊过滤， 即输入 tm,会排除扩展名中所有包括 tm 的文件。

4、模糊匹配模式

选择“模糊匹配模式”，在文本框中输入匹配的内容，假设用 a、b 表示一个字符串，输入的格式可为:a*，*a，a*b，*a*等，将分别排除文件名以 a 开头 文件名以 a 结尾，文件名以 a 开头 b 结尾，文件名中包含 a 的所有的文件。

5、排除事件类型

1）选择“文件修改事件”，则在监控的过程中，如监控端有文件被修改的事件发生时，系统不会视为篡改事件进行报警。

2）选择“文件删除事件”，则在监控的过程中，如监控端有文件被删除的事件发生时，系统不会视为篡改事件进行报警。

3）选择“文件新建事件”，则在监控的过程中，如监控端有新建文件的事件发生时，系统不会视为篡改事件进行报警。

4）选择“文件命名事件”，则在监控的过程中，如监控端有文件重命名的事件发生时，系统不会视为篡改事件进行报警。

设置完成后，点击“确定”，保存设置的内容，点击“取消”，取消保存设置的内容返回。

3.4.6.2. 设置备份策略

若网站中的某些内容在备份时不需要进行备份，通过策略设置，来排除这些不用备份的内容。这些排除的内容， 在进行网站备份时将不会进行备份。网站只有在启用的状态下，才可以设置策略。

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要设置策略的网站所在的主机组， 列出该组中所有的网站，点击要设置策略的网站，在“配置管理”面板内选择“备份策略”，弹出备份策略设置窗口，如图 3-34：

图 3-34

1、排除目录列表、排除文件列表、排除类型列表和模糊匹配模式策略的设置同 2.4.6.1 节监控策略设置。

2、包含文件属性

1）选择“文件长度上限”，在文本框中输入设置的文件长度的上限值，文件大小大于该值的文件将不进行备份。

2）选择“文件长度下限”，在文本框中输入设置的文件长度的下限值，文件大小小于该值的文件将不进行备份。

3）选择“指定起始日期时间”，设置起始时间，则文件最后修改时间早于该时间的文件将不进行备份。

4）选择“指定结束日期时间”,设置结束时间，则文件最后修改时间晚于该时间的文件将不进行备份。

设置完成后，点击“确定”，保存设置的内容，点击“取消”，取消保存设置的内容返回。

3.4.6.3. 设置同步策略

同步主要是同步端有对文件的操作时，监控端同时有相同的文件操作，若网站中的某些内容不需要进行同步时， 通过策略设置，来排除这些不用同步的内容。这些排除的内容，在自动同步的过程中将不会自动同步。网站只有在启用的状态下，才可以设置策略。

点击导航条上的“网站管理”，进入网站管理界面,点击“同步主机组管理”前的按钮，列出所有的同步主机组，点击要设置策略的网站所在的主机组， 列出该组中所有的网站，点击要设置策略的网站，进入如下界面，如图 3-35：

图 3-35

1、设置自动同步策略

在“配置管理”面板内选择“自动同步策略”，弹出自动同步策略设置窗口，策略设置的具体操作同 3.4.6.1 监控策略的设置。

2、设置手动同步策略

在“配置管理”面板内选择“手动同步策略”，弹出手动同步策略设置窗口，策略设置的具体操作同 3.4.6.2 同步策略的设置。

3.4.6.4. 设置报警策略

每个网站需要单独设置自己的报警策略，报警策略主要设置在有篡改事件发生时，以何种方式向用户发送报警信息。

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要设置策略的网站所在的主机组， 列出该组中所有的网站，点击要设置策略的网站，在“配置管理”面板内选择“报警策略”，弹出报警策略设置窗口，如图 3-36：

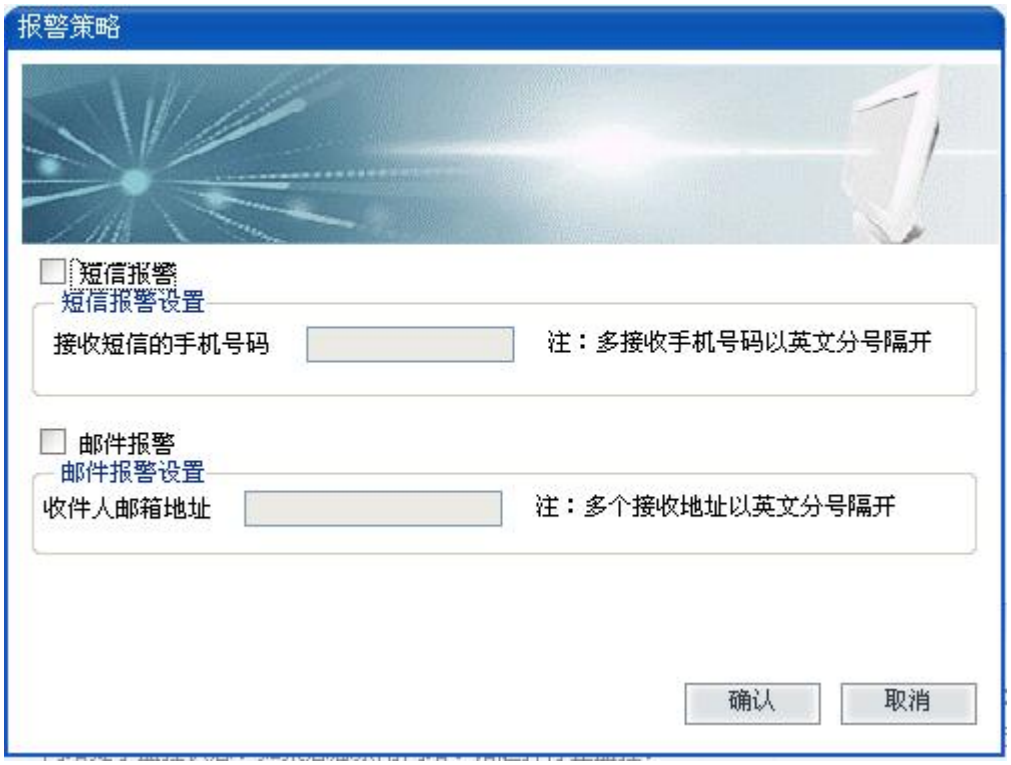


图 3-36

1、设置短信报警策略，在文本框中输入接收短信的手机号码，多个接收手机号码以英文分号隔开，然后选择使用短信进行报警的消息类型。

2、设置邮件报警策略，在文本框中输入收件人的邮箱地址，多个接收地址以英文分号隔开然后选择使用邮件进行报警的消息类型。

设置完成后，点击“确定”，保存设置的内容，点击“取消”，取消保存设置的内容返回。

当网站有报警信息时，系统按照设置的策略发送报警信息。

3.4.6.5. 设置监控过滤器

用户通过设置监控过滤器，选择在监控的过程中需要开启的监控器。

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要设置监控过滤器的网站所在的主机组， 列出该组中所有的网站，点击要设置策略的网站，在“配置管理”面板内选择“监控器类型”，弹出监控器管理窗口，如图 3-37：

图 3-37

界面会显示有一个默认选中的监控器，选择要开启的监控过滤器，每类监控器的参数设定属于高级选项，需在专业人员的指导下进行，不建议自行设置。这些参数的主要应用有：

1.可以设置性能优化的参数

2.可以设置参数，以满足部分特殊应用需求。

点击“保存”保存设置的内容，保存前必须选定一个监控过滤器，否则会提示错误。

3.4.7. 网站目录管理

3.4.7.1. 修改目录属性

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要修改属性的目录所在的主机组， 列出该组中所有的网站，点击包含该目录的网站，列出该网站下 所有的目录，选择要修改属性的目录，进入如下界面，如图 3-38：

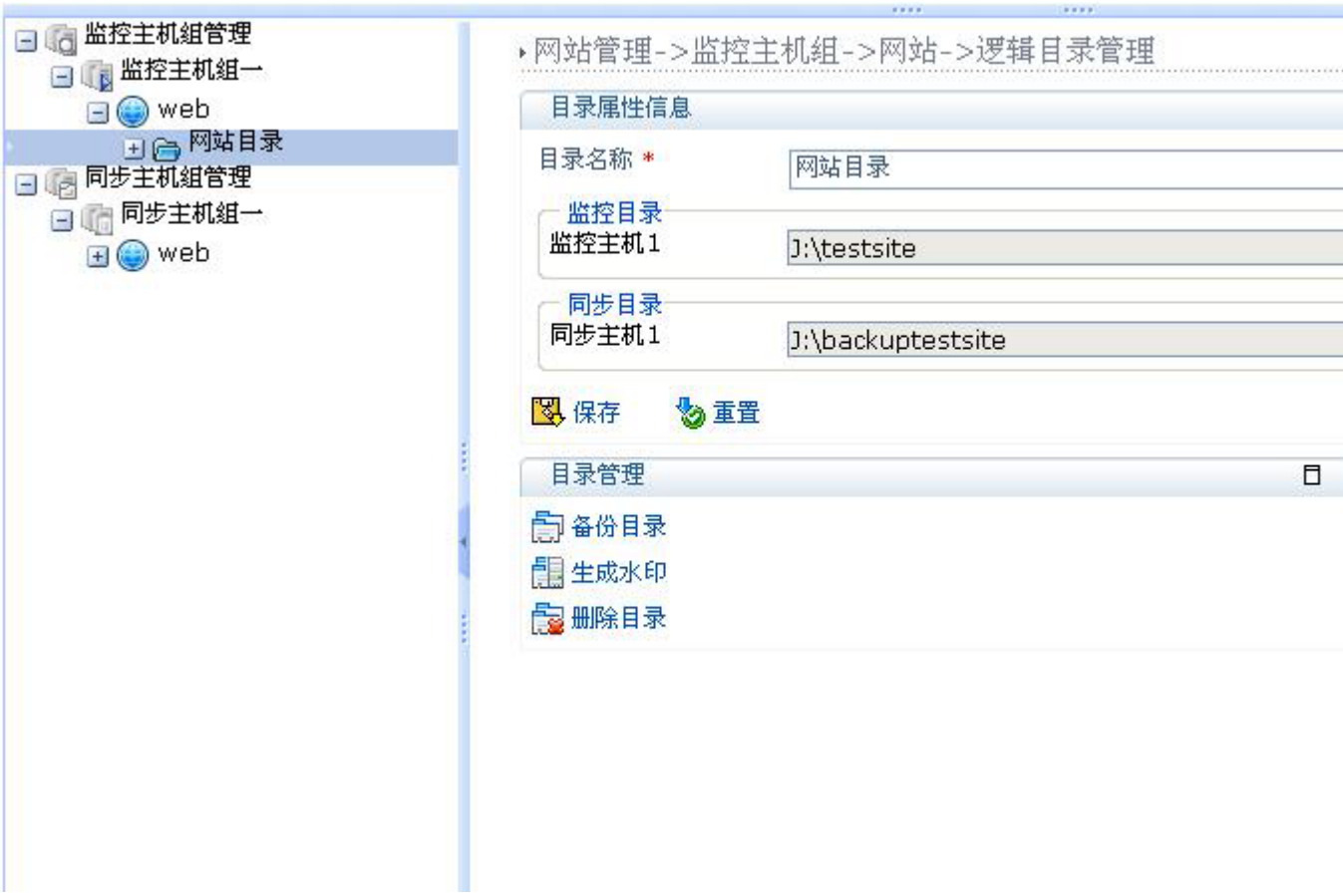


图 3-38

在“目录属性信息”面板内，可以修改目录的名称，修改该目录对应的监控目录和备份目录。点击“确定”，保存新设置的属性，点击“重置”还原修改。 保存成功后，导航树中出现新设置的目录名称。

在“帮助”面板内显示了在修改目录属性时需要注意的一些提示信息。

在同步主机组中选择目录，也可修改目录的属性。

3.4.7.2. 初始化目录

在进行目录初始化之前，必须设置好了该目录的监控目录和备份目录。

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要初始化的目录所在的主机组， 列出该组中所有的网站，点击包含该目录的网站，列出该网站下所有的目录，选择要进行初始化的目录，进入如下界面，如图 3-39：

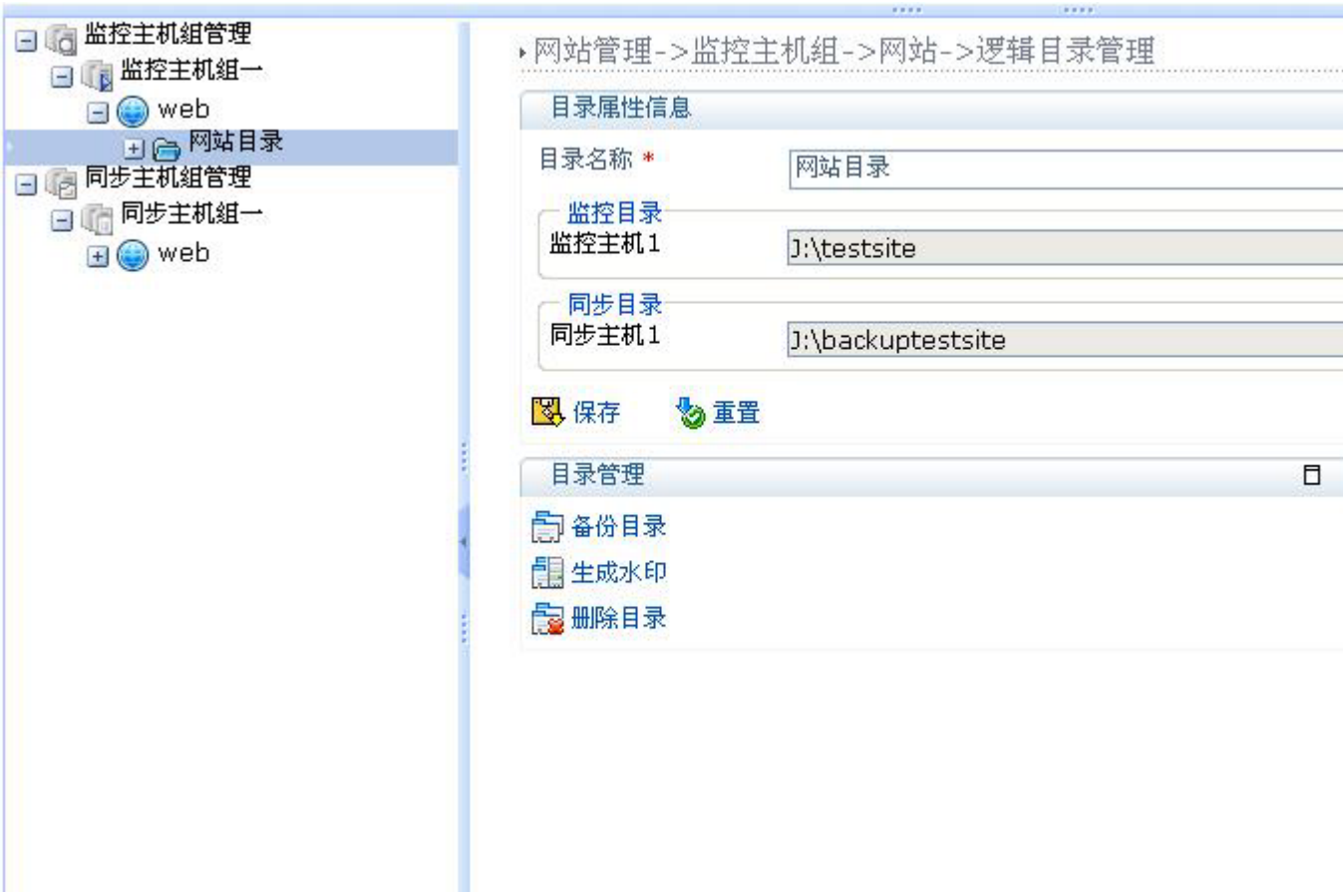


图 3-39

在“目录管理”面板内，选择“初始化目录”，弹出询问窗口，点击“是”初始化目录，点击“否”取消初始化目录。在同步主机组中选择目录，也可进行目录的初始化。

3.4.7.3. 备份目录

在进行目录备份之前，必须设置好了该目录的监控目录和备份目录。备份一个目录主要是在网站的监控端添加了目录， 或者修改了某个目录下的内容，不希望进行网站的备份时，单独备份这个目录。

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要备份的目录所在的主机组， 列出该组中所有的网站，点击包含该目录的网站，列出该网站下所有的目录，选择要进行备份的目录，在“目录管理”面板内，选择“备份目录”， 弹出窗口界面操作同 2.4.4.2 节备份网站。

在同步主机组中选择目录，也可进行目录的备份。

3.4.7.4. 删除目录

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要删除的目录所在的主机组， 列出该组中所有的网站，点击包含该目录的网站，列出该网站下所有的目录，选择要删除的目录，在“目录管理”面板内，选择“删除目录”，弹出询问窗口。

点击“是”删除目录，点击“否”取消删除目录。在同步主机组中选择目录，也可进行目录的删除。

3.4.7.5. 备份物理目录

若只备份网站下的某个目录或者某个文件，直接进行物理目录的备份，在进行目录备份之前，必须设置好了该目录的监控目录和备份目录。

点击导航条上的“网站管理”，进入网站管理界面，点击“监控主机组管理”前的按钮，列出所有的监控主机组，点击要备份的目录所在的主机组， 列出该组中所有的网站，点击包含该目录的网站，列出该网站下所有的目录，点击要进行备份的目录， 列出该目录的物理目录的根结点，点击根结点，进入如下界面，如图 3-40：

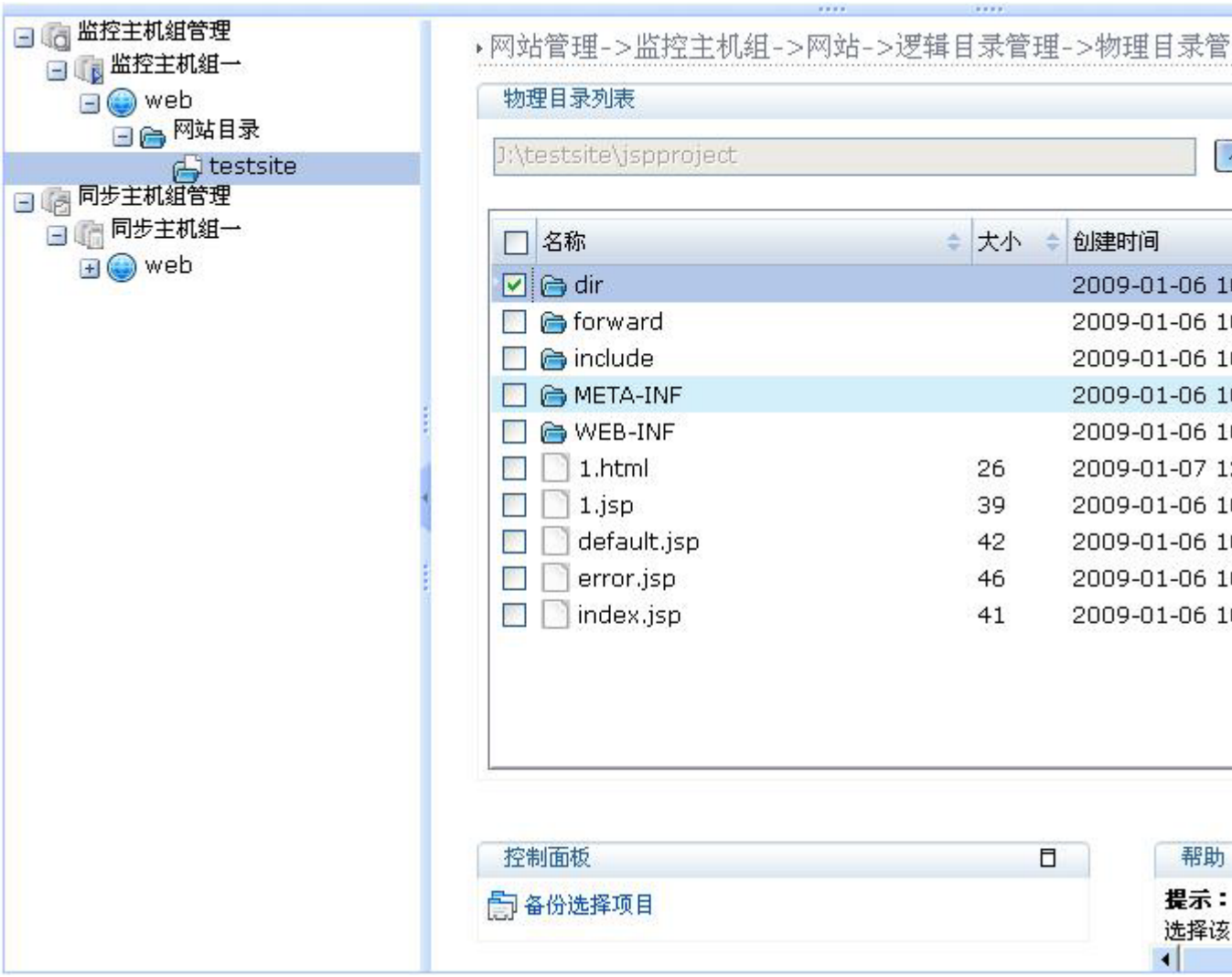


图 3-40

在“目录列表”面板顶部的文本框显示出该目录监控端的物理目录，列表框中列出 该目录根结点下所有的目录和文件，可选择该目录下的各级目录或文件进行备份。目录旁的两个按钮，左边的为返回上一级目录的按钮，右边的 为刷新按钮，用于刷新目录列表。选择某个目录或文件，点击“控制面板”内的“备份选择项目”，如果选择的是一个目录，弹出界面操作同 2.4.4.2 节备份网站。

如果选择一个文件，将直接进行备份。

3.5. 报警管理

3.5.1. 报警平台参数管理

在利用邮件或者短信发送报警信息时，需要设置用于发送邮件的服务器的一些信息，用于发送短信的 COM 端口的信息，否则将不能发送。

点击导航条上的“配置管理”，出现如下界面，如图 3-41：

图 3-41

1、邮件报警设置

在文本框中输入邮件服务器地址、帐号名、密码和发件人 Email 地址，邮件服务器地址为用于发送邮件的服务器 IP 地址，帐号名和密码为用户在邮件服务器上注册的帐号名和密码。

输入收件人邮箱地址，此处设置的收件人邮箱地址，用于接收该管理中心下所有的网站和主机的报警信息。若网站设置了报警策略，按照网站设置的策略发送报警消息。

2、短信报警设置

短信报警需要设置用于报警的 COM 端口，端口为 COM1-COM5，可在下拉列表框中选择，一般情况下使用 COM1 端口。

输入接收短信的手机号码，此处设置的接收号码，用于接收该管理中心下所有的网站和主机的报警信息。若网站设置了报警策略，按照网站设置的策略发送报警消息。

点击“确认”按钮或快捷键（Enter），将参数保存至配置文件，点击“重置”按钮，还原修改操作，点击“关闭”按钮或快捷键（ESC）退出参数管理窗口。

3.5.2. 报警信息管理

3.5.2.1. 报警信息展示

报警信息展示主要展示一个管理中心下所有主机和网站的历史报警信息。

点击导航条上的“报警管理”，进入如下界面，如图 3-42

图 3-42

1、选择大图标方式

选择大图标方式的界面如上图所示，“网站视图”显示监控中心下的所有网站，“主机视图”显示监控中心下的所有主机。在“视图选择”处可以选择视图选择的方式。

将鼠标放在网站图片上，可看到网站的名称，点击图片，可弹出网站的历史报警信息页面。

将鼠标放在主机图片上，可看到主机的名称和 IP 地址，点击图片，可弹出主机的历史报警信息页面。

2、选择小图标方式

小图标方式的展示和大图标一样，只是图标的大小不一样。

3、选择列表方式

选择列表方式的界面如下图所示，网站视图显示监控中心下所有网站的基本信息，若网站有未处理的报警消息，则状态为红色，正常状态下为绿色。 主机视图显示监控中心下所有主机的基本信息，若主机有未处理的数据错误类报警消息时，状态为红色，正常状态下为绿色，如图 3-42：

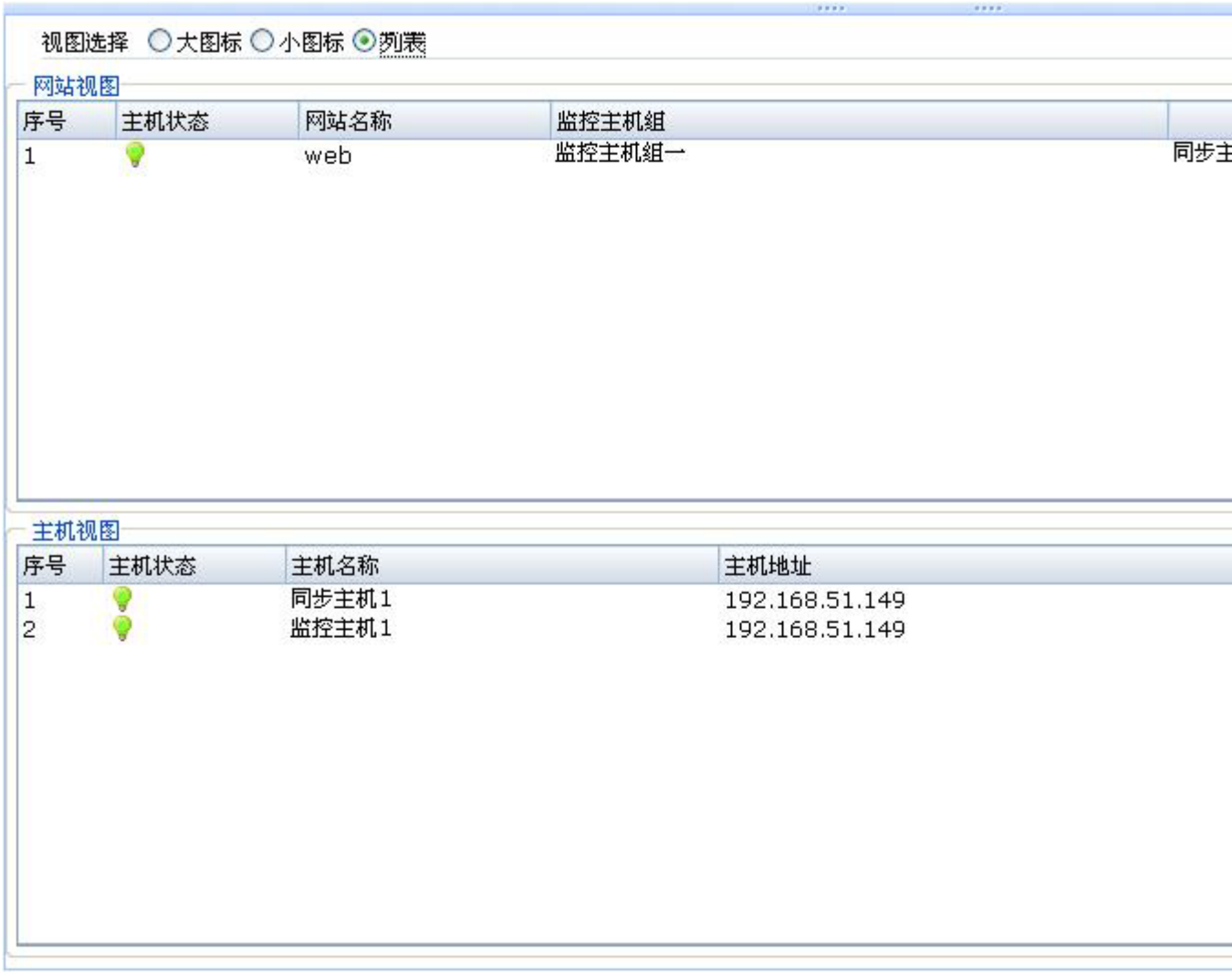


图 3-42

3.5.2.2. 查看报警信息

系统提供了报警信息查询的功能，可以查询各个网站和各个主机的历史报警信息，在查询时可以设置各类查询条件。

1、查看网站的报警信息

点击导航条上的“报警管理”，点击“网站视图”中要查看的网站，弹出网站的历史告警信息页面，如图 3-44：

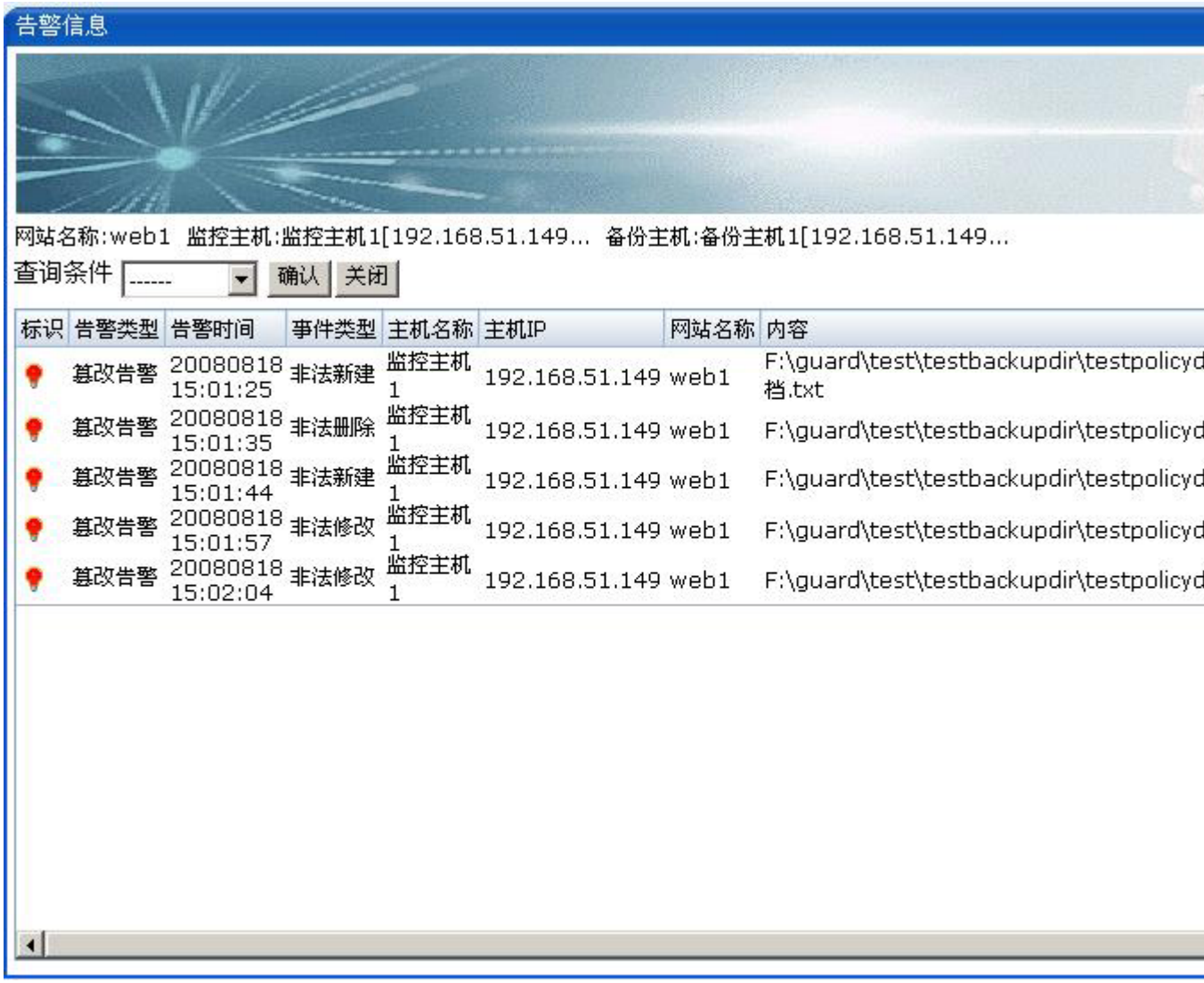


图 3-44

列表中显示出该网站全部的报警信息，设置查询条件，点击确定，在列表中显示查询结果。查询条件有以下几种：

1）报警时间

选择按报警时间查询后，在旁边会出现用于设置时间的文本框，设置好起始时间和结束时间 后确定，则列表中显示出设置的时间段内的所有报警信息。

2）报警类型

选择按报警类型查询后，在旁边会出现用于选择具体报警类型的下拉框，设置了报警类型和子类型后， 点击确定，则列表中显示该类型的所有告警信息。

3）处理结果

选择按处理结果查询后，旁边出现用于选择处理状态的下拉框，设置了处理状态，点击确定， 则列表中显示该处理状态的所有报警信息。

报警消息处于“未处理”状态时，点击该条报警记录可以将状态改为“已处理”。

2、查看主机的报警信息

点击“主机视图”中要查看的主机，弹出主机的历史报警信息页面，列表中显示出该主机全部的报警信息。具体查询操作同查看网站的报警信息。

3.6. 日志管理

3.6.1. 展示日志

点击导航条上的“日志管理”，进入日志管理界面，如图 3-46：

图 3-46

选择要显示的日志类型，列表中则列出该日志类型最新的日志信息，列表中最多显示 100 条日志,如果其中没有您需要的请使用查询功能.

在“统计结果”面板内，用饼形图显示对各个日志类型中各种具体日志的统计结果。主要显示各类具体操作所占的比例。

“帮助”面板内显示了日志管理界面一些操作的提示信息。

3.6.2. 查询日志

系统提供了日志查询的功能，可以按条件查询各类篡改日志、系统运行日志、系统操作日志、系统错误日志和系统维护日志。

点击导航条上的“日志管理”，进入日志管理界面。选择“控制面板”内的“查询日志”，弹出查询日志的窗口，如图 3-47：

图 3-47

设置查询条件，点击“确定”按设置的条件查询日志，点击“取消”，取消查询操作返回，查询成功后，在“日志列表”中显示查询的结果。

3.6.3. 保存日志

系统在记录日志时会覆盖比较老的日志，如果用户需要保留某些类型的日志，先查询出这些日志，然后将这些日志保存起来。

点击导航条上的“日志管理”，进入日志管理界面。选择“控制面板”内的“保存日志”，弹出保存日志的窗口，如图 3-48：

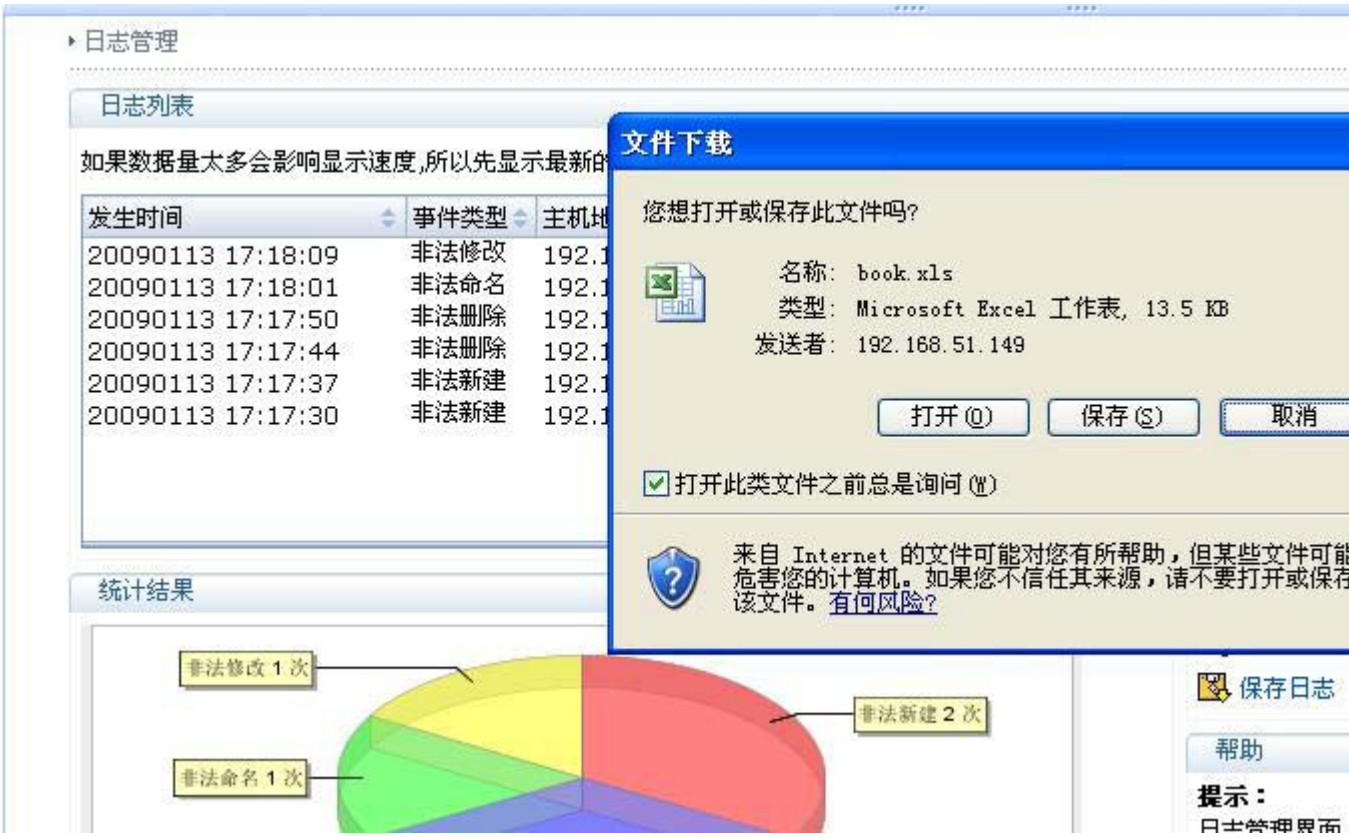


图 3-48

选择“打开方式”按钮，并选择打开方式，则以选择的方式打开日志文件。

选择“保存到磁盘”按钮，将会把日志文件保存到指定的磁盘上。

3.7. 用户管理

3.7.1. 添加用户

点击导航条上的“用户管理”，进入用户管理界面，如图 3-49：

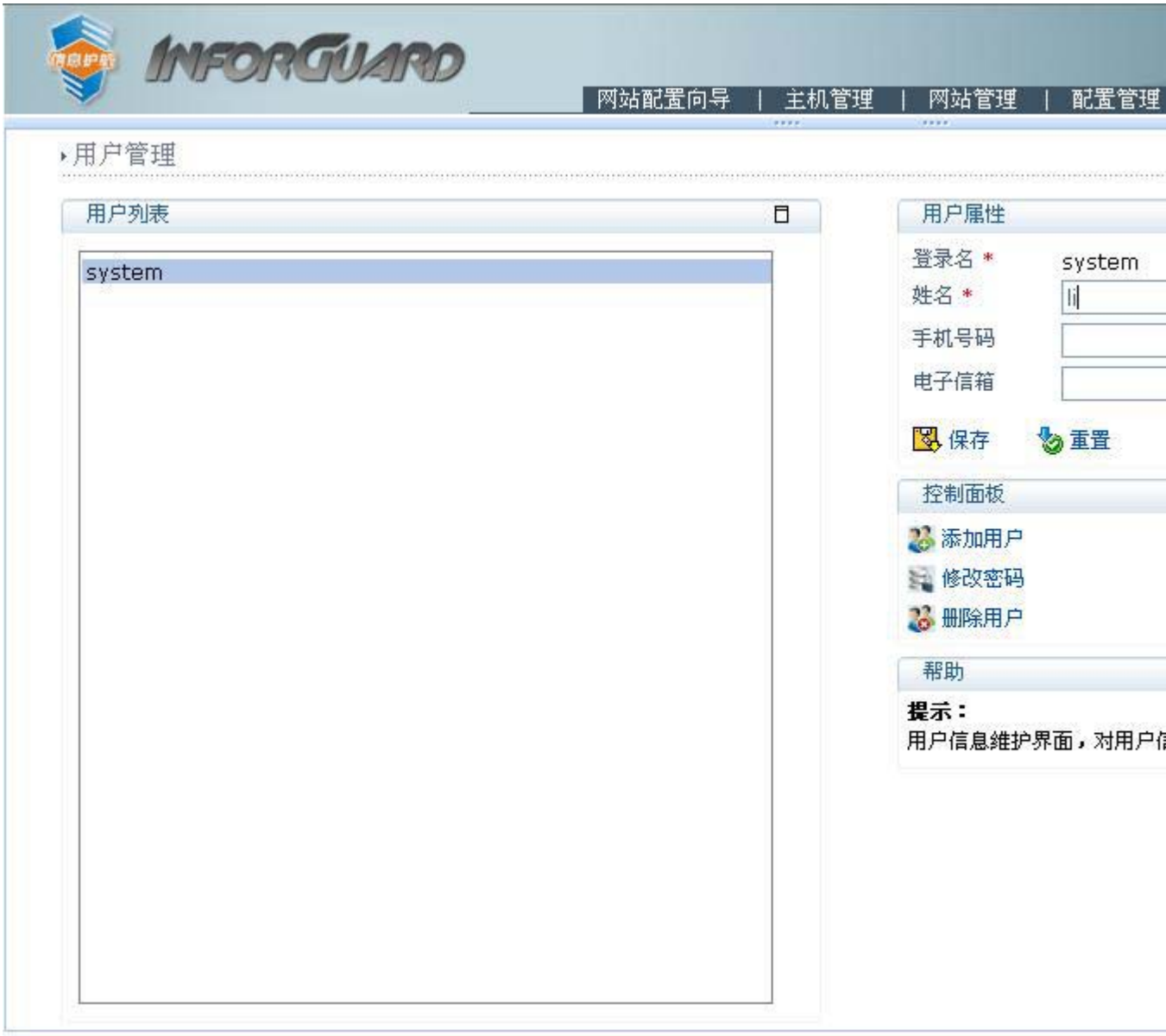


图 3-49

选择“控制面板”内的“添加用户”，弹出添加用户的窗口，如图 3-50：

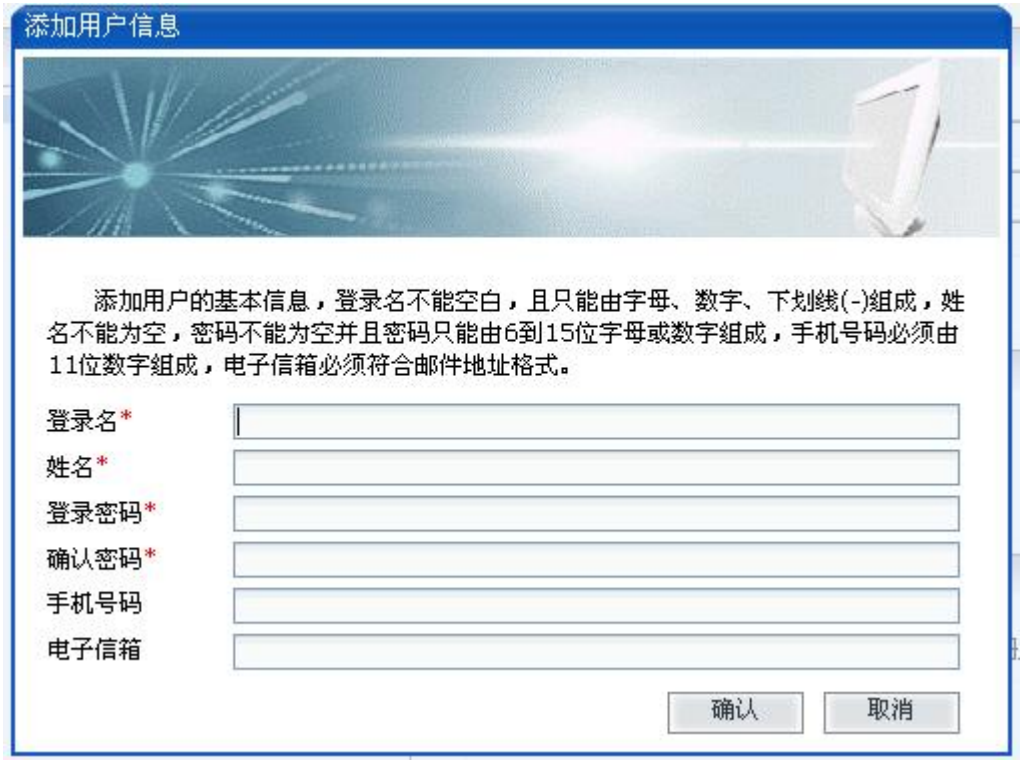


图 3-50

输入用户信息，带*号的属性项为必填项，填写完成后点击“确定”保存用户信息， 点击“取消”，取消添加用户。添加成功后，在用户管理界面的“用户列表”中，可以看到新添加的用户。

3.7.2. 修改用户属性

点击导航条上的“用户管理”，进入用户管理界面，如图 3-51：

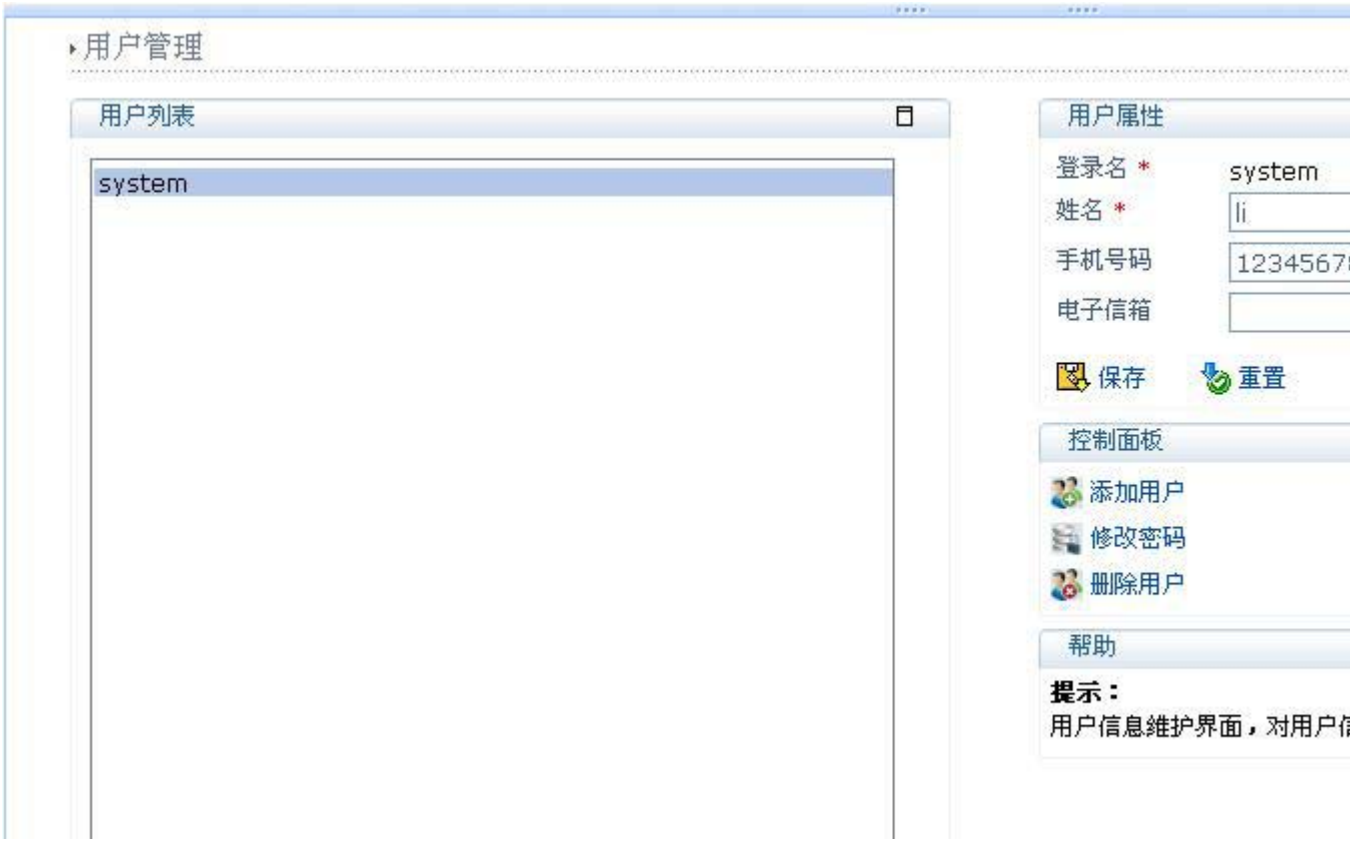


图 3-51

在“用户列表”中选择要修改属性的用户，在“用户属性”面板内可修改用户的属性， 带*号的属性必须填写，修改完成后点击“保存”，保存新设置的属性，点击“重置”还原设置。

3.7.3. 删除用户

点击导航条上的“用户管理”，进入用户管理界面，在“用户列表”中选择要删除的用户，在“控制面板”内选择“删除用户”，弹出提示窗口， 点击“是”删除用户，点击“否”取消删除返回。

3.8. 用户管理

3.8.1. 添加用户

点击导航条上的“用户管理”，进入用户管理界面，如图 3-49：

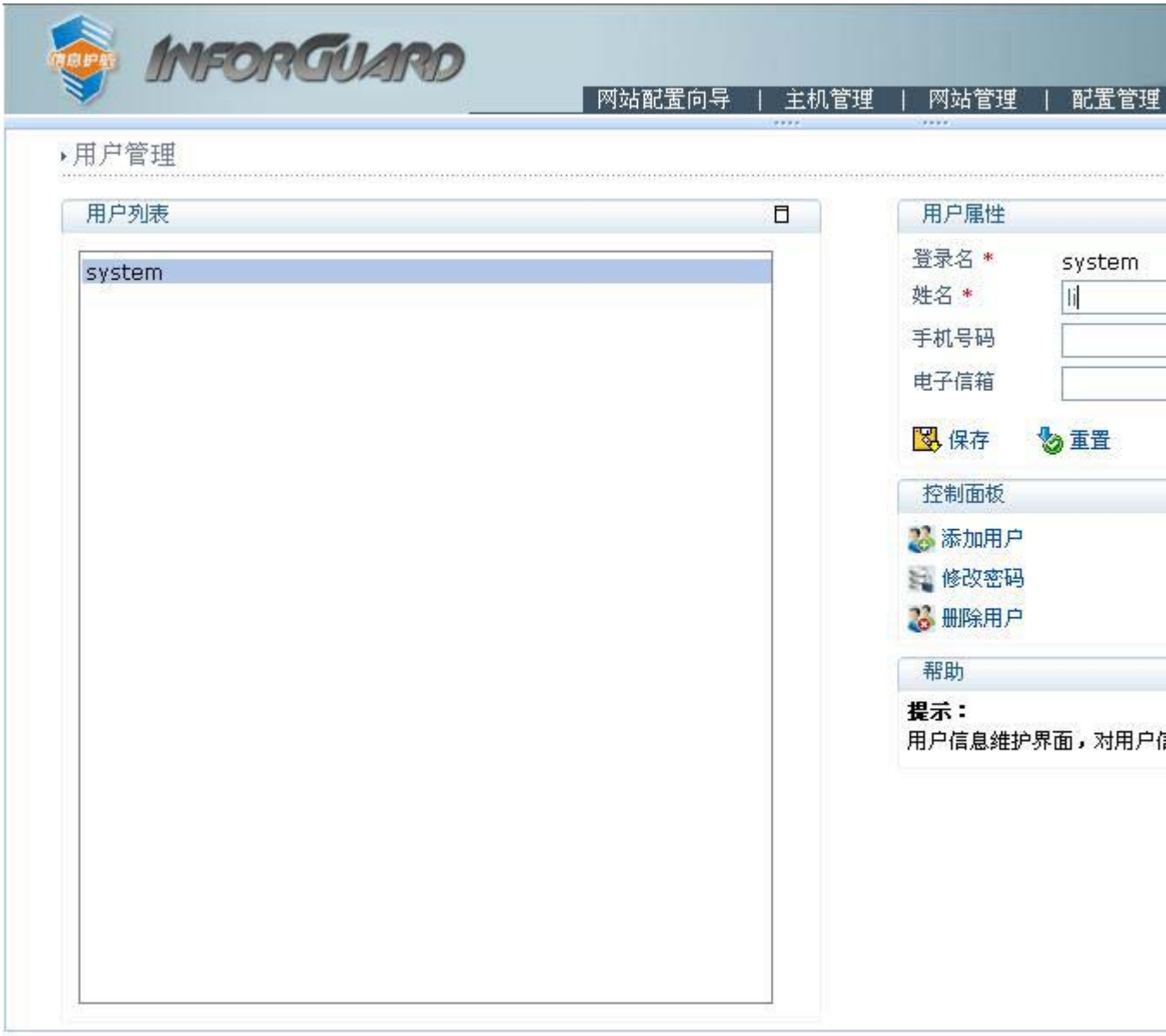


图 3-49

选择“控制面板”内的“添加用户”，弹出添加用户的窗口，如图 3-50：

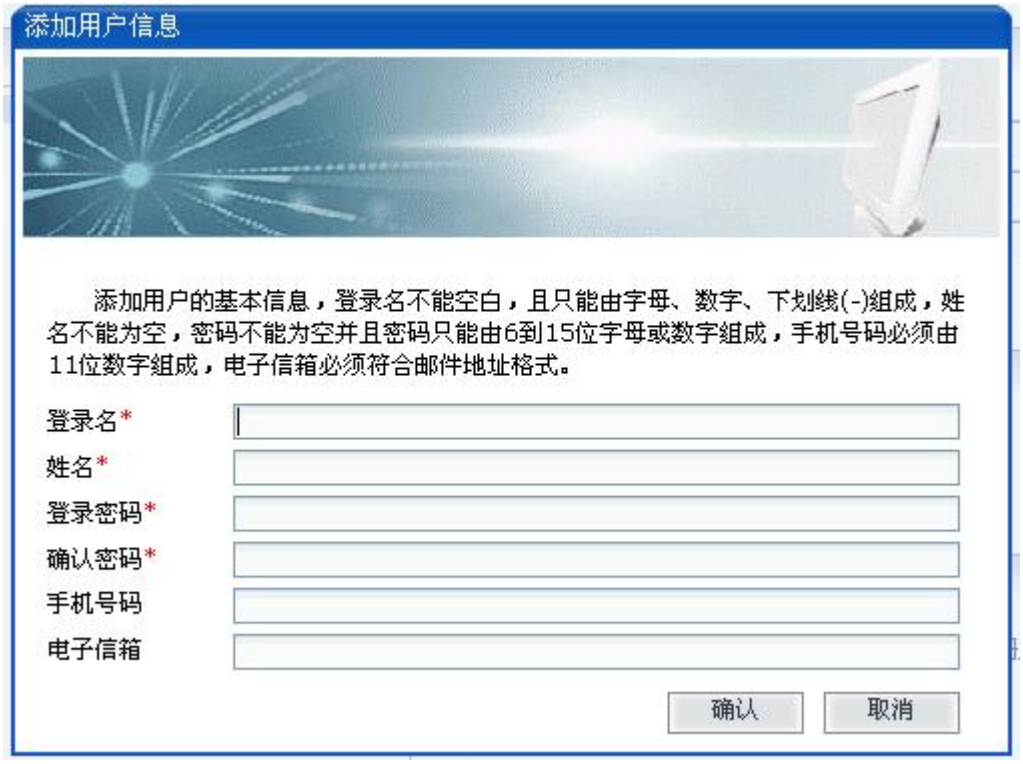


图 3-50

输入用户信息，带*号的属性项为必填项，填写完成后点击“确定”保存用户信息， 点击“取消”，取消添加用户。添加成功后，在用户管理界面的“用户列表”中，可以看到新添加的用户。

3.8.2. 修改用户属性

点击导航条上的“用户管理”，进入用户管理界面，如图 3-51：

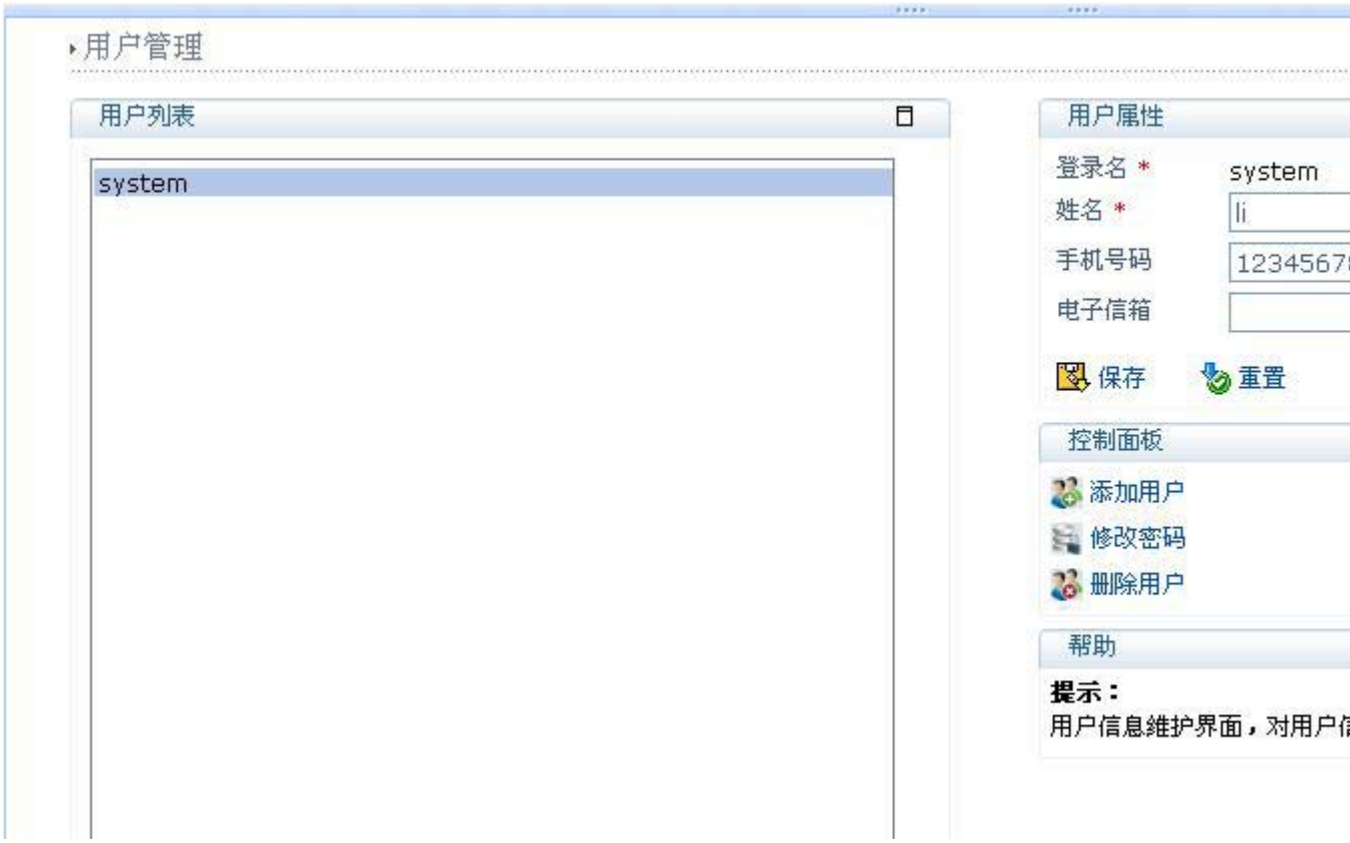


图 3-51

在“用户列表”中选择要修改属性的用户，在“用户属性”面板内可修改用户的属性， 带*号的属性必须填写，修改完成后点击“保存”，保存新设置的属性，点击“重置”还原设置。

3.8.3. 删除用户

点击导航条上的“用户管理”，进入用户管理界面，在“用户列表”中选择要删除的用户，在“控制面板”内选择“删除用户”，弹出提示窗口， 点击“是”删除用户，点击“否”取消删除返回。

3.9. 工具使用

3.9.1. 清理信号量和共享内存工具的使用

1、非 Windows 平台

进入 InforGuard MA 或 InforGuard SA 的安装目录/bin ，该目录下有一个清理信号量和共享内存的脚本文件 ks.

执行命令./ks 即可。

3.9.2. 日志及配置文件打包工具的使用

1、Windows 平台

进入 InforGuard MA 的安装目录\bin，执行该目录下的 MaInfor.bat 脚本，执行完成后在安装目录下生成 MaInfor.zip。

进入 InforGuard SA;的安装目录\bin，执行该目录下的 SaInfor.bat 脚本，执行完成后在安装目录下生成 SaInfor.zip。

2、非 Windows 平台

进入 InforGuard MA 的安装目录\bin，执行该目录下的 MaInfor.sh 脚本，执行完成后在安装目录下生成 MaInfor.tar.gz。

进入 InforGuard SA;的安装目录\bin，执行该目录下的 SaInfor.sh 脚本，执行完成后在安装目录下生成 SaInfor.tar.gz。