前 言

欢迎使用iGuard(V5.5)网页防篡改系统。

iGuard(V5.5)网页防篡改系统是上海天存信息技术有限公司研究开发的网站/网页保护软件的全新版本，它通过全方位的防护视角，采用多手段的检测机制，完整实现了对静态网页、脚本，以及动态内容的实时检测、防护和恢复，使得网站系统和Web应用免受各种攻击和篡改，彻底解决了网站/网页应用的防篡改问题。

本手册详细地介绍了iGuard(V5.5)网页防篡改系统的安装、配置和使用方法。

本手册适用的环境包括：

- 发布服务器：Windows 2003/2008/2010/2012/8/8.1版本。
- 发布服务器：Linux 2.6.XX、3.0.XX 等版本。
- 同步服务器：Windows 2003/2008/2010/2012/8/8.1版本。
- 同步服务器：Linux 2.6.XX、3.0.XX、AIX 5等版本。

本手册内容在印刷后如有更新，恕不一一通知。

技术支持

您在使用iGuard网页防篡改系统V5.5过程中遇到任何技术问题，可以与本产品的制造商上海天存信息技术有限公司联系。

- Web网站：http://www.tcxa.com.cn/
- 电子邮件：support@tcxa.com.cn
- 电话：400-880-8292

第一章 产品概述

1.1 iGuard V5.5 简介

一直以来，上海天存致力于打造高可靠性且简捷易用的网页防篡改系统。

iGuardV5网页防篡改系统是上海天存网页防篡改系统的全新版本。 它延续了 iGuard 3.0网页防篡改系统的特点和优势，同时针对网页防篡改的三大核心问题，对篡改检测点、篡改识别手段、篡改处理机制进行全面优化， 通过全方位的防护视角、使用多种篡改检测手段、辅之以灵活多样的篡改处理机制，彻底解决了网页防篡改所面临的三大核心问题，达到了100%可靠的网页防篡改效果。

iGuard 5.5 版的新特性包括：

- 全新的UI 设计
- 新增事件触发、定时扫描的篡改检查机制；
- 新增文件属性检查、文件内容扫描的篡改识别手段；
- 新增指定恢复、精确同步的篡改恢复同步方式；
- 新增对云平台部署方式的支持；
- 优化发布系统的功能和安全性，增加网页发布的安全审核过程；
- 新增一站式的Web管理中心，对各服务模块进行统一配置和管理；
- 新增被改页面快照、Webshell检查、文件主动备份功能
- 增加邮件、syslog报警方式
- 增加toolbox工具箱配置

1.2 iGUARDV5.5 组成

iGuard V5由发布服务器（STAGINGD）、同步服务器（IGDAGENT）和管理服务器组成，如图示1-1所示。

图示1-1 iGuardV5.5 组成

1.2.1 发布服务器STAGINGD

在发布服务器上，运行了iGuard V5.5发布服务模块，所有网页的合法变更（包括增加、修改、删除、重命名等）都在发布服务器上进行。发布服务器上具有与Web服务器上的网页文件完全相同的目录结构，发布服务器上的任何文 件/目录的变化都会自动和即时地反映到Web服务器的相应位置上，文件/目录变更的方法可以是任意方式的（例如：FTP、SFTP、RCP、NFS、文件共享等）。网页变更后，iGuard V5.5发布服务模块将其同步到Web服务器上。

1.2.2 同步服务器IGDAGENT

同步服务器上运行了iGuard V5.5同步服务模块，以及各个防篡改模块（包括事件触发模块、核心内嵌模块、定时扫描模块）。 其中，同步服务模块负责与发布服务模块进行通信，将发布服务器上的所有网页文件变更同步到Web服务器本地；防篡改模块负责对Web请求进行检查和对网页进行完整性检查。

1.2.3 管理服务器

管理服务器上运行了iGuard V5.5管理中心，所有网页同步规则、防篡改策略、报警通知等都需要在管理中心进行统一配置，完成后再下发到各个发布服务器上。

1.3 典型部署

iGuard V5.5 的典型部署模式应包括发布服务器、管理服务器、Web服务器、内容服务器等。其中，Web服务器和内容管理系统都完全沿用原来的机器，仅需要增加一台发布服务器。对内容管理系统唯一需要做的只是改变它的设置， 将静态页面分发的目标由Web服务器地址改为发布服务器地址即可，无须安装iGuard V5.5 的任何组件。典型部署示意图如图示1-2所示。

图示1-2 典型部署示意图

从下一章开始，将分章节介绍每个模块的组成和使用。如果需要快速入门指导，请首先阅读“第4章 快速配置向导”

第二章 产品安装

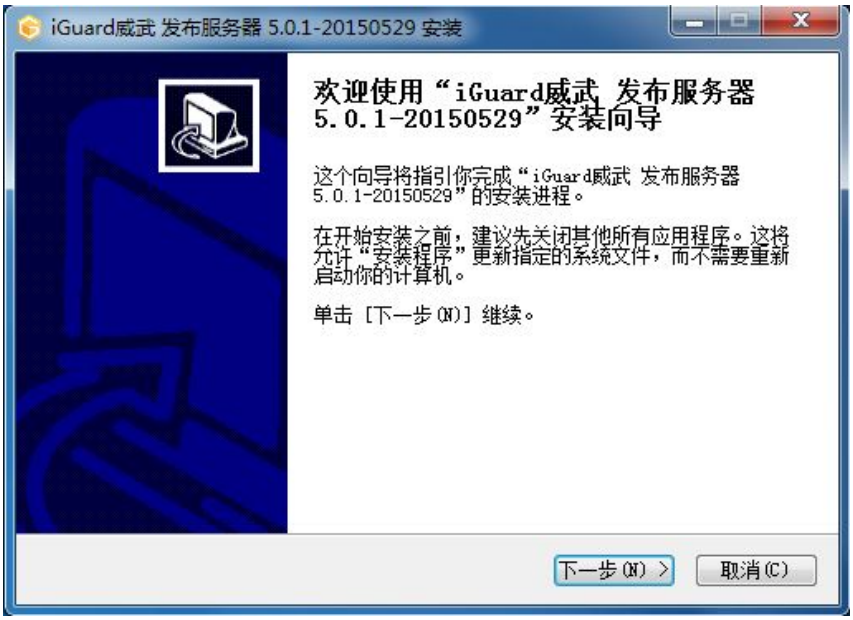
2.1 发布服务器STAGINGD

2.1.1 Windows 发布服务器

2.1.1.1 安装过程

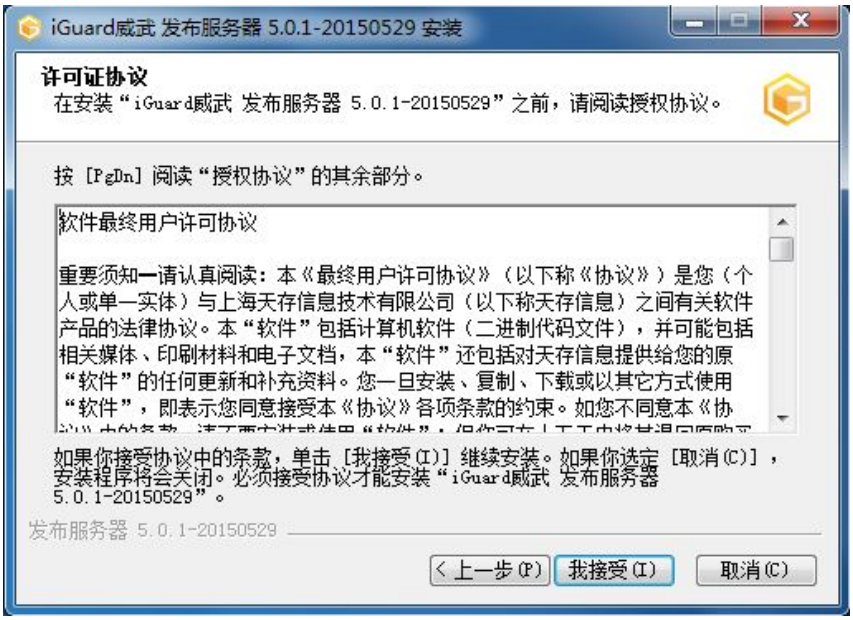
1) 运行发布服务器软件包iGuard5-Stagingd-5.0.1-XXXXXXXX.exe；

2) 安装向导，点击【下一步】按钮（图示2-1）；



图示2-1 安装向导

3) 阅读软件最终用户许可协议，点击【我接受】按钮（图示2-2）；

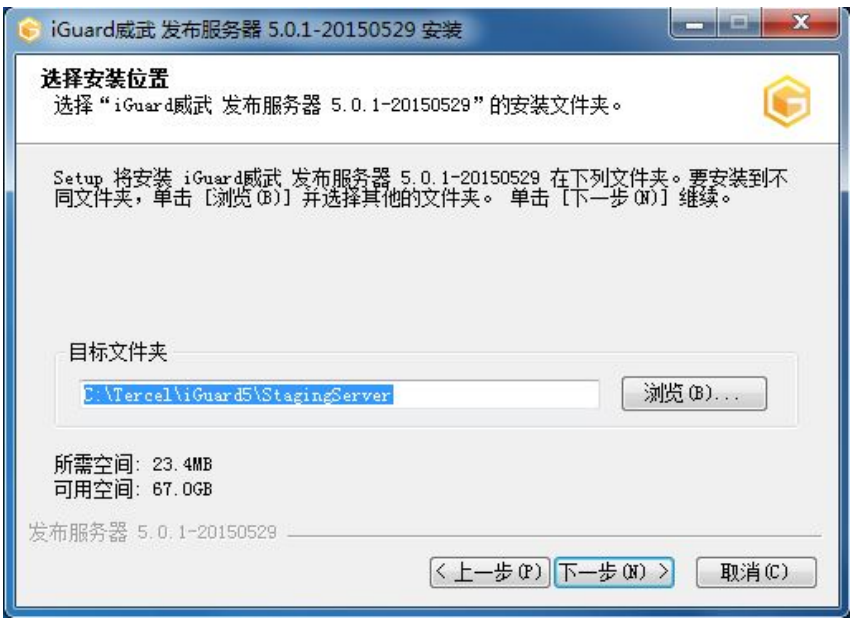


图示2-2 软件最终用户许可协议

4) 输入所购买产品的许可证信息，点击【下一步】按钮（图示2-3）；

图示2-3 许可证信息

5) 选择安装目录，可以点击【浏览】按钮选择其它目标文件夹，确定后点击【下一步】按钮（图示2-4）；



图示2-4 选择安装位置

6) 选中【生成发布服务器标识文件】复选框，点击【安装】按钮（图示2-5）；

注意：发布服务器标识文件用于发布服务器和同步服务器之间进行通讯验证，生成后请在安装目录下找到该文件，并妥善保存。 在安装同步服务器过程中，将会要求使用该标识文件。如果是覆盖安装或者升级，可以选择不重新生成标识文件。一旦该标识文件被重新生成， 请务必将其更新到同步服务器的安装目录下，以确保发布服务器和同步服务器之间能够正常通讯。

图示2-5 生成标识文件

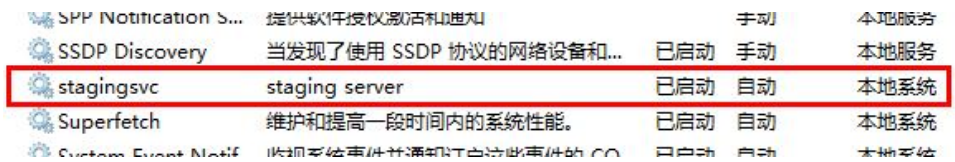
7) 文件将自动复制到目标文件夹，完成后可以选中【立即启动iGuard V5发布服务】复选框，点击【完成】按钮结束安装过程（图示2-6）。

图示2-6 完成安装

2.1.1.2 服务启动和停止

1) 图形界面方式

打开Windows操作系统的【管理工具】→【服务】窗口，查找名称为stagingd5服务，如图示2-7所示。该服务默认自动启动，可以在其【属性】窗口中手工进行启动/停止服务的操作。



图示2-7 stagingd5服务的图形界面管理

2) 命令行方式

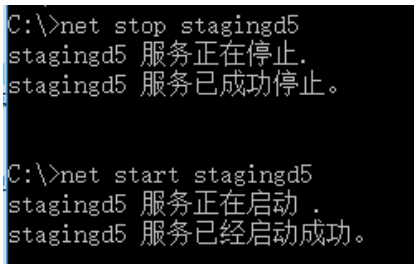
打开Windows操作系统的命令行窗口（在【开始】→【运行】里输入“cmd”命令），输入

> **net start stagingd5**

可以进行启动服务的操作。而输入

> **net stop stagingd5**

可以进行停止服务的操作，如图示2-8所示。



图示2-8 stagingd5服务的命令行方式启动

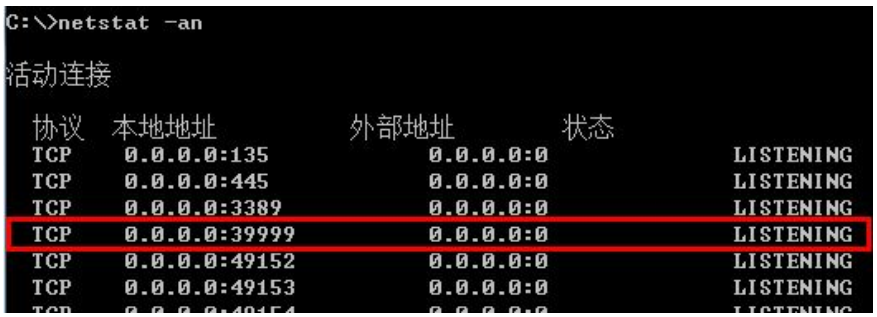
注意：Windows Vista以上版本，需要以管理员身份运行命令行窗口。

2.1.1.3 服务状态查看

打开Windows操作系统的命令行窗口（在【开始】→【运行】里输入“cmd”命令），输入

> **netstat -an**

可以查看网络连接状态，若有TCP端口39999处在监听（LISTENING）状态，则表示发布服务已正常运行，如图示2-9所示。



图示2-9 stagingd5服务状态查看

注意：发布服务的默认端口号是TCP端口39999，若在配置文件中进行了修改，则需要查看相应端口号的状态。

2.1.2 Linux 发布服务器

iGuardV5 发布服务器支持的操作系统内核版本号至少需要 **2.6.32** 以上。

2.1.2.1 安装过程

1) 选择适用的产品包放在需要安装发布服务器的主机上，适用的原则是内核版本尽量接近，硬件平台需要一致。如以Redhat 6 64位平台的安装为例。首先在操作系统中输入“uname -an”命令确认系统内核版本和硬件平台：

```
# uname -an
Linux localhost.localdomain 2.6.32-358.el6.x86_64 #1 SMP Fri Feb 22 00:31:26 UTC 2013 x86_64 x86_64 x86_64
GNU/Linux
```

2) iGuard5-stagingd-Linux-2.6.32-71.el6.x86_64-yyyymmdd.tar.gz为相对应平台的安装程序，把该文件放到需要安装的主机上。

3) 切换到上述安装程序所在的目录，执行以下步骤：

```
# tar xzvf iGuard5-stagingd-Linux-2.6.32-71.el6.x86_64-20160119.tar.gz
# cd iGuard5-stagingd-Linux-2.6.32-71.el6.x86_64
# ./install.sh
```

在输入“./install.sh”脚本命令后，出现以下交互式安装过程。在【Destination dir to install】的停顿提示处，可以手工输入自定义的安装目录。如果直接回车，则安装在默认的“/usr/local/iguard5/stagingd”目录下。

```
Welcome to iGuard Staging Server Installation
(C)Copyright 2002-20015 Shanghai Tercel Info Tech. Co., Ltd.
All rights reserved.
Destination dir to install
(default:/usr/local/iguard5/stagingd)
Server install ok!
Run '/usr/local/iguard5/stagingd/admtool start' to start server
```

2.1.2.2 服务启动和停止

上述安装步骤的最后，提示“**Run '/usr/local/iguard5/stagingd/admtool start' to start server**”，这是启动发布服务器的具体命令，前面的路径会根据实际路径变化。直接按照提示的信息，输入启动服务：

```
# /usr/local/iguard5/stagingd/admtool start
```

如需停止发布服务，则执行：

```
# /usr/local/iguard5/stagingd/admtool stop
```

2.1.2.3 服务状态查看

可通过如下命令，查看39999端口是否处于监听状态，确实安装和启动是否成功。

```
# netstat -an |grep -i 39999
tcp 0 0 0.0.0.0:39999 0.0.0.0:* LISTEN
```

也可以通过以下进程查看命令，确认iGuard发布服务是否正常。通常应该有2个名为stagingd的工作进程。

```
# ps -ef|grep stagingd
root 7769 1 0 16:07 00:00:00 /usr/local/iguard5/stagingd/stagingd -d /usr/local/iguard5/stagingd
root 7770 7769 0 16:07 00:00:00 /usr/local/iguard5/stagingd/stagingd -d /usr/local/iguard5/stagingd
```

完成安装后，则可以通过在浏览器里访问 **https://发布服务器IP:39999/**，登录Web控制台，进行下一步配置，具体参见第三章【管理中心】。

2.1.2.4 设置自启动

编辑系统自启动文件/etc/rc.local，在最后加入以下一行：

```
/usr/local/iguard5/stagingd/admtool start
```

2.1.2.5 Linux 文件监控模式一：inotify（默认）

Linux版Stagingd服务安装完成后，即可默认监控原生本地目录下的文件变化，使用的是inotify机制。

该机制的缺陷是，文件过多或者目录过深的时候，可能导致监控的失效。所以在安装完成后，建议调整该数量，增大监控数量。方法是编辑 /etc/sysctl.conf 系统配置文件，加入：

```
#编辑 /etc/sysctl.conf
fs.inotify.max_user_watches=10485760
```

然后以root用户权限，执行以下命令使配置生效：

> **# sysctl -p**

确认配置已生效：

> **# cat /proc/sys/fs/inotify/max_user_watches**

备注：Linux从kernel 2.6.13开始支持inotify机制。它的各项默认内核参数为：

- **/proc/sys/fs/inotify/max_queued_events** 默认值: 16384 排队的inotify事件最大值，超出这个值的事件会被丢弃，但会触发IN_Q_OVERFLOW报警
- **/proc/sys/fs/inotify/max_user_instances** 默认值: 128 每一个用户可创建的inotify实例数量上限
- **/proc/sys/fs/inotify/max_user_watches** 默认值: 8192 每个inotify 实例可关注的目录上限

注意！使用默认inotify机制做文件变化监控，可能有如下两个问题：**1）目录太深或文件数量太多的情况下，有可能会有文件变化信息丢失的问题；2）在监控目录下，如果存在软链接形式的子目录时，有可能导致目录嵌套，任务死循环的问题。** 这两个问题可以使用iLocker 监控方式解决。

2.1.2.6 Linux 文件监控模式二：iLocker模式

也可以通过天存公司的iLocker文件监控模式，监控Linux下的文件变化。

先按常规方式安装iLocker for linux，如以使用 ilocker-20170518.tar.gz 安装包为例，可执行：

> **# tar xzvf ilocker-yyyymmdd.tar.gz**
> **# cd ilocker**
> **# cp -rf * /usr/local/iguard5/stagingd/**

到iLocker/lib子目录下，选择合适的ilocker.ko文件，以下是示例的步骤，请根据实际情况选择适用的ilocker.ko文件。

> **cd /usr/local/iguard5/stagingd/lib**
> **ln -sf ilocker\@2.6.32-573.el6.x86_64\@x86_64\@rhel6.7\@.ko ilocker.ko #这步要根据uname -an的实际情况选择合适模块**

无需做其他配置，正常地启动iLocker：

> **# /usr/local/iguard5/stagingd/bin/ilocker start**

在 linux版发布服务器的安装目录下执行：

```
# cd /usr/local/iguard5/stagingd
# mv libfen.so libfen.so.original
# ln -sf liblsmxfen.so libfen.so
```

在完成上述步骤后，才能启动iGuard发布服务程序：

```
# cd /usr/local/iguard5/stagingd/admtool start
```

然后通过Web控制台，常规地设置源目录和同步目录即可。

最后，再设置自启动文件（通常为/etc/rc.local时），一定要先写ilocker start这句命令，再接着写stagingd的admtool start，不要把顺序颠倒过来，例如：

```
/usr/local/iguard5/stagingd/bin/ilocker start
/usr/local/iguard5/stagingd/admtool start
```

备注：iLocker2 做发布监控时的调试命令：

```
# echo instruction=print > /dev/ilocker1
# dmesg
```

在执行dmesg命令后，能看到发布程序里配置的监控目录，说明两者关联好了，可以正常监控指定目录的文件变化了。如果执行了dmesg后，没看到发布程序里的监控目录，那就是有问题的。

注意！使用默认iLocker机制做文件变化监控，可能有如下两个问题：**1）需要提前确定系统的版本，因为iLocker需要使用比较符合的系统版本的模块；2）如果把iLocker监控用在NFS服务器端，有微小可能会有消息遗漏的现象，不推荐使用。**

备注：如果依然需要使用iLocker1作为Linux 发布监控模式，具体步骤参见 FAQ 5.4.11 "Linux发布服务器怎么切换为 iLocker1做文件变化监控？"

2.1.2.7 Linux 文件监控模式三：Fuse模式

如果一个地方已经装过iGuardvV3的Linux发布服务器，稳定运行了很长一段时间了。 现在换用V5，还是可以继续沿用V3的fuse模式文件监控的。

具体方法是在发布服务器的安装目录下，执行以下命令：

```
# mv libfen.so libfen.so.original
# cp libnfslogfen.so libfen.so
```

其他使用方式和iGuardv3版本一致。

以上三种监控方式，只能同时采用其中一种，不能混合使用。

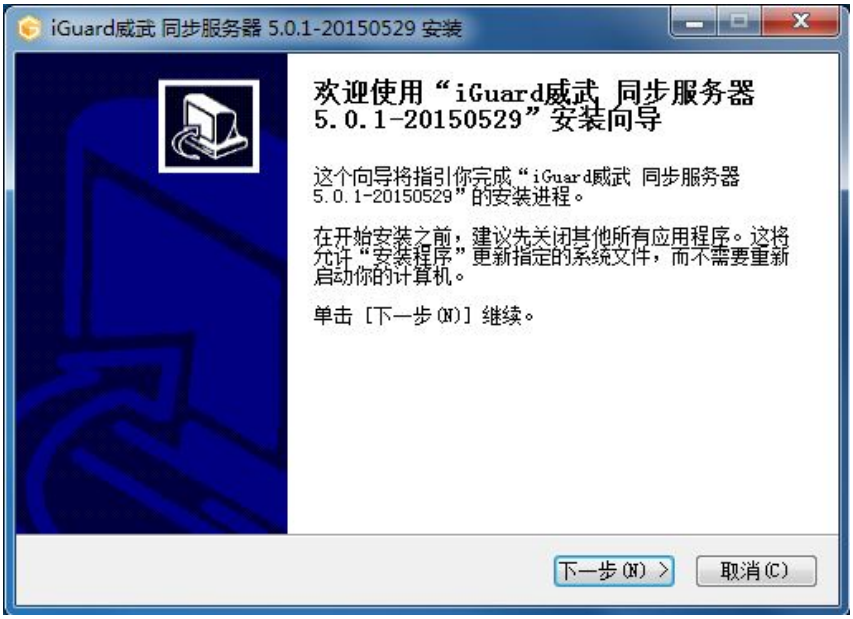
2.2 同步服务器IGDAGENT

2.2.1 Windows同步服务器

2.2.1.1安装过程

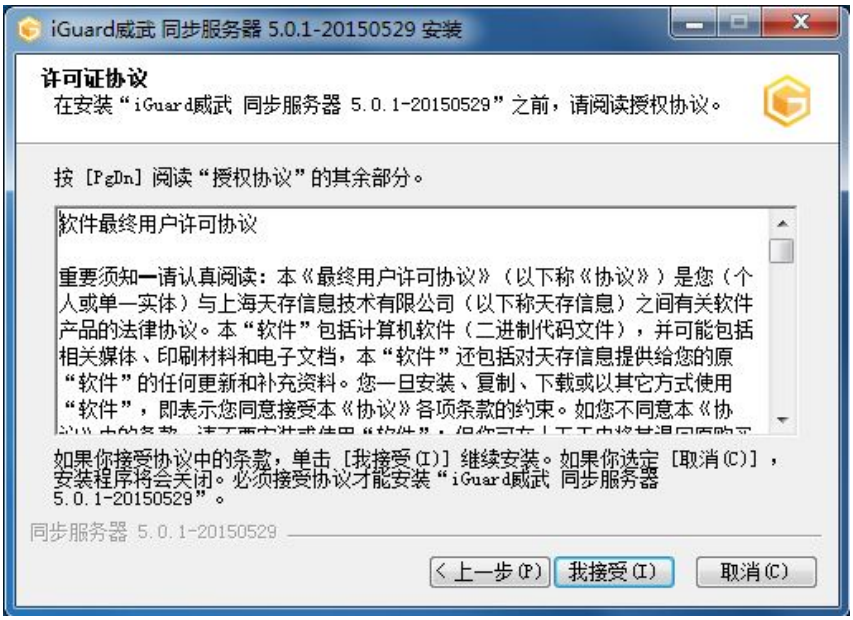
1) 运行发布服务器软件包iGuard5-igdagent-5.0.1-XXXXXXXX.exe;

2) 安装向导，点击【下一步】按钮（图示2-10）；



图示2-10 安装向导

3) 阅读软件最终用户许可协议，点击【我接受】按钮（图示2-11）；



图示2-11 软件最终用户许可协议

4) 选择安装目录，可以点击【浏览】按钮选择其它目标文件夹，确定后点击【下一步】按钮（图示2-12）；

图示2-12 选择安装位置

5) 选择发布服务器标识文件所在位置，点击【安装】按钮（图示2-13）； 注意：发布服务器标识文件用于发布服务器和同步服务器之间进行通讯验证，请在发布服务器的安装目录下查找该文件。

图示2-13 选择标识文件

6) 文件将自动复制到目标文件夹，完成后可以选中【立即启动iGuard V5同步服务】复选框，点击【完成】按钮结束安装过程（图示2-14）。

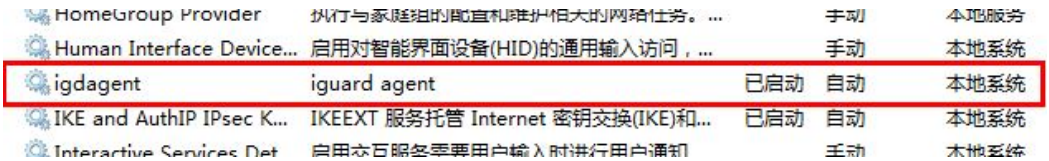
图示2-14 完成安装

注意：在同步服务器的安装过程中，将以驱动程序的方式同时安装文件变化检测系统FCNOTIFY。

2.2.1.2服务启动和停止

1) 图形界面方式

打开Windows操作系统的【管理工具】→【服务】窗口，查找名称为igdagent的服务，如图示2-15所示。该服务默认自动启动，可以在其【属性】窗口中手工进行启动/停止服务的操作。



图示2-15 igdagent服务的图形界面管理

2) 命令行方式

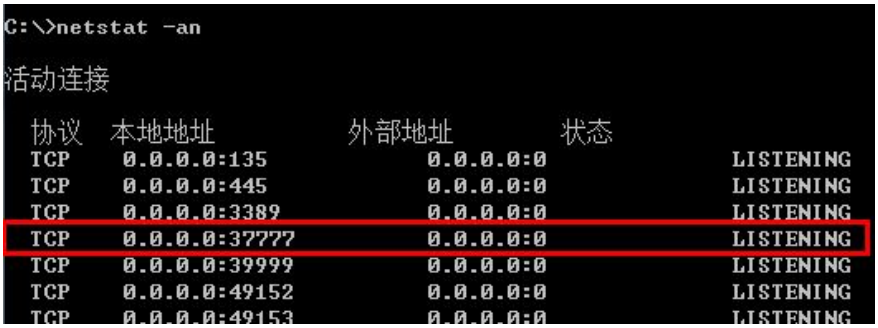
打开Windows操作系统的命令行窗口（在【开始】→【运行】里输入“cmd”命令），输入“net start igdagent” 可以进行启动服务的操作，输入“net stop igdagent”可以进行停止服务的操作，如图示2-16所示。

图示2-16 igdagent服务的命令行管理

注意：Windows Vista以上版本，需要以管理员身份运行命令行窗口。

2.2.1.3服务状态查看

打开Windows操作系统的命令行窗口（在【开始】→【运行】里输入“cmd”命令），输入“netstat -an” 可以查看网络连接状态，若有TCP端口37777处在监听（LISTENING）状态，则表示同步服务已正常运行，如图示2-17所示。



图示2-17 igdagent服务状态查看

注意：同步服务的默认端口号是TCP端口37777，若在配置文件中进行了修改，则需要查看相应端口号的状态。

2.2.2 Linux/UNIX 同步服务器

iGuardV5 同步服务器支持的操作系统内核版本号至少需要 **2.6.32** 以上。

2.2.2.1 安装过程

1) 选择适用的产品包放在需要安装的Web服务器主机上，适用的原则是内核版本尽量接近，硬件平台需要一致。如以Redhat 6 64位平台的安装为例。首先在操作系统中输入“uname -an”命令确认系统内核版本和硬件平台：

> **# uname -an**
> **Linux localhost.localdomain 2.6.32-358.el6.x86_64 #1 SMP Fri Feb 22 00:31:26 UTC 2013 x86_64 x86_64 x86_64 GNU/Linux**

2) 所以选择iGuard5-igdagent-Linux-2.6.32-71.el6.x86_64-yyyymmdd.tar.gz为相对应平台的安装程序，把该文件放到需要安装的主机上。

3) 把与之相配套的发布服务器安装目录下的身份认证文件【staging.id】也要放到同一台Web服务器上待用，存放的目录不限。安装完后，该文件不再需要，可以直接删除。以下假设【staging.id】文件放在/tmp目录下。

4)切换到上述iGuard5-igdagent-Linux-2.6.32....tar.gz安装程序所在目录，执行以下步骤：

> **# tar xzvf iGuard5-igdagent-Linux-2.6.32-71.el6.x86_64-20160119.tar.gz**
> **# cd iGuard5-igdagent-Linux-2.6.32-71.el6.x86_644**
> **# ./install.sh**

在输入“./install.sh”脚本命令后，出现以下交互式安装过程：在【Destination dir to install】的停顿提示处，可以手工输入自定义的安装目录，如果直接回车，则安装在默认的“/usr/local/iguard5/igagent”目录下；在【Locate the file path of ‘staging.id’】 的输入里，填入从发布服务器端拷贝的相应staging.id文件路径，如举例中为/tmp/staging.id；在【Will install wmktool now?】提示下，可以选择是否安装水印签发工具，默认直接回车为选择安装。

```
Welcome to iGuard Agent Server Installation
(C)Copyright 2002-2015 Shanghai Tercel Info Tech. Co., Ltd.
All rights reserved.
Destination dir to install
(default:/usr/local/iguard5/igdagent)

Locate the file path of 'staging.id',
which is created during the installation of staging server
/tmp/staging.id
Will install wmktool now?
Confirm [yes/no]:yes
Server install ok!
Run '/usr/local/iguard5/igdagent/admtool start' to start server
```

2.2.2.2 服务启动和停止

上述安装步骤的最后，提示“Run ‘**/usr/local/iguard5/igagent/admtool start’ to start server**”，这是启动同步服务器的具体命令，前面的路径会根据实际路径变化。直接按照提示的信息，输入启动服务：

> **# /usr/local/iguard5/igagent/admtool start**

如需停止发布服务，则执行：

> **# /usr/local/iguard5//igagent/admtool stop**

2.2.2.3 服务状态查看

可通过如下命令，查看37777端口是否处于监听状态，确实安装和启动是否成功。

> **# netstat -an |grep 37777**
> **tcp 0 0 0.0.0.0:37777 0.0.0.0:* LISTEN**

也可以通过以下进程查看命令，确认iGuard发布服务是否正常。通常应该有2个名为igdagent的工作进程。

> **# ps -ef |grep igdagent**
> **root 8769 1 0 16:07 ? 00:00:00 /usr/local/iguard5/igdagent/igdagent -d /usr/local/iguard5/igdagent...**
> **root 8770 7769 0 16:07 ? 00:00:00 /usr/local/iguard5/igdagent/igdagent -d /usr/local/iguard5/igdagent...**

2.2.2.4 设置系统自启动

编辑系统自启动文件/etc/rc.local，在最后加入以下一行：

```
/usr/local/iguard5/igdagent/admtool start
```

如果需要以特定的用户权限，如weblogic用户启动同步服务，加入的启动命令为：

```
su -c “/usr/local/iguard5/igdagent/admtool start” weblogic
```

2.3 防护方式 Windows

2.3.1 文件水印初始化

在加载各核心内嵌模块之前，需要对保护的网站目录进行初始化，初始化的过程就是扫描整个网站保护目录，对所有文件添加水印的过程。在初始化之前，请先确认当前网站没有被非法添加网页木马， 没有隐藏后门，否则一旦经过初始化阶段，这些有问题的文件也会被认定为合法文件了。

如果需要检查网站是否包含网页后门，请查阅【5.2 检查网页木马/Windows】章节。

推荐在控制台里，使用图形化方式初始化水印。如果需要在控制台里执行水印初始化，**一定要先做好站点的路径映射和服务器关联**，否则无法在控制台上执行该步骤。水印初始化的具体步骤请见【3.4.6 水印签发 】章节。

在少量特殊情况下，也可以使用命令行方式批量签发水印。方法：

- 编辑”同步服务器安装目录“/wmktool.conf 配置文件，把其中的 dirs 段，改为需要做水印初始化的目录；如果有多个目录，需要用逗号分隔，每个目录的两边用双引号括起来；目录分隔符要使用正斜杠”/“：

```
{"ServerRoot":"C:/Tercel/iGuard5/igdagent",
"filter":[
""
],
"dirs":[
"C:/Apache24/htdocs","C:/Apache2427/htdocs"
]
}
```

- cmd回到命令行状态，执行以下命令，可以对wmktool.conf里指定的目录执行水印初始化：

> **wmktool.exe -f wmktool.conf**

- 如果需要查询某个特定文件的水印值是否正常，可以执行：

> **wmktool.exe -f wmktool.conf -c verify ”需要校验的文件名“**

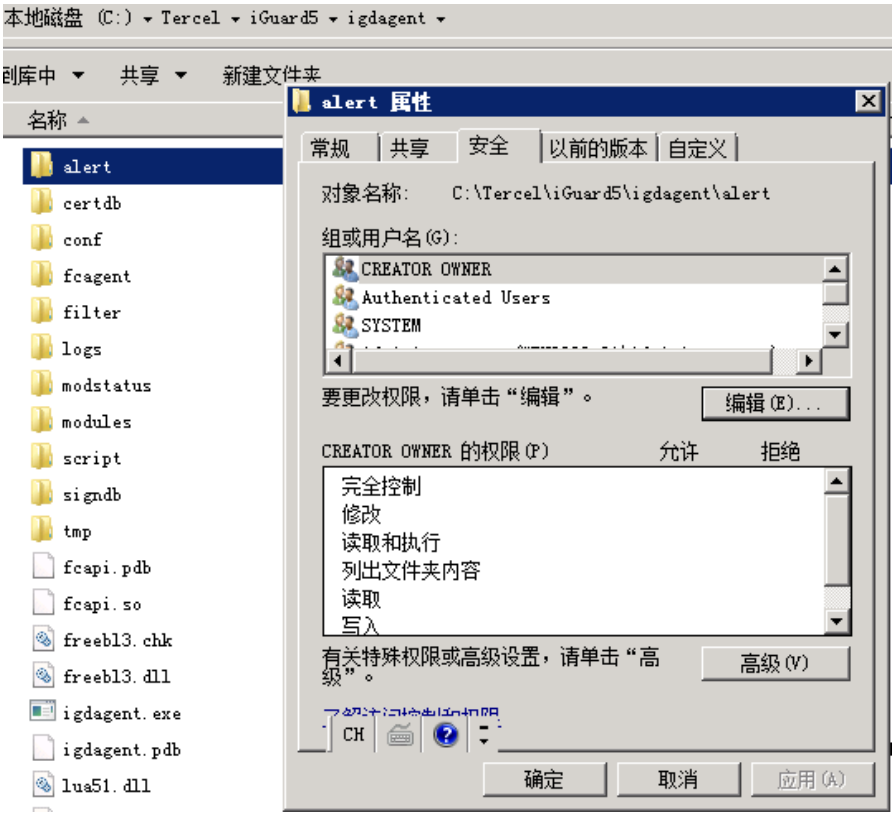
如果返回码为0，则校验通过；如果返回码为110，则校验失败。

2.3.2 Windows IIS7 核心内嵌

- 加载本模块前，请先确认已经为网站目录文件做过初始化，详见【3.4.4 水印签发 】章节。
- 如果需要对特定的文件/目录做特殊处理，如不需要进行防护，请提前做好设置，具体步骤参见【4.3.2对核心内嵌模块，放开对特定文件/目录的防护】章节。

在上述两步已完成的基础上，再进行以下配置。

1） 目录权限设置：分别设置同步服务器安装目录（默认C:\Tercel\iGuard5\igdagent）下的三个子目录：alert、modules、signdb对用户Authenticated Users'具有可读和可写权限。具体操作方法为： 右击要设置权限的子目录，选择“共享与安全”，在“安全”选项卡里，选择“添加”，选择用户“Authenticated Users”，并赋予该用户对子目录的读写权限（图示2-18）。

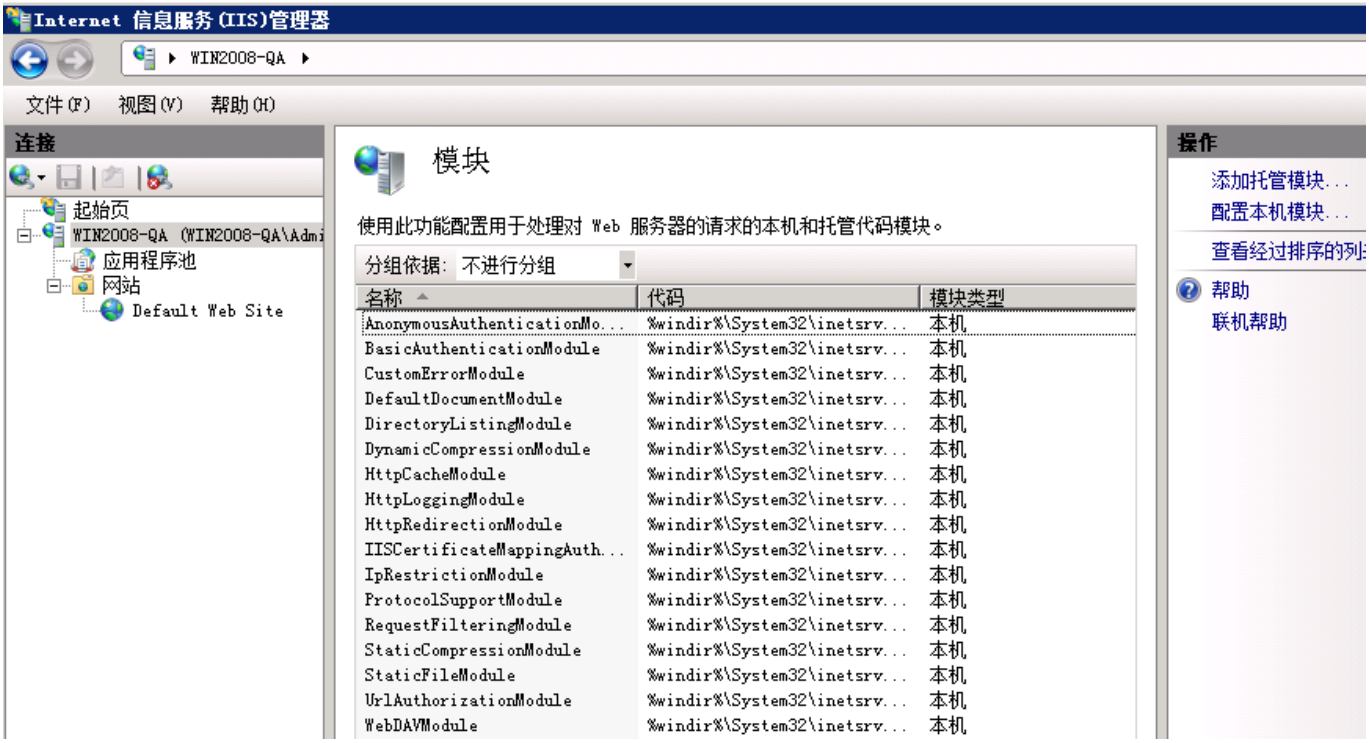


图示 2-18 设置特定目录的用户权限

2）在全局注册模块：运行“开始”→“管理工具”→“Internet信息服务”或直接执行Inetmgr。点击“Internet信息服务（IIS）管理器”主窗体下的顶级主机名（如本例中“WIN2008-QA”），显示IIS配置主页（图示2-19）。

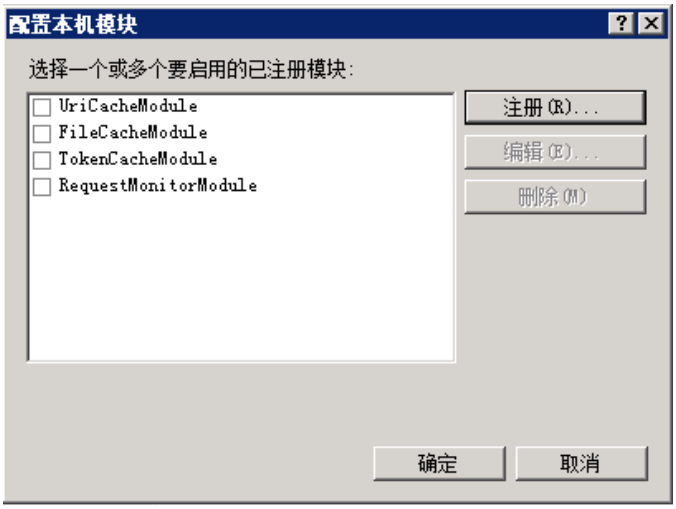
图示 2-19 显示IIS配置管理器主页（IIS7.0）

在IIS配置管理器主页中的功能列表中，选择“模块”功能，双击打开，进入模块界面（图示2-20）。



图示 2-20 打开模块界面（IIS7.0）

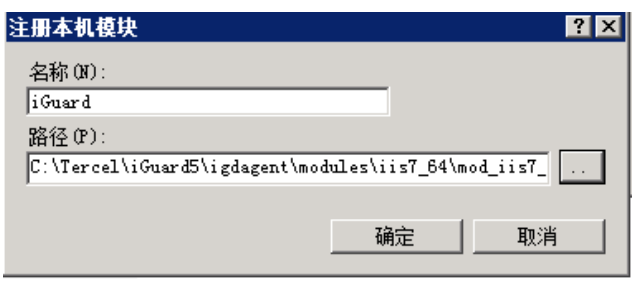
点击右上角的“配置主机模块”，再打开的配置主机模块窗体中点击“注册”按钮（图示2-21）。



图示 2-21 配置本机模块

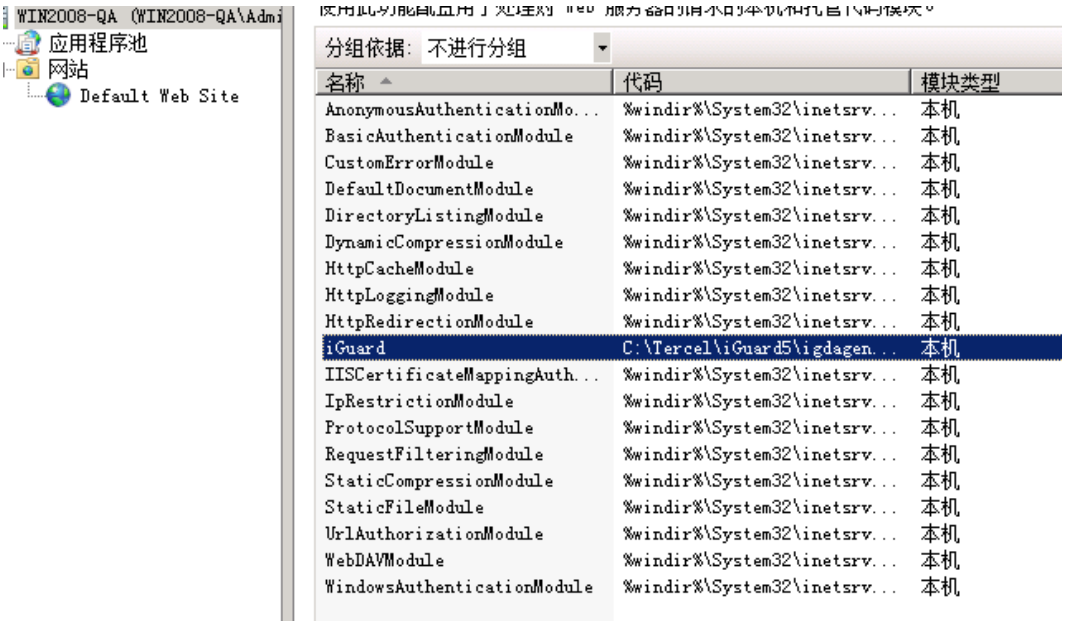
并在弹出的注册本机模块窗体中“名称（N）”中填入“iGuard”，“路径”浏览选择同步服务器安装目录下的mod_iis7_iguard.dll模块（图示2-22）。

> **32位系统请选择：'C:\Tercel\iGuard5\igdagent\modules\iis7\mod_iis7_iguard.dll'**
> **64位系统请选择：'C:\Tercel\iGuard5\igdagent\modules\iis7_64\mod_iis7_iguard.dll'**



图示2-22 注册本机模块（IIS7.0）

完成后点击“确定”按钮，“注册本机模块”窗体中的iGuard模块已成功注册。此时iGuard模块会显示在全局启用的模块列表中（图示2-23）。

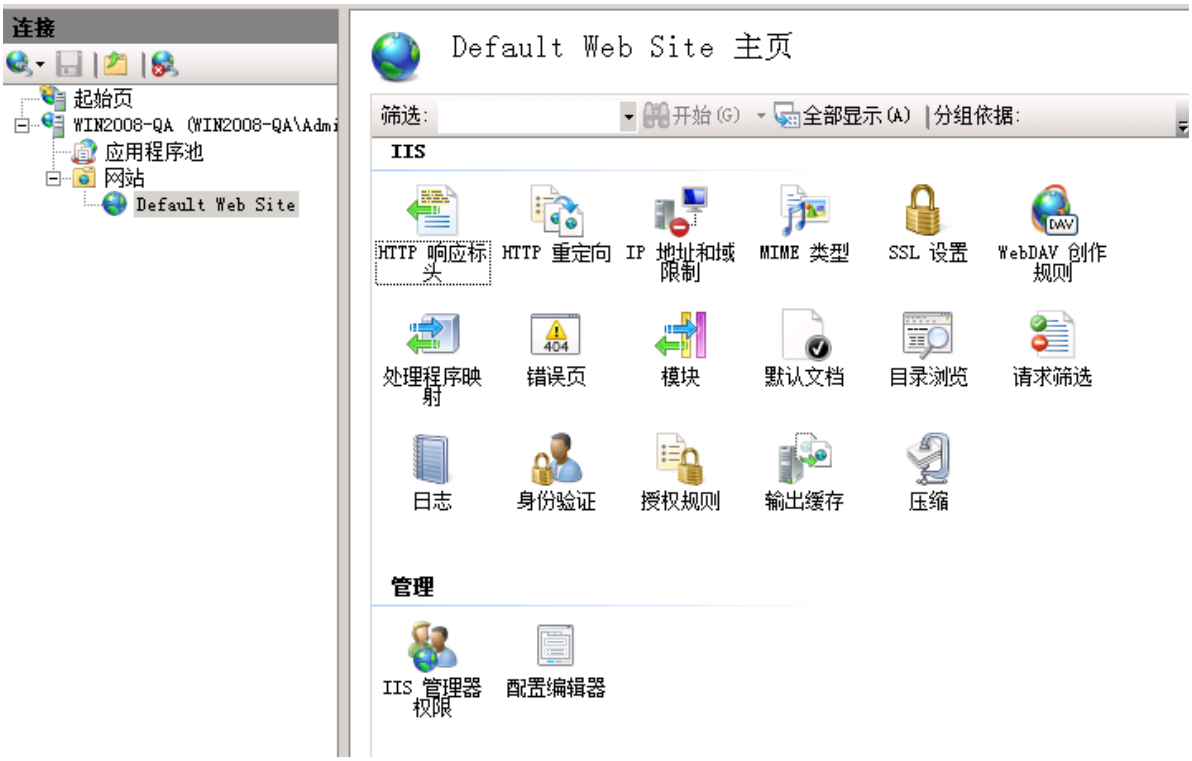


图示2-23 注册完成后的模块列表（IIS7.0）

默认情况下，在完成全局iGuard注册和加载后，“网站”下的所有的虚拟主机也会继承iGuard防护，无需再单个配置。

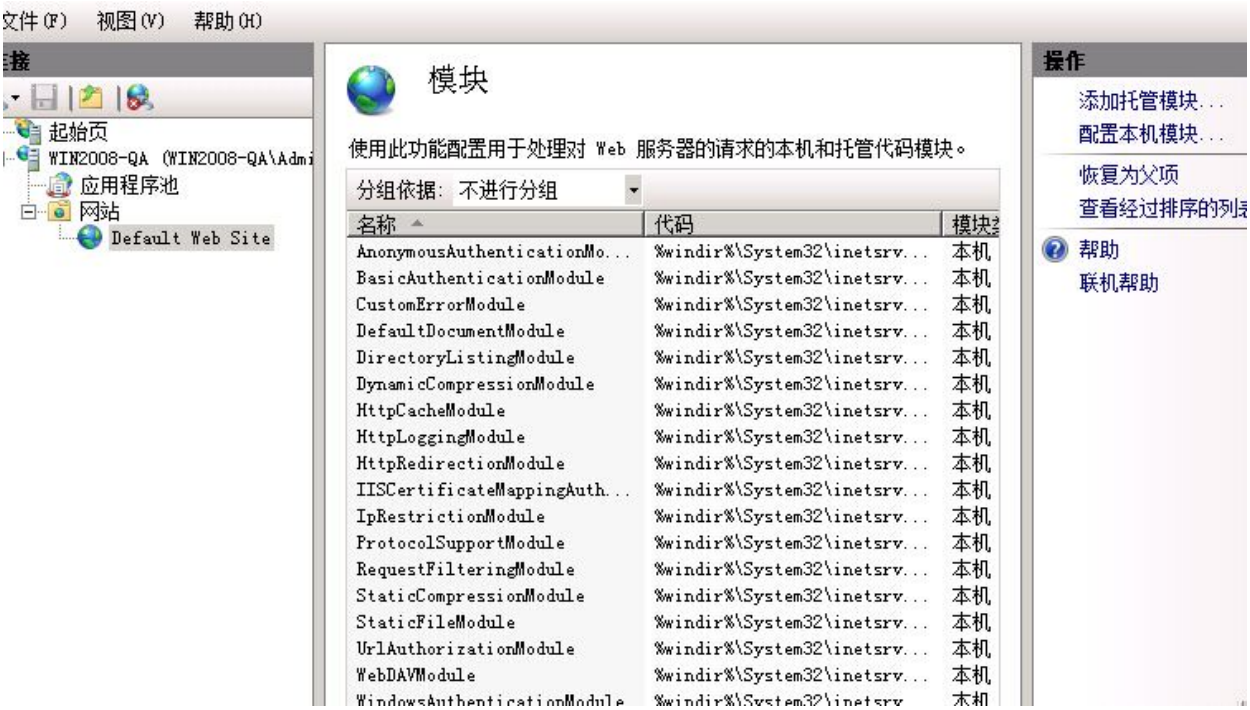
3）但也有部分使用场景，仍然需要对单个虚拟主机设置加载iGuard模块。通常而言，是该虚拟主机曾经删除过iGuard模块，其后又重新加载，才会需要执行以下步骤。

首先点击主窗体下需要加载模块的虚拟主机（如“Default Web Site”），显示该主机的配置主页（图示2-24）。



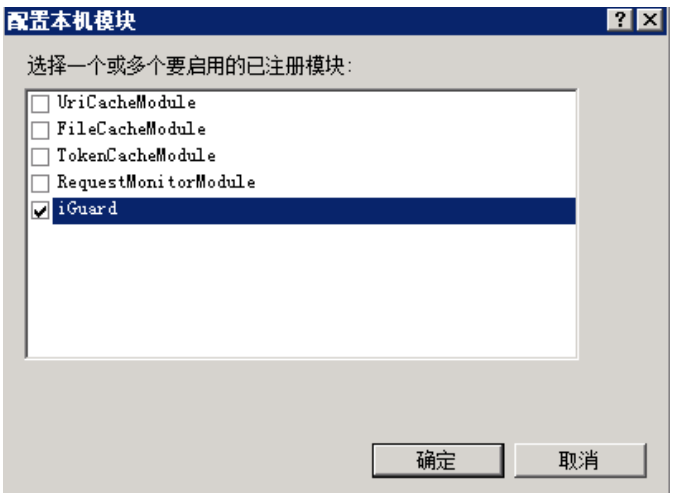
图示2-24 单个虚拟主机的配置主页（IIS7.0）

再点击其中的“模块”功能，确认在当前模块列表中没有iGuard模块（图示2-25）。



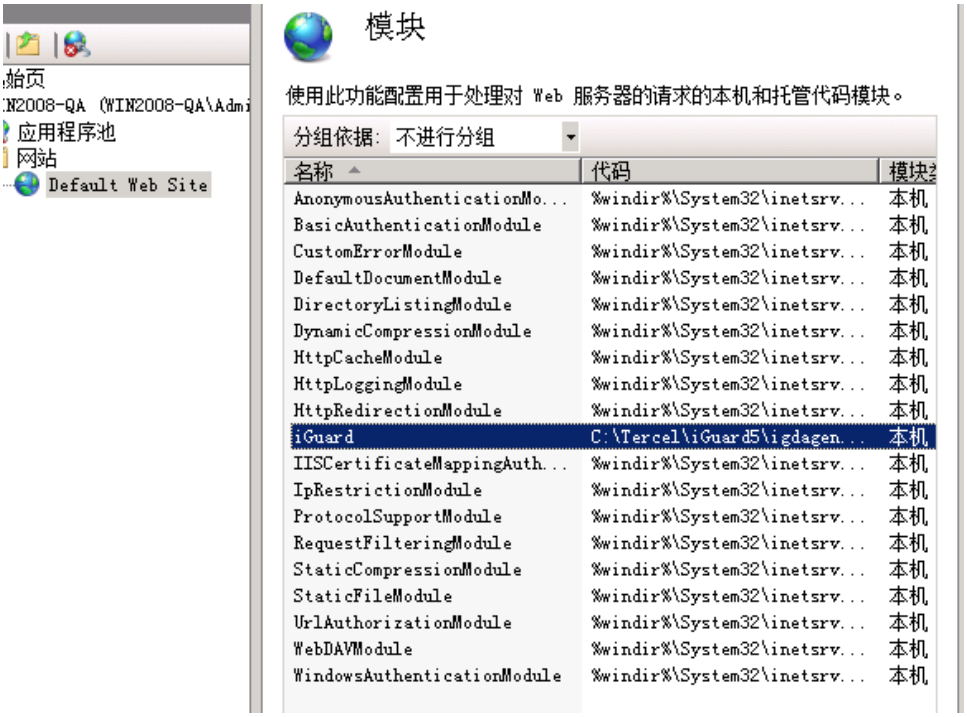
图示2-25 单个虚拟主机的模块列表（IIS7.0）

点击右侧的“配置本机模块”。在显示的当前模块列表中，核选“iGuard”模块一项（图示2-26）。



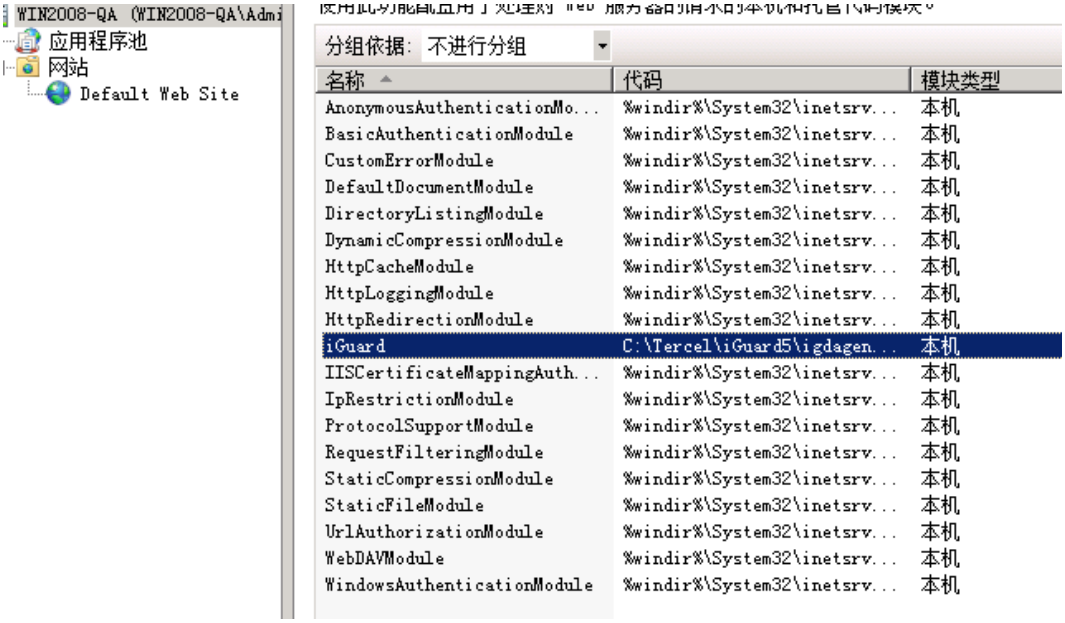
图示2-26 单个虚拟主机的iGuard模块配置（IIS7.0）

最后点击“确定”退出。确认在当前虚拟主机“Default Web Site”的模块列表中，出现“iGuard”（图示2-27）。



图示2-27 单个虚拟主机的模块列表（IIS7.0）

最后可能需要重启IIS，以使模块生效：右击IIS顶级主机名（如“WIN2008-QA”），选择右侧“重新启动”（图示2-28）。



图示2-28 重启IIS（IIS7.0）

2.3.3 Windows Apache 核心内嵌

- 加载本模块前，请先确认已经为网站目录文件做过初始化，详见【3.4.4 水印签发 】章节。
- 如果需要对特定的文件/目录做特殊处理，如不需要进行防护，请提前做好设置，具体步骤参见【4.3.4对核心内嵌模块，放开对特定文件/目录的防护】章节。

在上述两步已完成的基础上，再进行以下配置。

1） 首先确认所使用Apache的正确版本。执行以下命令（此处举例假设Apache安装在D:\appservers\Apache24目录下，请根据实际使用情况修改）：

```
cmd
D:
cd D:\appservers\Apache24\bin
D:\appservers\Apache24\bin>httpd.exe -V
```

得到以下输出内容：

```
Server version: Apache/2.4.12 (Win32)
Apache Lounge VC11 Server built:   Jan 28 2015 16:48:40
Server's Module Magic Number: 20120211:41
Server loaded:  APR 1.5.1, APR-UTIL 1.5.4
Compiled using: APR 1.5.1, APR-UTIL 1.5.4
Architecture:   32-bit
Server MPM: WinNT
  threaded: yes (fixed thread count)
  forked: no
```

在【Server version】一项写着"2.4.12"，在【Architecture】一项写着32-bit，说明应该选用32位的2.4版本模块。

2） 编辑Apache的配置文件httpd.conf，根据Apache的不同版本，在文本的最后加入以下两行。这2行根据不同的 Apache版本(2.2 vs 2.4，32位vs 64位)会有细微的差异，请根据步骤1，确认正确的版本。

- Apache 2.2 32位：

```
LoadModule ap2x_iguard5_module C:/Tercel/iGuard5/igdagent/modules/ap22/mod_ap22_iguard5.so
LoadiGuardConfigFile C:/Tercel/iGuard5/igdagent/modules/ap22/mod_iguard5.conf
```

- Apache 2.2 64位：

```
LoadModule ap2x_iguard5_module C:/Tercel/iGuard5/igdagent/modules/ap22_64/mod_ap22_iguard5.so
LoadiGuardConfigFile C:/Tercel/iGuard5/igdagent/modules/ap22_64/mod_iguard5.conf
```

- Apache 2.4 32位：

```
LoadModule ap2x_iguard5_module C:/Tercel/iGuard5/igdagent/modules/ap24/mod_ap24_iguard5.so
LoadiGuardConfigFile C:/Tercel/iGuard5/igdagent/modules/ap24/mod_iguard5.conf
```

- Apache 2.4 64位：

```
LoadModule ap2x_iguard5_module C:/Tercel/iGuard5/igdagent/modules/ap24_64/mod_ap24_iguard5.so
LoadiGuardConfigFile C:/Tercel/iGuard5/igdagent/modules/ap24_64/mod_iguard5.conf
```

3）最后重启Apache服务。

2.3.4 Windows Java中间件

- 加载本模块前，请先确认已经为网站目录文件做过初始化，详见【3.4.4 水印签发 】章节。
- 如果需要对特定的文件/目录做特殊处理，如不需要进行防护，请提前做好设置，具体步骤参见【4.3.4对核心内嵌模块，放开对特定文件/目录的防护】章节。

在上述两步已完成的基础上，再进行以下配置。

1）确定中间件所用JDK的正确版本：

注意： 要选择32位还是64位的JAVA JNI库文件，取决于当前中间件程序使用的JDK版本是哪种。确定JDK版本的步骤为，在“开始”菜单的“运行”里，输入“cmd”，返回命令行状态。再继续输入(以下示例假设JDK安装路径为D:\jdk1.7，请根据实际情况修改)：

```
cd D:\jdk1.7\bin
java –version
```

得到的输出信息为：

```
java version "1.7.0_67"
Java(TM) SE Runtime Environment (build 1.7.0_67-b01)
Java HotSpot(TM) 64-Bit Server VM (build 24.65-b04, mixed mode)
```

如上执行结果则为64位（中间显示“**64-bit**”信息），否则为32位。根据不同的平台信息，选择不同的JNI库文件：

- 32位版本JDK时，需要的库文件为安装目录下的：“modules\jee\igx5_jni.dll”和“modules\jee\libigx5.dll”；
- 64位版本JDK时，需要的库文件为安装目录下的：“modules\jee_64\igx5_jni.dll”和“modules\jee_64\libigx5.dll”。

2) 把步骤1中确立的JNI库文件放到Java的java.library.path路径下。要确定java.library.path路径的位置，可以新建一个testpath.jsp文件，内部为以下代码：

```
<%
out.println(System.getProperty("java.library.path"));
%>
```

再通过浏览器访问http://主机IP:主机端口/目录/testpath.jsp，获得如下内容：

```
D:\jdk1.7\bin;C:\WINDOWS\Sun\Java\bin;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\system32;C:\WINDOWS;……
```

如上结果时，则可以把igx5_jni.dll、libigx5.dll两个文件放到其中任一目录下，如D:\jdk1.7\bin。

在某些比较干净的系统里，可能还需要Visual Studio2010实时库文件msvcr100.dll的支持，所以还需要相应地把msvcr100.dll一起复制到特定目录下。

3）再把相应的中间件过滤器类文件（modules\jee\iguardfilter5.jar）添加到中间件服务器的CLASSPATH路径中。对于不同的Java应用服务器，这步操作各不相同，具体可参见各产品的技术文档。以下是常见中间件产品中的做法。

- Tomcat 6、7、8系列：修改%Tomcat_HOME%/conf/catalina.properties配置文件里的

> **shared.loader=**

改为

> **shared.loader="C:/Tercel/iGuard5/igdagent/modules/jee/iguardfilter5.jar"**

- WebLogic系列：编辑WebLogic启动目录下（如：C:\bea\weblogic92\samples\domains\wl_server\bin）的setDomainEnv.cmd文件，把类似以下这句：

> **set PRE_CLASSPATH=C:\bea\weblogic92\samples\server\examples\build\serverclasses**

修改为：

> **set PRE_CLASSPATH=C:\bea\weblogic92\samples\server\examples\build\serverclasses;C:\Tercel\iGuard5\igdagent\modules\jee\iguardfilter5.jar**

4）然后备份原Web应用配置文件web.xml为web.xml.bak，备份完成后，在web.xml文件内加入以下内容。这段内容在web.xml里的位置请参阅官方文档中【filter和filter-mapping】两部分在全局中的相对位置： http://docs.oracle.com/cd/E12839_01/web.1111/e13712/

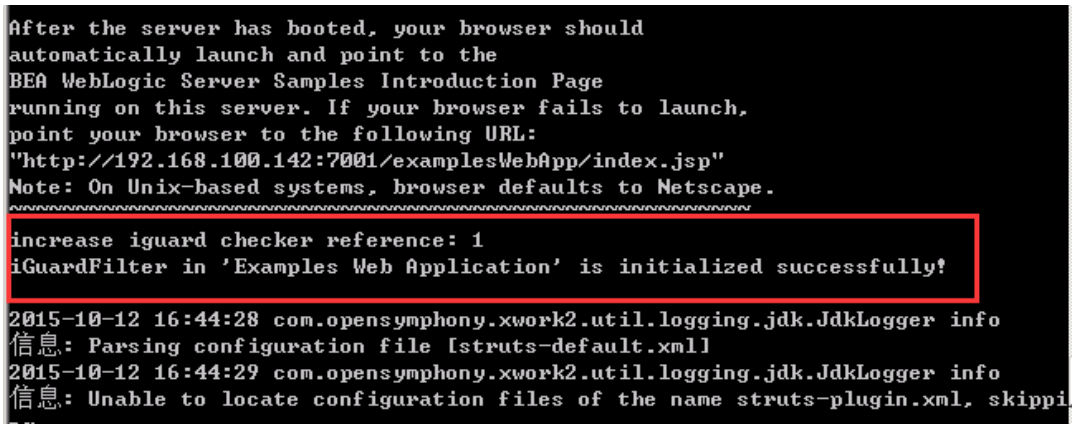
> **web_xml.htm**

```
<filter>
<filter-name>iGuard Filter</filter-name>
<filter-class>cn.com.tcxa.iguard5.IguardFilter</filter-class>
<init-param>
<param-name>iguardConf</param-name>
```

```
<!-- 如果Java为64位，以下路径最好改为 C:/Tercel/iGuard5/igdagent/modules/jee_64/mod_iguard5.conf -->
<param-value>C:/Tercel/iGuard5/igdagent/modules/jee/mod_iguard5.conf</param-value>
</init-param>
<init-param>
<param-name>debug</param-name>
<param-value>false</param-value>
</init-param>
</filter>

<filter-mapping>
<filter-name>iGuard Filter</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>
```

5）最后，需要彻底重启中间件服务。重启过程中，观察启动日志，当看到类似以下信息，则为iGuard启动成功的标志。



图示2-29 iGuard在Java中间件中启动成功的标志

2.3.5 网络校验方式

从iGuardV5版本开始，本地模块和网络校验模块合并为同一个文件，只靠配置文件确定以哪种方式工作。

网络校验方式往往用在多台前端Web服务器共享同一个NAS存储分区的情况下。如果不是这个网络环境，通常不需要使用这种部署模式。

在网络校验模式下，多台Web服务器中，必须选择其中一台安装同步服务器igdagent服务，在同步服务igdagent安装过程中，必须选择【安装网络校验服务模块】，安装完成后，在系统服务里，会增加一个名为【iwmsvc】的服务，该服务对应的默认端口为18999。除了这一台Web服务器外，其他的Web服务器都无需安装这个【网络校验服务】。

在这台安装了【网络校验服务】的网站上，模块的安装为常规方式，配置文件完全无需更改。但除了这一台特殊的机器之外，其他的几套Web服务器，则需要选择以网络校验的方式安装，需要更改mod_iguard5.conf配置文件。

这些特殊服务器上的mod_iguard5.conf中的合适位置，新增以下内容：

```
{
 ...
"Mode":"net",
"CheckServer": {
"Address":$address,
"Port":$port
},
...
}
```

其中$address为安装了【网络校验服务】那台机器的IP地址，而$port为【网络校验服务】端口，如18999。所以完整的mod_iguard5.conf可能如下：

```
{
  "interrupt_action":"block",
  "interrupt_status_code":403,
  "interrupt_content_type":"text/html",
  "interrupt_info":"<html>403 Access Denied.</html>",

  "filter":[
  ],

  "ServerRoot":"C:/Tercel/iGuard5/igdagent",
  "cache":{
  "width":"",
  "height":"",
  "ttl":""
  },

  "Mode":"net",
  "CheckServer": {
  "Address":"192.168.100.9",
  "Port":18999
  },

  "name":"Apache22-x86",
  "type":"AP22",
  "desc":"Apache22的32位防护模块"
}
```

具体每种Web服务器的加载和配置方式，则与常规无异，参考上述章节即可。

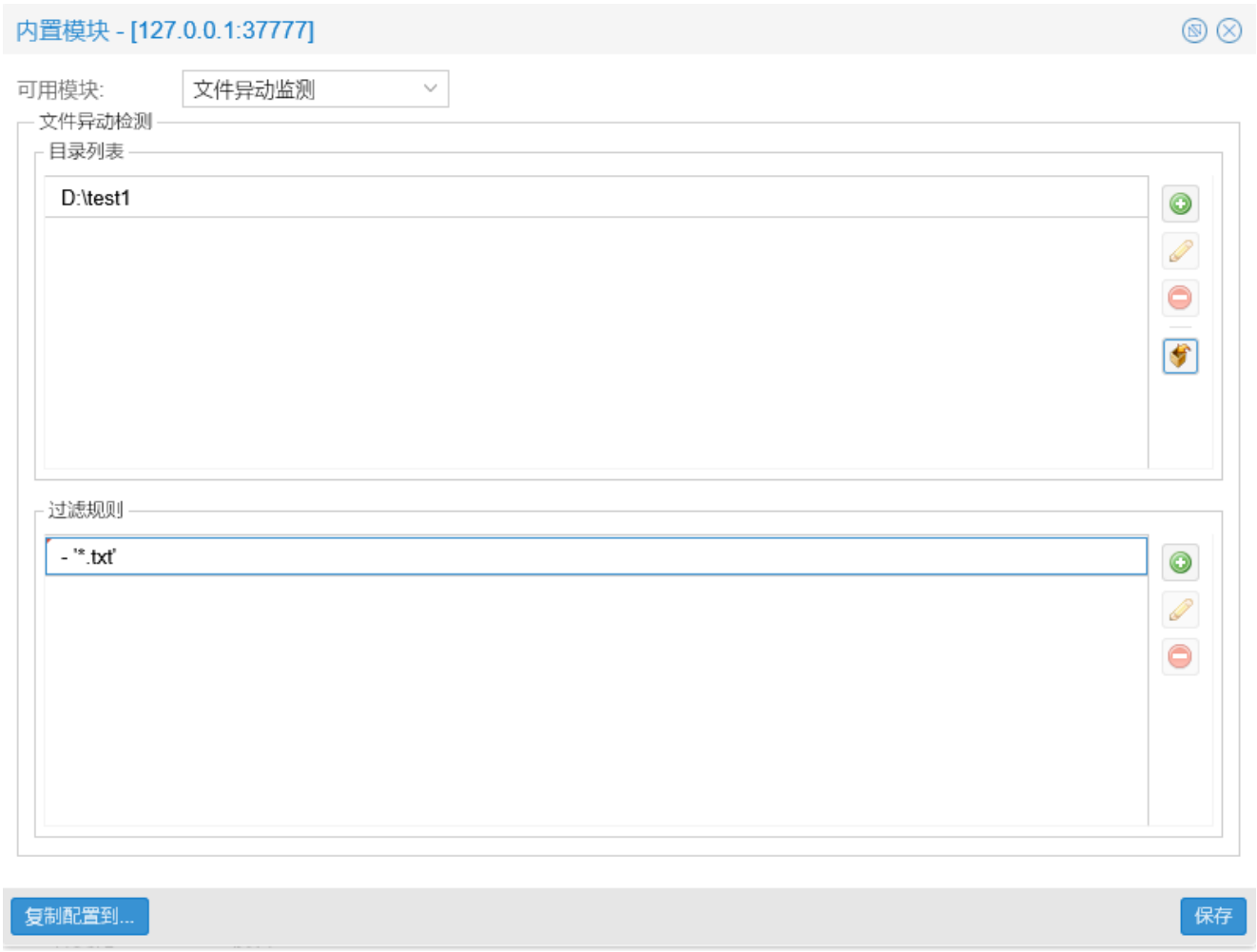
2.3.6 文件异动检测

在Windows 2008 R2以上平台里，iGuardV5支持主动发现非法的文件修改操作，并实时地从备份端恢复源文件。以下为这种部署方式的大致描述：

1）正常地部署发布和同步服务器。在发布控制台上，新增一个站点，配置该站点对应的源目录和目标目录（必须步骤），关联相应的同步服务器，确认发布服务器和同步服务器网络上联通。和以上各种模块类似，先初始化水印，详见【3.4.4 水印签发 】章节。

2）完成以上步骤后，点击桌面上的“防护状态”，再选择需要配置的服务器对应【操作】列里的“内置模块”，在可用模块下拉列表里，选择“文件异动检测”。在目录列表框，选择“从站点中导入”按钮

，把前面“路径映射”中设定的“目标目录”自动导入为防护目录。也可以不使用“导入”功能，而是手工指定需要防护的目录。确定后点击【保存】。



图示2-30 文件异动检测

自动导入的目录列表实际上就是站点配置中目标目录。

- 目录列表：需要监视文件异常变化的目录列表，可以点击【导入】按钮从关联站点的映射路径获取；
- 文件过滤：监视过程中需要排除的文件或目录；包含（+）即需要对满足条件的文件实时监控，排除（-）即不需要对满足条件的文件实时防护，默认值为在目录列表中的所有文件都受到实时防护。

注意1：这种防护方式依赖于fcnotify文件驱动。在不确定的情况下，请在网站服务器端以管理员权限执行 fltmc ，查看系统是否已加载fcnotify驱动。如果没有，可能需要执行C:\Tercel\iGuard5\igdagent\filter\install_driver.bat 重新安装一下该驱动程序。

注意2：如果配置完成并保存后，该功能并不生效，需要在网站服务器端手工重启Web服务器上的【fcagent服务】。

2.3.7 仅监控文件变化

在某些部署环境中，可能仅需要监控和记录网页目录的异常文件变动（该功能针对的往往是用户产生的数据，如上传目录），而无需做其他额外处理。以下为这种部署方式的大致描述：

1） 正常地部署发布和同步服务器。在发布控制台上，新增一个站点，该站点**未必需要设置源目录和目标目录**，仅需要关联某台同步服务器的IP地址即可。确认发布服务器和同步服务器网络上联通。

2） 在同步服务器端，编辑监控配置文件C:\Tercel\iGuard5\igdagent\conf\filewatch.conf（此为默认路径，以实际情况为准）。该文件为json格式，注意不要破坏文件格式：

```
{
  "watch":["C:\\inetpub\\wwwroot\\uploads","C:\\tomcat\\webapps"],
  "process_filter":["+ '*\\httpd.exe'",
                    "+ '*\\w3wp.exe'",
                    "+ '*\\java.exe'",
                    "- '*'"],
  "file_filter":["*"]
}
```

- "watch" 开头的一行，为需要监控的目录，可以写多项，每个目录的前后需要加双引号，每两个目录项之间以逗号“,”分隔；
- "process_filter" 的部分为需要监控的进程名，可以使用通配符。前面有 "+"加号的进程，为需要监控的进程，前面为"-"减号的进程，为无需监控的进程。如上例子中所写，则只需要监控 httpd.exe、w3wp.exe和java.exe三个进程对 "C:\inetpub\wwwroot\uploads" 和 "C:\tomcat\webapps" 两目录的写操作，其他进程（以*符号代表）的写操作，则一律忽略。如果需要监控所有的进程，则写为：* "+ '*' "
- "file_filter" 为需要监控的文件模式，一般写 "* "即可。

3） 按照以上步骤调整 C:\Tercel\iGuard5\igdagent\conf\filewatch.conf 配置文件后，还需要到“系统工具”->“服务”中，重启名为**【fefilter】**的文件监控服务，使设置生效；

4） 以后如果设定的目录下有非法文件改动，具体的动作、用户名、进程信息等将详细记录在fefilter-yyyymmdd.log 文件中；

5）在发布服务器的Web控制台上，也可以看到相应的报警信息。

6）以上报警仅记录，没有其他处理。

7) 以上fefilter-yyyymmdd.log日志和控制台上的报警，实际上都是由C:\Tercel\iGuard5\igdagent\plugin\lua\alert.lua脚本实现的。如果有其他延伸需求，可以从这个接口再做二次开发。

注意1：这种防护方式依赖于fcnotify文件驱动。在不确定的情况下，请在网站服务器端以管理员权限执行 fltmc ，查看系统里是否已加载fcnotify驱动。如果没有，可能需要以管理员权限，手工执行C:\Tercel\iGuard5\igdagent\filter\install_driver.bat 重新安装一下该驱动程序。

注意2：如果配置完成并保存后，该功能并不生效，需要在网站服务器端手工重启Web服务器上的【fefilter 服务】。

2.4 防护方式 Linux

2.4.1 文件水印初始化

在加载各核心内嵌模块之前，需要对保护的网站目录进行初始化，初始化的过程就是扫描整个网站保护目录，对所有文件添加水印的过程。在初始化之前，请先确认当前网站没有被非法添加网页木马， 没有隐藏后门，否则一旦经过初始化阶段，这些有问题的文件也会被认定为合法文件了。

如果需要检查网站是否包含网页后门，请查阅【5.2 检查网页木马/Linux】章节

在做文件水印初始化之前，**一定要先做好站点的路径映射和服务器关联**，否则无法在控制台上做水印初始化。

水印初始化的具体步骤请见【3.4.4 水印签发 】章节。

在少量特殊情况下，也可以使用命令行方式批量签发水印。方法：

- 编辑”同步服务器安装目录“/wmktool.conf 配置文件，把其中的 dirs 段，改为需要做水印初始化的目录；如果有多个目录，需要用逗号分隔，每个目录的两边用双引号括起来；目录分隔符要使用正斜杠”/“：

```
{"ServerRoot":"/usr/local/iguard5/igdagent",
"filter":[
""
],
"dirs":[
"/usr/local/apache2/htdocs","/usr/local/apache24/htdocs"
]
}
```

- cd 到同步服务器安装目录，执行以下命令，可以对wmktool.conf里指定的目录执行水印初始化：

> **./run-wmktool.sh -f wmktool.conf**

- 如果需要查询某个特定文件的水印值是否正常，可以执行：

> **./run-wmktool.sh -f wmktool.conf -c verify ”需要校验的文件名“**

如果返回码为0，则校验通过；如果返回码为110，则校验失败。

2.4.2 Linux/Unix Apache 核心内嵌

- 加载本模块前，请先确认已经为网站目录文件做过初始化，详见【3.4.4 水印签发 】章节。
- 如果需要对特定的文件/目录做特殊处理，如不需要进行防护，请提前做好设置，具体步骤参见【4.3.4对核心内嵌模块，放开对特定文件/目录的防护】章节。

在上述两步已完成的基础上，再进行以下配置。

1） 首先确认所使用Apache的正确版本。执行以下命令（此处举例假设Apache安装在/usr/local/apache2目录下，请根据实际使用情况修改）：

> **# cd /usr/local/apache2/bin**
> **# ./apachectl -V**

得到以下输出内容：

```
Server version: Apache/2.2.31 (Unix)
Server built:   Jan 29 2016 12:24:38
Server's Module Magic Number: 20051115:40
Server loaded:  APR 1.5.2, APR-Util 1.5.4
Compiled using: APR 1.5.2, APR-Util 1.5.4
Architecture:   64-bit
Server MPM: Prefork
threaded: no
forked: yes (variable process count)
Server compiled with....
```

在【Server version】一项写着"2.2.31"，在【Architecture】一项写着64-bit，说明应该选用64位的2.2版本模块。

编辑Apache的配置文件httpd.conf，根据Apache的不同版本，在文本的最后加入以下两行。这2行根据不同的 Apache版本(2.0、2.2或2.4)会有细微的差异。

- Apache 2.0：

> **LoadModule ap2x_iguard5_module /usr/local/iguard5/igdagent/modules/ap2/mod_ap2_iguard5.so**
>
> **LoadiGuardConfigFile /usr/local/iguard5/igdagent/modules/ap2/mod_iguard5.conf**

- Apache 2.2：

> **LoadModule ap2x_iguard5_module /usr/local/iguard5/igdagent/modules/ap22/mod_ap22_iguard5.so**
> **LoadiGuardConfigFile /usr/local/iguard5/igdagent/modules/ap22/mod_iguard5.conf**

- Apache 2.4：

> **LoadModule ap2x_iguard5_module /usr/local/iguard5/igdagent/modules/ap24/mod_ap24_iguard5.so**
> **LoadiGuardConfigFile /usr/local/iguard5/igdagent/modules/ap24/mod_iguard5.conf**

创建和修改alert报警文件的权限，执行以下命令：

> **# cd /usr/local/iguard5/igdagent/alert**
> **# touch alert.log**
> **# chmod 664 alert.***

最后重启Apache服务。

> **# cd /usr/local/apache2/bin**
> **# ./apachectl restart**

2.4.3 Linux/Unix Java中间件核心内嵌

- 加载本模块前，请先确认已经为网站目录文件做过初始化，详见【3.4.4 水印签发 】章节。
- 如果需要对特定的文件/目录做特殊处理，如不需要进行防护，请提前做好设置，具体步骤参见【4.3.4对核心内嵌模块，放开对特定文件/目录的防护】章节。

在上述两步已完成的基础上，再进行以下配置。

1）确认当前中间件使用的JDK版本。方法为执行以下命令（以下执行结果为举例，请以实际环境为准）：

> **# ps -ef |grep java**

如下执行结果为64位（中间显示“64-bit”信息），否则为32位。

```
java version "1.7.0_09-icedtea"
OpenJDK Runtime Environment (rhel-2.3.4.1.el6_3-x86_64)
OpenJDK 64-Bit Server VM (build 23.2-b09, mixed mode)
```

根据实际情况， 把对应版本的JNI库文件放到Java的java.library.path路径下。

- JNI 库文件为安装目录里的 “modules/jee/libigx5_jni.so”；

要确定JNI库文件的位置，可以新建一个testpath.jsp文件，内部为以下代码：

```
<%
out.println(System.getProperty("java.library.path"));
%>
```

再通过浏览器访问http://主机IP:主机端口/目录/testpath.jsp，获得以下内容：

```
/usr/java/packages/lib/amd64:/usr/lib64:/lib64:/lib:/usr/lib ……
```

如上结果时，则可以把上述modules/jee/libigx5_jni.so 文件放到其中任一目录下，如/usr/lib64。

2）再把相应的中间件过滤器类文件（modules/jee/iguardfilter5.jar）添加到中间件服务器的CLASSPATH路径中。而对于不同的Java应用服务器，这步操作各不相同，具体可参见各产品的技术文档。以下是常见中间件产品中的做法。

- Tomcat 6、7、8系列：修改%Tomcat_HOME%/conf/catalina.properties配置文件里的

> **shared.loader=**

改为

> **shared.loader="/usr/local/iguard5/igdagent/modules/jee/iguardfilter5.jar"**

- WebLogic系列：编辑WebLogic启动目录下的setDomainEnv.sh文件，加入以下2行：

> **IGUARD_PATH="/usr/local/iguard5/igdagent/modules/jee/iguardfilter.jar"**
> **export IGUARD_PATH**

把原来的这一行：

> **CLASSPATH="${PRE_CLASSPATH} ..... "**

修改为：

> **CLASSPATH="${PRE_CLASSPATH} ..... ${IGUARD_PATH}"**

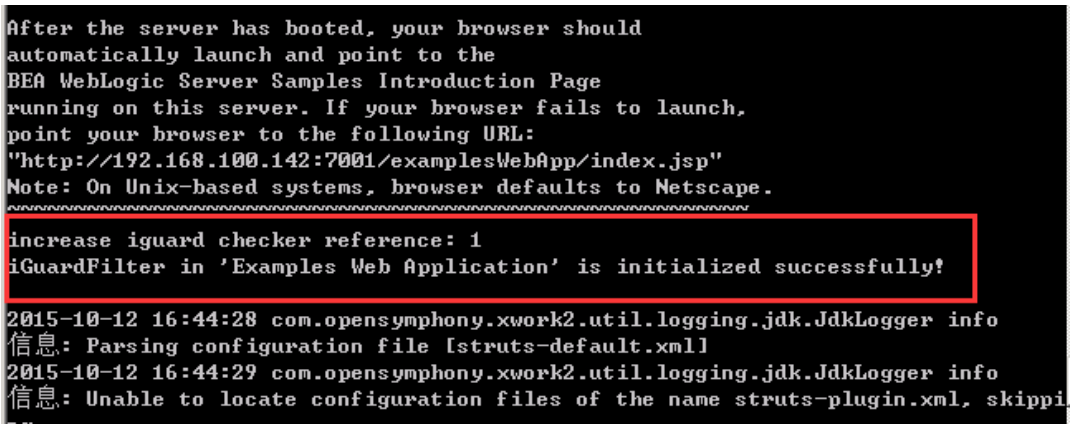
3）然后备份原Web应用配置文件web.xml为web.xml.bak，备份完成后，在web.xml文件内加入以下内容。这段内容在web.xml里的位置请参阅官方文档中【filter和filter-mapping】两部分在全局中的相对位置： http://docs.oracle.com/cd/E12839_01/web.1111/e13712/

> **web_xml.htm**

```
<filter>
<filter-name>iGuard Filter</filter-name>
<filter-class>cn.com.tcxa.iguard5.IguardFilter</filter-class>
<init-param>
<param-name>iguardConf</param-name>
<param-value>/usr/local/iguard5/igdagent/modules/jee/mod_iguard5.conf
</param-value>
</init-param>
<init-param>
<param-name>debug</param-name>
<param-value>false</param-value>
</filter>
<filter-mapping>
<filter-name>iGuard Filter</filter-name>
<url-pattern>/*</url-pattern>
```

```
16  </filter-mapping>
```

最后，需要彻底重启中间件服务。重启过程中，观察启动日志，当看到类似以下信息，则为iGuard启动成功的标志。



图示2-29 iGuard在Java中间件中启动成功的标志

2.4.4 Linux/Unix Nginx

由于Nginx的结构限制，不能动态加载模块，所以必须重新编译一次Nginx。在编译新的Nginx之前，一定要做好原Nginx程序和配置文件（nginx.conf）的备份。

1）首先获得原Nginx的编译参数：由于要重新编译Nginx，加入iGuard模块，编译时最好能和原Nginx模块和功能保持一致，否则原来的配置文件可能没法使用。

```
# cd /usr/local/nginx
# bin/nginx -V
```

获得原来的编译参数可能如下（以下仅为举例）：

```
1  configure arguments: --prefix=/usr/local/nginx --with-select_module --with-poll_module --with-http_flv_module --with-
   http_gzip_static_module --without-http_ssi_module --without-http_auth_basic_module --without-http_geo_module --without-
   http_map_module --without-http_referer_module --without-http_proxy_module --without-http_fastcgi_module --without-
   http_uwsgi_module --without-http_scgi_module --without-http_upstream_ip_hash_module --without-mail_pop3_module --without-
   mail_imap_module --without-mail_smtp_module --with-pcre=/tmp/pcre-8.40
```

2）备份Nginx安装目录/sbin/nginx执行文件和conf/nginx.conf配置文件：

```
# cd /usr/local/nginx
# cp sbin/nginx sbin/nginx.orig
# cp conf/nginx.conf conf/nginx.conf.orig
```

3）从以下网址下载Nginx加载器的源代码 nginx-iguardloader-V5.tgz： http://app.tcxa.com.cn/bbs/viewtopic.php?f=42&t=1337

4）把 nginx-iguardloader-V5.tgz 上传到Nginx服务器所在的机器，并执行解压，解压后目录为iguardloader：

```
# tar xzvf nginx-iguardloader-V5.tgz
```

5）重新下载同一个版本的Nginx连同上述Nginx iGuard加载器进行编译，方法是在复制原有的编译参数基础上，再加入一句”--add-module=/tmp/iguardloader“ （假设Nginx源代码解压在 /tmp/nginx-1.13.0目录下，iguardloader解压在 /tmp/iguardloader）：

```
# cd /tmp/nginx-1.13.0
# ./configure --prefix=/usr/local/nginx --with-select_module --with-poll_module --with-http_flv_module --with-
http_gzip_static_module --without-http_ssi_module --without-http_auth_basic_module --without-http_geo_module --
without-http_map_module --without-http_referer_module --without-http_proxy_module --without-http_fastcgi_module -
-without-http_uwsgi_module --without-http_scgi_module --without-http_upstream_ip_hash_module --without-
mail_pop3_module --without-mail_imap_module --without-mail_smtp_module --with-pcre=/tmp/pcre-8.40 --add-
module=/tmp/iguardloader
```

6）新的Nginx编译完成后，在原来的"nginx安装目录/sbin"目录下，会生成一个新的nginx可执行文件，原nginx已备份为nginx.bak

7）编辑"nginx安装目录/conf/nginx.conf"配置文件，在其中http{... ...}段内，加入以下配置（或参考igdagent/modules/nginx/nginx.conf模板里的路径写法）

```
load_iguard /usr/local/iguard5/igdagent/modules/libigx5/libigx5.so
/usr/local/iguard5/igdagent/modules/nginx/mod_iguard5.conf;
enable_iguard on;
```

注意：在重新启动Nginx，使以上配置生效前，也需要先根据【3.4.4 水印签发 】章节的内容，对文件做一次初始化。

2.4.5 网络校验方式

从iGuardV5版本开始，本地模块和网络校验模块合并为同一个文件，只靠配置文件确定以哪种方式工作。

网络校验方式往往用在多台前端Web服务器共享同一个NAS存储分区的情况下。如果不是这个网络环境，通常不需要使用这种部署模式。

在网络校验模式下，多台Web服务器中，必须选择其中一台安装同步服务器igdagent服务，在同步服务igdagent安装过程中，必须选择【安装网络校验服务模块】，该服务的默认端口为18999。除了这一台Web服务器外，其他的Web服务器都无需安装这个【网络校验服务】。

在这台安装了【网络校验服务】的网站上，模块的安装为常规方式，配置文件完全无需更改。但除了这一台特殊的机器之外，其他的几套Web服务器，则需要选择以网络校验的方式安装，需要更改mod_iguard5.conf配置文件。

这些特殊服务器上的mod_iguard5.conf中的合适位置，新增以下内容：

```
{
 ...
"Mode":"net",
"CheckServer": {
"Address":$address,
"Port":$port
},
...
}
```

其中$address为安装了【网络校验服务】那台机器的IP地址，而$port为【网络校验服务】端口，如18999。所以完整的mod_iguard5.conf可能如下：

```
{
  "interrupt_action":"block",
  "interrupt_status_code":403,
  "interrupt_content_type":"text/html",
  "interrupt_info":"<html>403 Access Denied.</html>",

  "filter":[
  ],

  "ServerRoot":"/usr/local/iguard5/igdagent",
  "cache":{
  "width":"",
  "height":"",
  "ttl":""
  },

  "Mode":"net",
  "CheckServer": {
  "Address":"192.168.100.9",
```

```
  "Port":18999
  },

  "name":"Apache22-x86",
  "type":"AP22",
  "desc":"Apache22的32位防护模块"
}
```

具体每种Web服务器的加载和配置方式，则与常规无异，参考上述章节即可。

注意：安装Linux版同步服务器时，虽然安装包里已经打包了网络校验中心的程序，但执行./install.sh安装脚本时，并没有把该程序安装到默认目录下。如果需要，可以在解压目录下手工复制 iwmsvc 可执行和 iwmsvc.conf.tmpl 配置文件。这部分的操作待完善。

2.4.6 Linux iLocker 拦截模式

iLocker为核心内嵌防护模式之外的独立防护模式，它通过对**"用户账号"-"进程"-"进程参数"-"动作"-"文件模式"**的细粒度灵活组合设置，控制文件的产生。达到既不影响网站的正常应用，又具备严密防护的效果。它可以和iGuard同步、iGuard核心内嵌完美地整合使用。

iLocker的独立手册请参见：http://www.tcxa.com.cn/ilocker/linux/help/ 。对此手册的精简提炼如下：

- iLocker 的配置文件为安装目录下的conf/ilocker.conf ，在其中每条规则或命令占一行配置；
- 每条规则的指令包括：`uid, exe_path, cmdline,operation,file_path, action, ignore_case`，规则里的每项含义详见原手册：http://www.tcxa.com.cn/ilocker/linux/help/#header-n93
- 规则里经常用到的配置项为action，它包括三种文件处理动作：pass、deny和log。它设定对符合前面组合的条件的进程，会执行哪种事件处理：pass 会完全放行，不做处理；deny 会拦截，既该文件写操作被直接拒绝；log 会记录该文件操作但不拦截；
- iLocker 在作为网站服务器的防护方式时，默认使用的设备为 /dev/ilocker0；iLocker 作为发布服务器的文件变化监控时，默认使用的设备为 /dev/ilocker1 ；
- Linux iLocker 分1.0和2.0版本，两者配置文件格式不一样，无法兼容。以下描述仅适用于iLocker2.0。

以下为 iLocker2.0 搭配iGuardV5.5标准版使用，作为网页防护手段时，iLocker的安装步骤和配置建议：

1）获得iLocker 2.0 安装程序。根据实际文件名解压安装文件，再把解压目录下的文件，全部复制到iGuard同步目录下。具体步骤如下（实际文件名可能有差异）：

```
# tar xzvf ilocker2.0_20180607.tar.gz # cd ilocker
# cp -rf * /usr/local/iguard5/igdagent
```

此时，在/usr/local/iguard5/igdagent目录下应该有bin、doc和lib等子目录，在bin目录下应有如下文件：

```
# ls -l /usr/local/iguard5/igdagent/bin

-rwxr-xr-x. 1 root root 8269 May 19 14:42 ilocker
-rwxr-xr-x. 1 root root 812 May 19 14:42 ilocker_conf_loader.py
-rwxr-xr-x. 1 root root 89 May 19 14:42 ilockerconsole
-rwxr-xr-x. 1 root root 5636 May 19 14:42 ilocker_log_reader.py
-rwxr-xr-x. 1 root root 1379 May 19 14:42 ilocker-test.sh
```

2）配置 /usr/local/iguard5/igdagent/conf/ilocker.conf文件，假设存放网页文件的目录在 /var/www/html，需要使用iGuard同步服务器做更新，此外的其他操作都被视为非法行为。该配置文件的内容建议为：

```
#ilocker.conf建议配置，以下设置对/var/www/html/目录放行同步服务器的进程，但拦截其他所有进程的写操作
exe_path=/usr/local/iguard5/igdagent/igdagent,file_path=/var/www/html/*,action=pass
file_path=/var/www/html/*,action=deny
```

从iLocker2.0开始，需要使用许可文件，才有文件实时拦截功能。除了上述文件目录配置外，还需要更新ilocker.conf里的许可证信息，修改以下相应指令：

```
lic_name=ilocker测试[试用]
lic_code=TMGWC-7RYFT-D8XPJ-RGYXM-D9CTV
```

3）挑选合适的 iLocker 内核模块：cd 到lib子目录，根据系统的`uname -an`结果，选择合适的so模块，复制为ilocker.ko。如（可对比`uname`返回结果和`cp`命令里复制的文件名）：

> **# uname -an Linux localhost.localdomain 2.6.32-279.el6.x86_64 #1 SMP Wed Jun 13 18:24:36 EDT 2012 x86_64 x86_64 x86_64 GNU/Linux**
> **cd lib**
> **ls**
> **cp ilocker\@2.6.32-279.el6.x86_64\@x86_64\@rhel6.3\@.ko ilocker.ko**

4）启动iLocker防护，执行以下命令（这句命令必须以root权限执行！）：

> **# /usr/local/iguard5/igdagent/bin/ilocker -g start**

查看iLocker状态：

> **# /usr/local/iguard5/igdagent/bin/ilocker status**

重新加载iLocker

> **# /usr/local/iguard5/igdagent/bin/ilocker -g reload**

停止iLocker防护

> **# /usr/local/iguard5/igdagent/bin/ilocker stop**

5）把启动命令行加入自启动文件，如/etc/rc.local中，写入：

```
/usr/local/iguard5/igdagent/bin/ilocker -g start
```

6）按以上步骤设置和启动iLocker防护后，/var/www/html 目录将只能由iGuard同步服务器执行写入操作，其他写操作将一律被直接拒绝并记录。关于iLocker更详细的配置，请参阅 http://www.tcxa.com.cn/ilocker/linux/help/； 关于iLocker 用于发布端的文件变化监控，请参阅：【2.1.2.6 文件监控模式二：iLocker模式 】

2.4.7 Linux iLocker 自动恢复

iLocker还可以配合iGuardV5.5的报警机制，实现被改后主动发现和恢复的效果。步骤如下：

1）获得iLocker安装程序。根据实际文件名解压安装文件，再把解压目录下的文件，全部复制到iGuard同步目录下。具体步骤如下（实际文件名可能有差异）：

> **# tar xzvf ilocker-20170518.tar.gz**
> **# cd ilocker**
> **# cp -rf * /usr/local/iguard5/igdagent**

此时，在/usr/local/iguard5/igdagent目录下应该有bin、doc和lib等子目录，在bin目录下应有如下文件：

> **# ls -l /usr/local/iguard5/igdagent/bin**
>
> **-rwxr-xr-x. 1 root root 8269 May 19 14:42 ilocker**
> **-rwxr-xr-x. 1 root root 812 May 19 14:42 ilocker_conf_loader.py**
> **-rwxr-xr-x. 1 root root 89 May 19 14:42 ilockerconsole**
> **-rwxr-xr-x. 1 root root 5636 May 19 14:42 ilocker_log_reader.py**
> **-rwxr-xr-x. 1 root root 1379 May 19 14:42 ilocker-test.sh**

2）配置 /usr/local/iguard5/igdagent/conf/ilocker.conf文件，假设存放网页文件的目录在 /var/www/html，需要使用iGuard同步服务器做更新，此外的其他操作都被视为非法行为。该配置文件的内容建议为：

```
#ilocker.conf建议配置，请特别注意第二行的动作为log，而非上一节中的deny。这一行的动作里写log是仅记录不拦截模式
exe_path=/usr/local/iguard5/igdagent/igdagent,file_path=/var/www/html/*,action=pass
file_path=/var/www/html/*,action=log
```

3）挑选合适的 iLocker 内核模块：cd 到lib子目录，根据系统的`uname -an`结果，选择合适的so模块，复制为ilocker.ko。如（可对比`uname`返回结果和`cp`命令里复制的文件名）：

> **# uname -an Linux localhost.localdomain 2.6.32-279.el6.x86_64 #1 SMP Wed Jun 13 18:24:36 EDT 2012 x86_64 x86_64 x86_64 GNU/Linux**
> **cd lib**
> **ls**
> **cp ilocker\@2.6.32-279.el6.x86_64\@x86_64\@rhel6.3\@.ko ilocker.ko**

4）启动iLocker防护，执行以下命令（这句命令必须以root权限执行！同时一定要包含-g参数。）：

> **# /usr/local/iguard5/igdagent/bin/ilocker -g start**

5）把启动命令行加入自启动文件，如/etc/rc.local中，写入：

```
/usr/local/iguard5/igdagent/bin/ilocker -g start
```

6）把/usr/local/iguard5/igdagent/igdagent/plugin/lua 目录下的 _alert.lua 文件，重命名为 alert.lua，并重启同步服务，具体步骤如下：

> **# cd /usr/local/iguard5/igdagent/plugin/lua**
> **# mv _alert.lua alert.lua**
> **# cd /usr/local/iguard5/igdagent/igdagent**
> **# ./admtool stop**
> **# ./admtool start**

按以上步骤设置和启动iLocker防护后，/var/www/html 目录将只能由iGuard同步服务器执行写入操作，如果有其他进程进行写操作，iGuard会从源端重新恢复该文件。被改后的文件，也会备份到igdagent/backup目录下。

第三章 管理中心

3.1 访问管理中心

iGuard V5.5提供基于https协议的Web管理中心，支持Internet Explorer 8.0及以上版本 / Chrome / Firefox等浏览器。
访问iGuard V5.5管理中心的步骤如下：

1. 在管理计算机的浏览器地址栏输入https://**$man_ip**:**$man_port**，其中：
    - $man_ip：管理中心的IP地址，应替换成实际的IP地址；
    - $man_port：默认是39999，可以在配置文件中进行修改。
2. 显示登录页面，输入正确的用户名和密码即可进入系统（图示3-1-1）。iGuard V5.5管理中心出厂时内置用户的登录信息为：

- 用户名：admin
- 密码：iguard

图示3-1-1 登录页面

1. 显示管理中心主页面，分为管理、功能（开始）和快捷模式（界面）三个区域（图示3-1-2）。

图示3-1-2 管理中心主页面

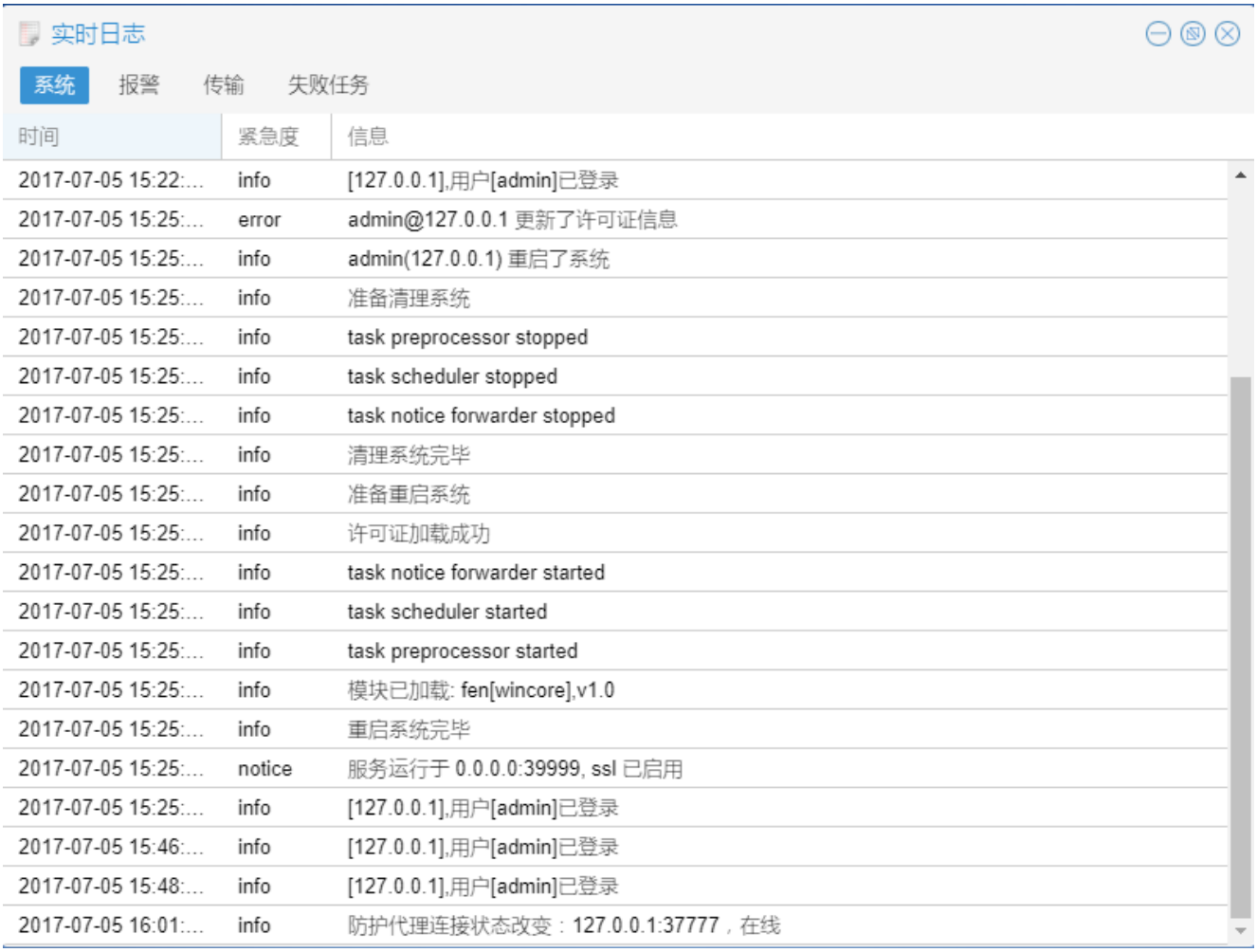
- 管理区域：当前登录用户进行管理操作的区域，包括
  【实时日志】：查看当前实施日志；
  【任务状态】：查看当前任务，任务处理动态和任务统计情况；

【防护状态】：查看当前防护代理服务器的工作状态；
【控制面板】：系统辅助功能设置，如邮件通知、文件传输和双机发布等功能。

- 功能区域：包括管理中心所有功能操作的菜单项列表，可以点击相应的菜单项进入。
- 快捷模式（界面）：点击图标快速查看实时日志、任务状态和系统防护状态等。

3.2 实时日志

点击界面【实时日志】快捷图标，页面显示当前的系统信息记录列表（图示3-2-1）。



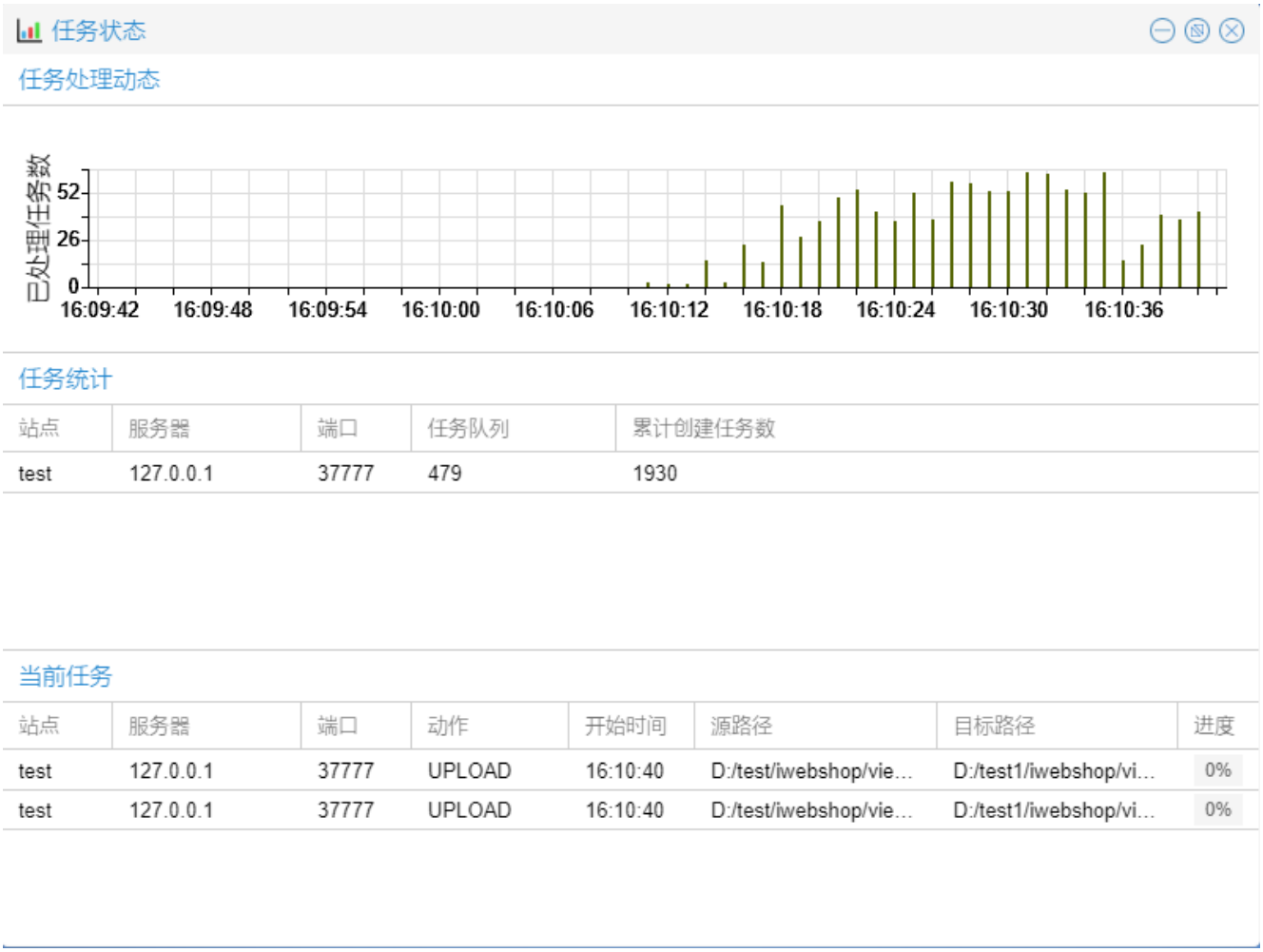
图示3-2-1 实时日志

在各个Tab页面中查看的系统信息包括：

- 系统记录：显示当前系统各功能项的日志记录。希望查看系统运行是否正常时，查看这一类别的日志；
- 报警记录：显示当前检测到的篡改行为的记录。希望查看前端监控的系统是否有报警，是否有攻击行为时，查看这一类别日志；
- 传输记录：显示当前文件同步传输的任务记录。希望确认文件传输状态时，查看这一类别日志；
- 失败任务记录：显示当前文件同步传输失败的任务记录。

3.3 任务状态

点击界面【任务状态】快捷图标，页面显示所有站点的文件同步传输任务状态（图示3-3-1）。



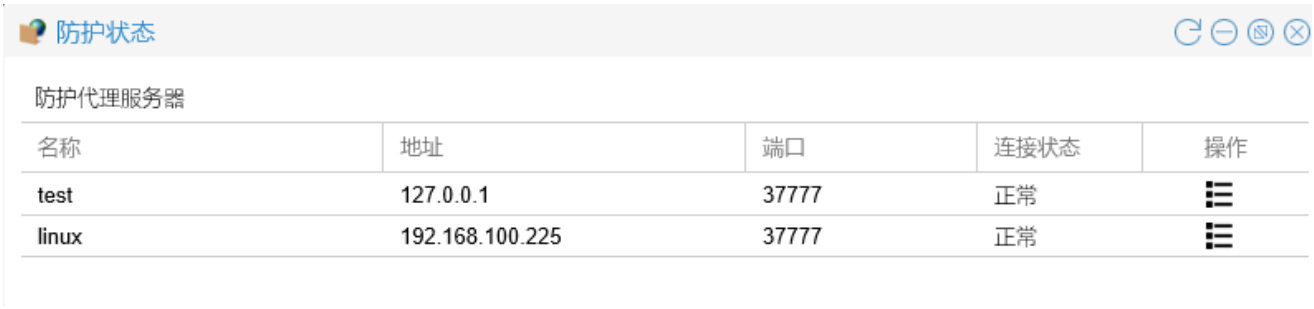
图示 3-3-1 任务状态—按站点

可以查看的状态信息包括：

- 任务处理处理动态：主要是某个时间段文件处理任务数。
- 任务统计，主要包括以下信息：
  - 站点：显示站点的名称；
  - 服务器：显示站点所关联的服务器列表；
  - 端口：显示关联服务器所对应的连接端口；
  - 任务队列：显示当前正在进行的文件同步传输任务详情，包括站点名称、主机名称、同步动作、时间、耗时、源/目标路径、文件大小、传输进度等；
  - 任务数：显示站点所关联的各个服务器当前正在进行的文件同步传输任务的数量。
- 当前任务，主要包括以下信息：
  - 站点：显示当前正在进行任务站点的名称；
  - 服务器：显示站点所关联的服务器列表；
  - 端口：显示关联服务器所对应的连接端口；
  - 动作：当前站点进行任务的操作，如UPLOAD，表示正在进行文件上传；
  - 开始时间：任务开始进行的时间；
  - 源路径：同步文件的源地址；
  - 目标路径：同步文件的目的地址；
  - 进度：文件同步速度。

3.4 防护状态

点击界面【防护状态】快捷退表，页面显示服务器列表，可以查看的信息包括：名称、IP、端口、连接状态、操作项等（图示3-4-1）。



图示 3-4-1 防护状态

在【操作】项里分为五个配置选项页：内置模块、WEB模块、水印签发、工具箱和系统维护。

以下为几个功能模块的解释：

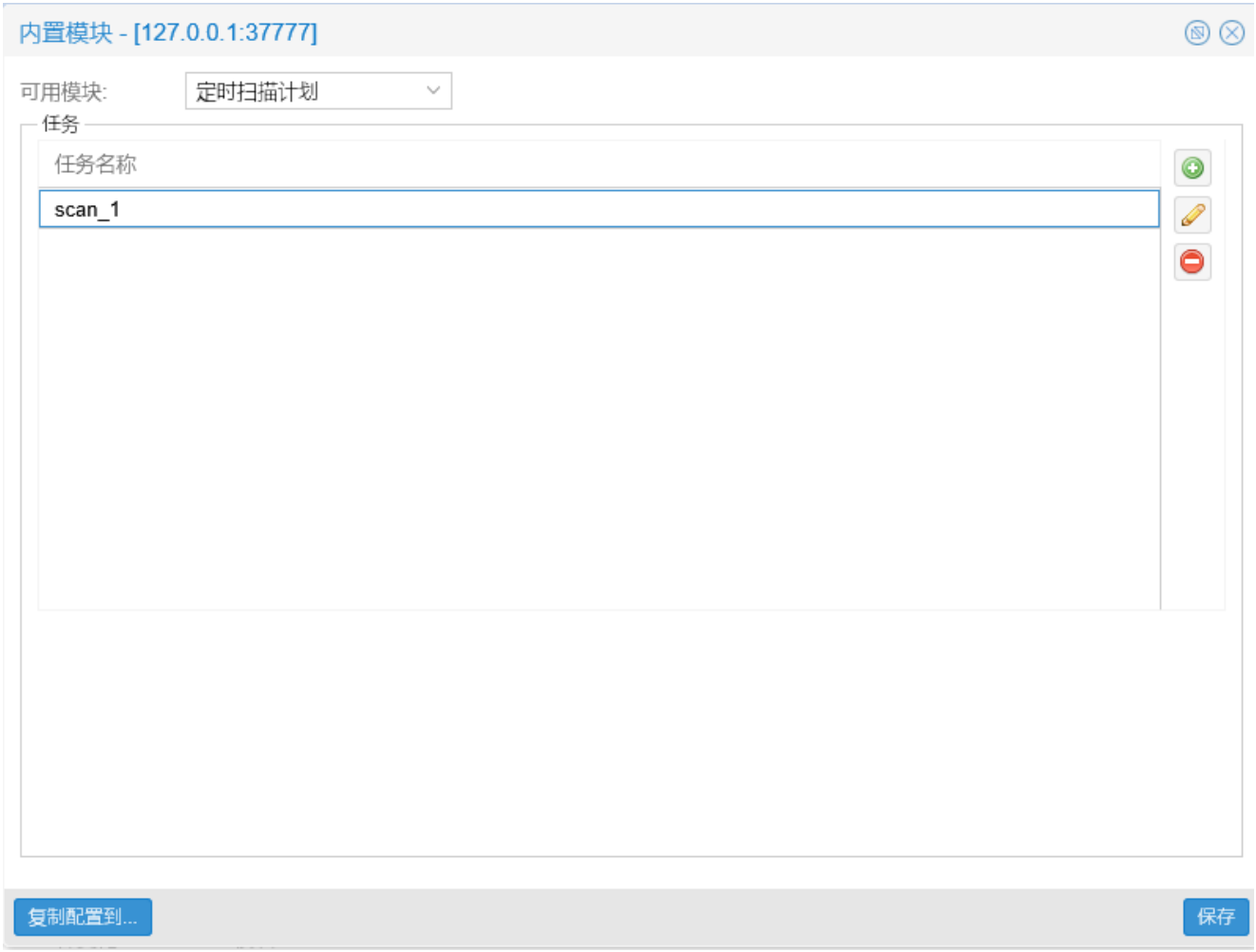
- 内置模块->定时扫描计划：定时扫描，在指定时间点对网站服务器上的受保护目录进行扫描；
- 内置模块->文件异动检测：设定网站服务器上文件变动检测的策略；
- WEB模块：核心内嵌模块，设定加载在Web服务器软件内的模块策略；
- 水印签发：远程设定网站服务器上的水印签发策略和执行；
- 工具箱：远程控制目标服务器上安装的辅助软件；
- 系统维护：在Web端远程重启目标服务器上的同步服务。

注意：防护状态内的所有功能，都必须在发布服务器和同步服务器能正常连接，许可证未过期时，才能操作！否则无法使用相应的功能。

3.4.1 内置模块 - 定时扫描计划

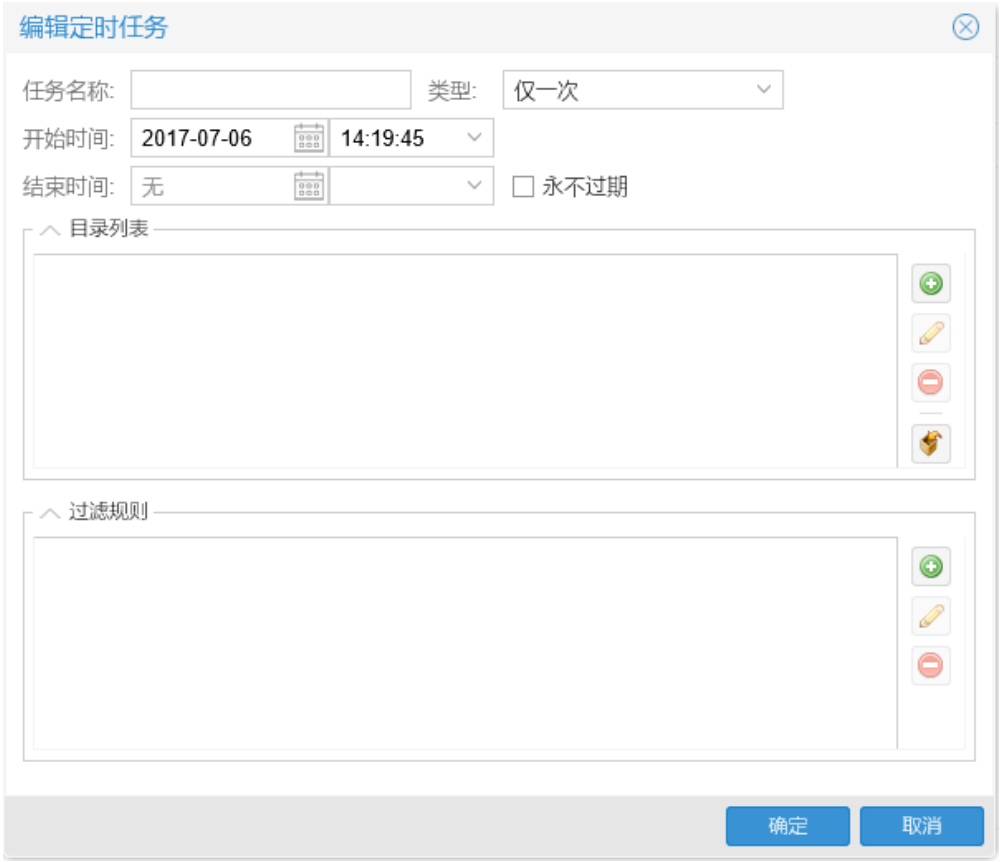
点击特定服务器对应的【操作】项 ，在【内置模块】的可用模块下拉菜单中，再选择【定时扫描计划】项。

下图显示了定时扫描的任务列表，可以点击 按钮增加任务，点击 按钮编辑任务，或点击 删除相应的扫描任务。完成后，点击【保存】扫描计划的配置（图示3-4-2）。



图示 3-4-2 定时扫描计划

点击 按钮添加新的扫描任务，弹出具体配置选项框（图示3-4-3）。



图示 3-4-3 编辑定时任务

可以进行的配置包括：

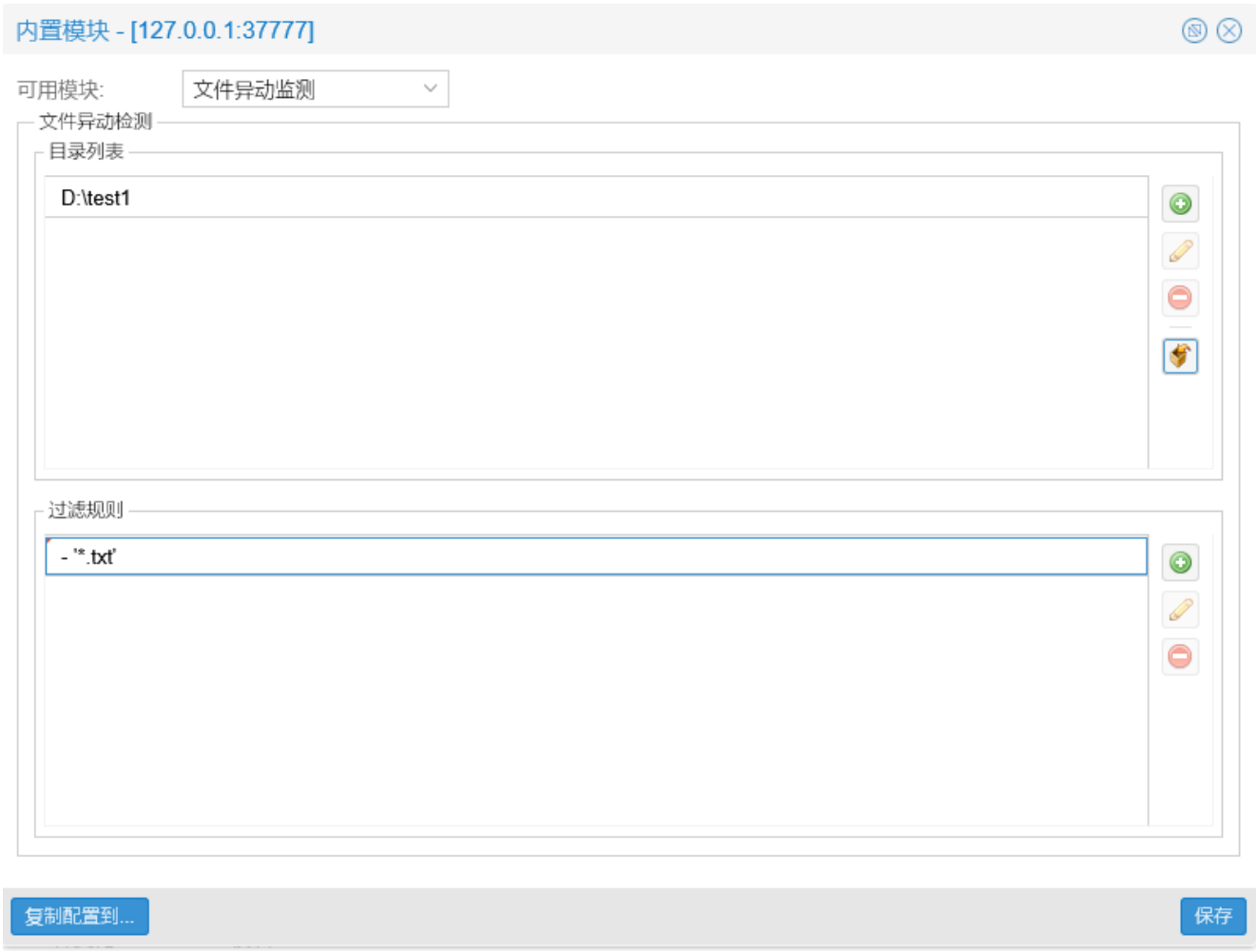
- 任务名称：扫描任务的显示名称；
- 类型：扫描频率设置，可以配置为仅一次、每天、每周、每月；
- 开始/结束时间：扫描任务的开始/结束时间；
- 永不过期：若选中，则扫描任务一直有效，无需设置结束时间；
- 目录列表：需要进行扫描的文件目录，可以点击 按钮从关联站点的映射路径获取；
- 过滤规则：扫描时需要排除的文件或目录。

如果需要把同一配置，分发到多台服务器上去，可以点击【复制配置到】按钮，选择需要配置扫描任务的目标服务器，会弹出配置选项框（图示3-4-4）。

图示 3-4-4 选择目标服务器

3.4.2 内置模块 - 文件异动检测

点击特定服务器对应的【操作】项 ，在【内置模块】的可用模块下拉菜单中，再选择【文件异动检测】项。配置界面如下：



图示 3-4-5 文件异动检测

可以配置项项目如下：

- 目录列表：需要监视文件异常变化的目录列表，可以点击 按钮从关联站点的映射路径获取；
- 过滤规则：监视过程中需要排除的文件或目录；包含（+）即需要对满足条件的文件实时监控，排除（-）即不需要对满足条件的文件实时防护，默认值为在目录列表中的所有文件都受到实时防护，然后点击【保存】按钮完成配置（图示3-4-6）

如果需要把同一配置，分发到多台服务器上去，可以点击【复制配置到】按钮选择需要配置的目标服务器。

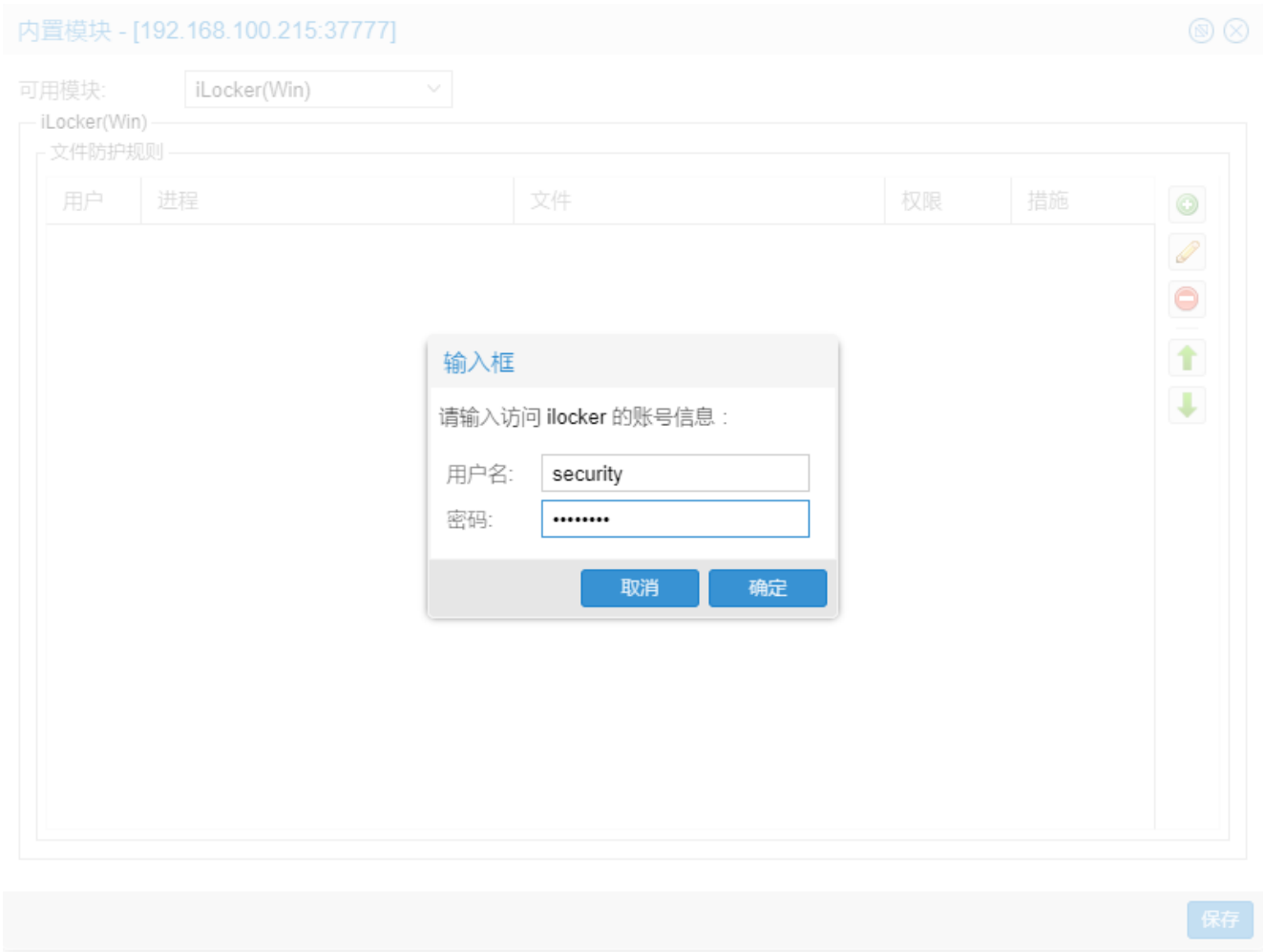
图示 3-4-6 选择目标服务器

3.4.3 内置模块 - iLocker(Win)

只有同步服务器为Windows 2008以上操作系统，并已成功安装了iLocker防护后，在【内置模块】里才能看到【iLocker(Win)】选项。如果没有该选项，需要先安装iLocker。

点击特定服务器对应的【操作】项 ，在【内置模块】的可用模块下拉菜单中选择【iLocker（Win）】选项。

首次使用时需要输入有效的用户账号，该账号为iLocker的安全组账号，默认为security，密码1234abcd。



图示 3-4-7 登录iLocker

登陆成功后，配置界面如下：

图示 3-4-8 编辑iLocker文件防护规则

点击 按钮增加防护规则，点击 按钮编辑防护规则，或点击 删除相应的防护规则。完成后，点击【保存】按钮完成配置（图示3-4-8）。

多条规则之间，按照排列的顺序确定优先级。排在前面的规则优先级更高。如果被前面的规则匹配到，后面符合的规则也自动失效。如果需要调整优先级，可点击上下按钮 ，使其符合具体的需求。

可以配置的项目如下：

- 用户名：可以填入一个具体准确的用户名，也可以用 * 做通配，代表匹配所有的用户；
- 进程路径：可以填入一个完整的进程路径，也可以用 * 做部分或全部的通配，以匹配特定模式的进程；
- 访问权限：**包括“不可改写”、“不可访问”和“完全控制”三种。**通常需要拒绝写操作的，选择“不可改写”；需要放行写操作的，选择“完全控制”；“不可访问”只有极少数场合下会使用，代表符合条件的进程，无法读取“以下文件/目录”里的内容，这个设定对功能影响较大，一般不会使用；
- 文件/目录：填入需要匹配上述规则的文件/目录模式，可以填入一个目录，如"D:\Apache2.2\htdocs"；也可以填入一个完整的文件路径，如"D:\Apache2.2\conf\httpd.conf"；也可以填入部分具有*号通配的路径模式，如 "*\uploadfile*"，自动匹配相似模式的文件；
- 违规措施：包括“记录访问日志”和“拦截访问动作”两者。这两个选项为复选的模式，可以只选择一种，也可以两种全选。如果访问权限里，已经选择“完全控制”，则这两项【违规措施】都不能选，因为此时文件就不受限制，可以直接读写了。如果只选择了“记录访问日志”，则系统不会拦截符合规律的动作，只会静默地记录其具体的操作信息。

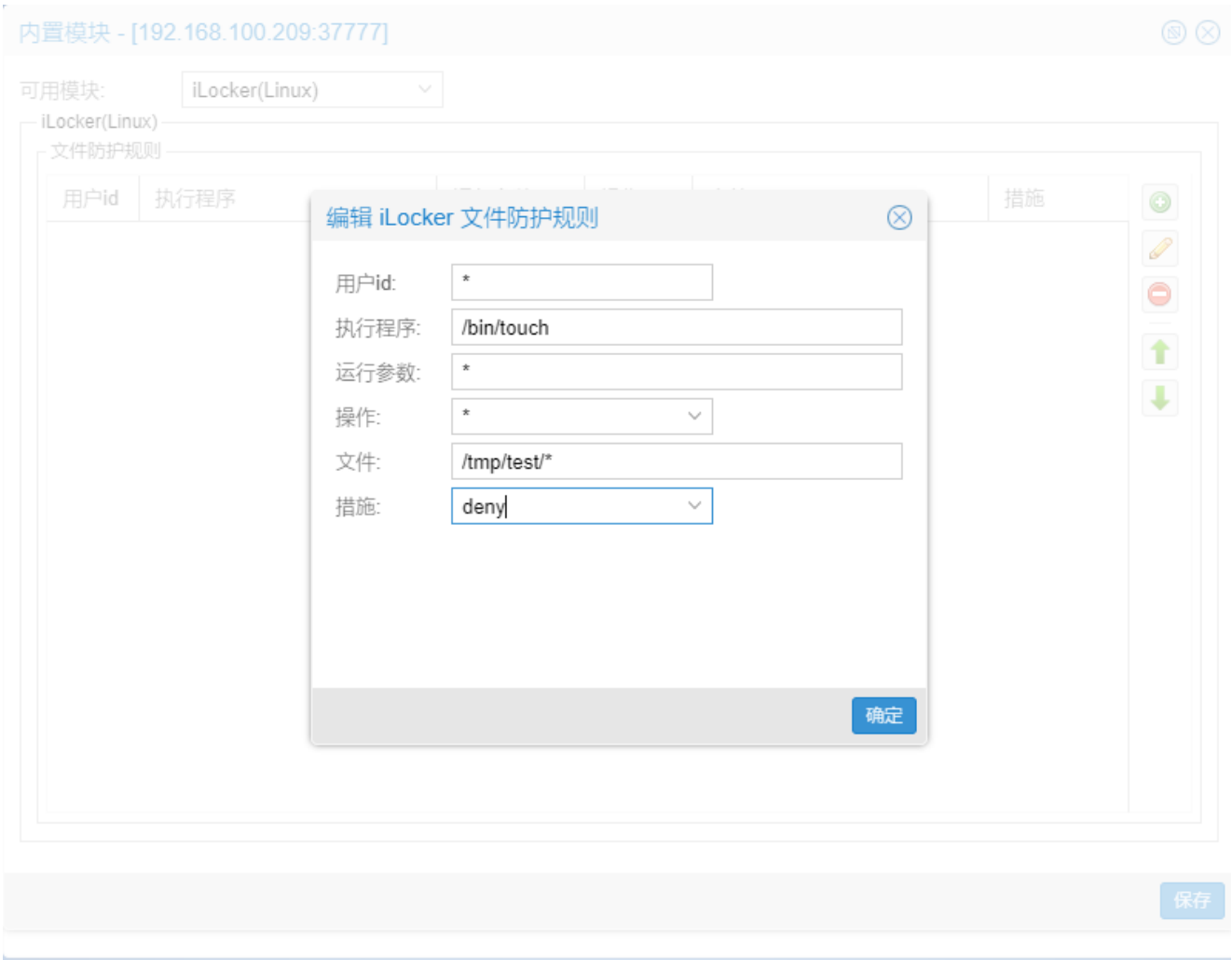
更具体配置建议参见独立的iLocker说明：http://www.tcxa.com.cn/ilocker/windows/help/ 。

3.4.4 内置模块 - iLocker(Linux)

只有同步服务器为Linux操作系统，并在igdagent目录下，安装了iLocker for linux后，此项配置才有意义。

在做此项配置之前，要确保：**iLocker Linux 已经安装在igdagent 目录下，也就是 /usr/local/iguard5/igdagent 目录下，分别有 bin、conf/ilocker.conf 和 lib/ilocker.ko 等必须的文件和目录。**

点击特定服务器对应的【操作】项 ，在【内置模块】的可用模块下拉菜单中选择【iLocker（Linux）】选项。配置界面如下：



图示 3-4-9 编辑iLocker文件防护规则

点击 按钮增加防护规则，点击 按钮编辑防护规则，或点击 删除相应的防护规则。完成后，点击【保存】按钮完成配置（图示 3-4-9）。

多条规则之间，按照排列的顺序确定优先级。排在前面的规则优先级更高。如果被前面的规则匹配到，后面符合的规则也自动失效。如果需要调整优先级，可点击上下按钮 ，使其符合具体的需求。

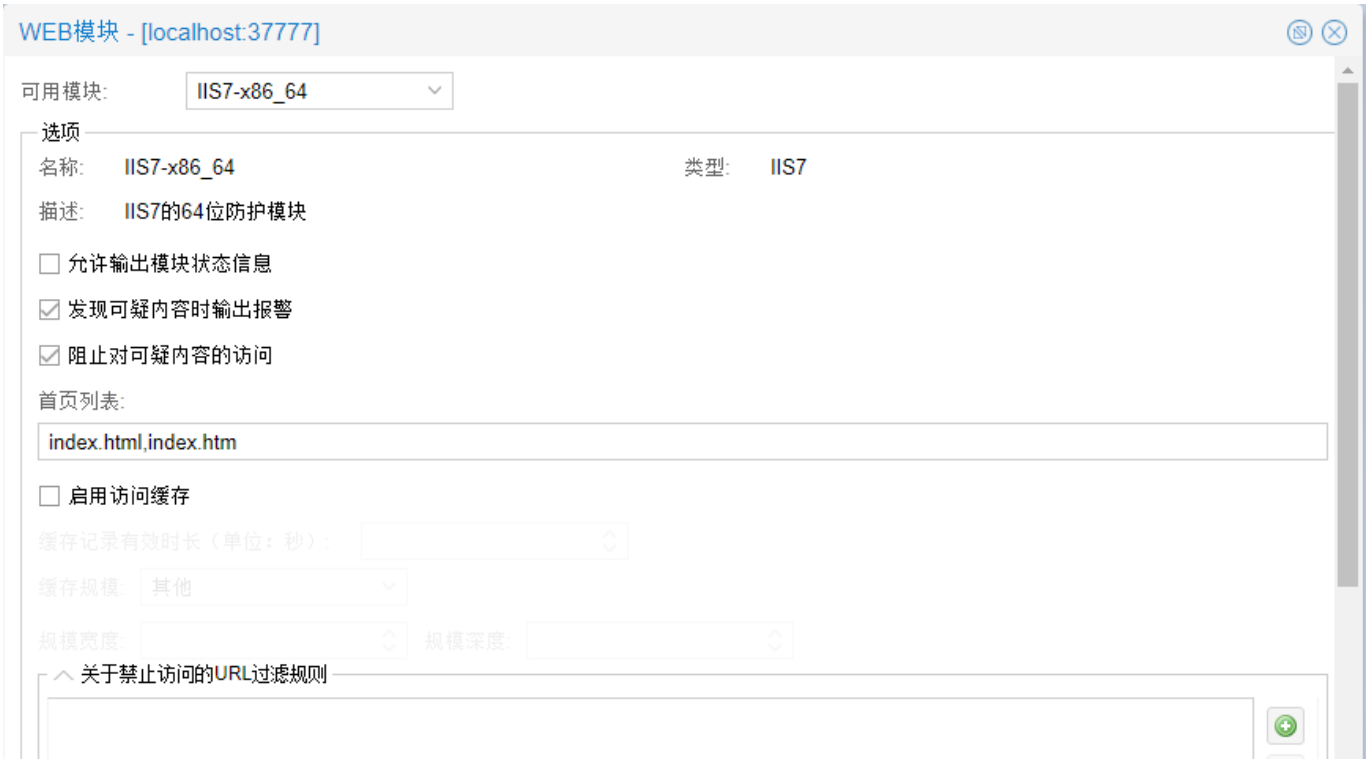
可以配置的项目如下：

- 用户id：可以填入一个具体准确的用户pid，如“500”，也可以用 " * " 做通配，代表匹配所有的用户；
- 执行程序：可以填入一个完整的进程路径，如”/bin/touch“，也可以用 * 做部分或全部的通配，如 "*/java"，以匹配特定模式的进程；
- 运行参数：是上一项【执行程序】的具体运行参数，如果不需要过细粒度的配置，直接写 " * " 即可；
- 操作：需要匹配的细粒度动作，具体的动作可以点击下拉菜单选择，如果不需要过细力度的配置，直接写 * 即可，代表匹配该进程的所有动作；
- 文件：填入需要匹配上述规则的文件/目录模式，如果需要填入一个目录，一定要在最后加入 * 通配符，如 "/var/www/html/*" ；也可以填入一个完整的文件路径，如"/usr/local/apache2/conf/httpd.conf"；也可以填入部分具有*号通配的路径模式，如 "*/uploadfiles/*"，自动匹配相似模式的文件

- 措施：可选的措施包括三种“log”、“deny”和“pass”。如果措施为“log”，则匹配上述规则的动作，仅被记录在日志里，不会拦截；措施为“deny”时，匹配上述规则的动作，不但会记录还是直接拦截阻断；如果措施为“pass”，该动作既不会被记录也不会被拦截，会直接放行。

3.4.5 WEB模块

点击特定服务器记录的操作项，在页面右侧出现的配置区域选择“WEB模块”配置选项页，可以选中需要进行远程配置的防护模块名称，在配置区域进行操作，点击【复制配置到】按钮选择需要配置的目标服务器，然后点击【保存】按钮完成WEB模块的远程配置（图示3-4-10）。



图示 3-4-10 防护模块远程配置

可以进行的配置包括：

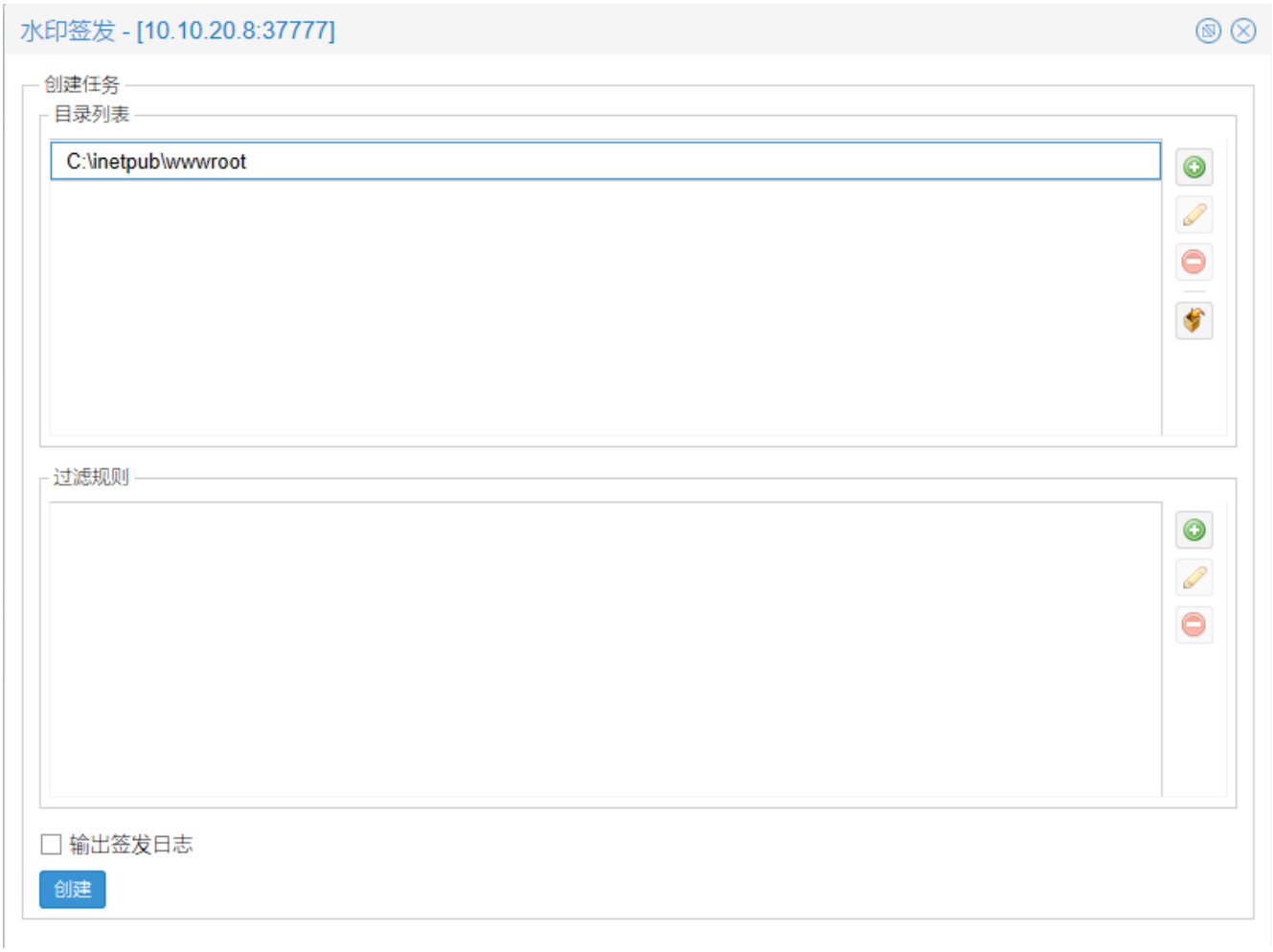
- 允许输出模块状态信息：是否允许在【防护状态】页面中显示本模块信息；
- 发现可疑内容时输出报警：默认开启
- 阻止对可疑内容的访问： 默认开启
- 拒绝URL规则：无论是否有水印，甚至未必有相应的文件或目录，本服务器就直接禁止（或允许）访问的URL列表；包含（+）即直接拒绝对该URL的访问，排除（-）即不需要拦截此URL的访问，默认值为不拒绝任何URL的访问；
- 拒绝文件规则：无论水印是否存在，在本服务器上直接禁止（或允许）访问的物理文件列表；包含（+）即直接拒绝对该文件模式的访问，排除（-）即不需要拦截此文件模式的访问，默认值为不拒绝任何文件的访问；
- 保护文件规则：本服务器需要（或不需要）检查水印的文件或目录列表；包含（+）即需要检查此文件的水印值，排除（-）即不需要检查此文件的水印值，默认值为需要检查所有文件的水印值。

点击【复制配置到】按钮可以选择需要配置WEB模块的目标服务器，会弹出配置选项框（图示3-4-11）。

图示 3-4-11 选择目标服务器

3.4.6 水印签发

点击特定服务器记录的操作项，在页面右侧出现的配置区域选择“水印签发”配置选项页。在配置界面里根据实际情况填入，完成后，点击【创建】按钮（图示3-4-12）。

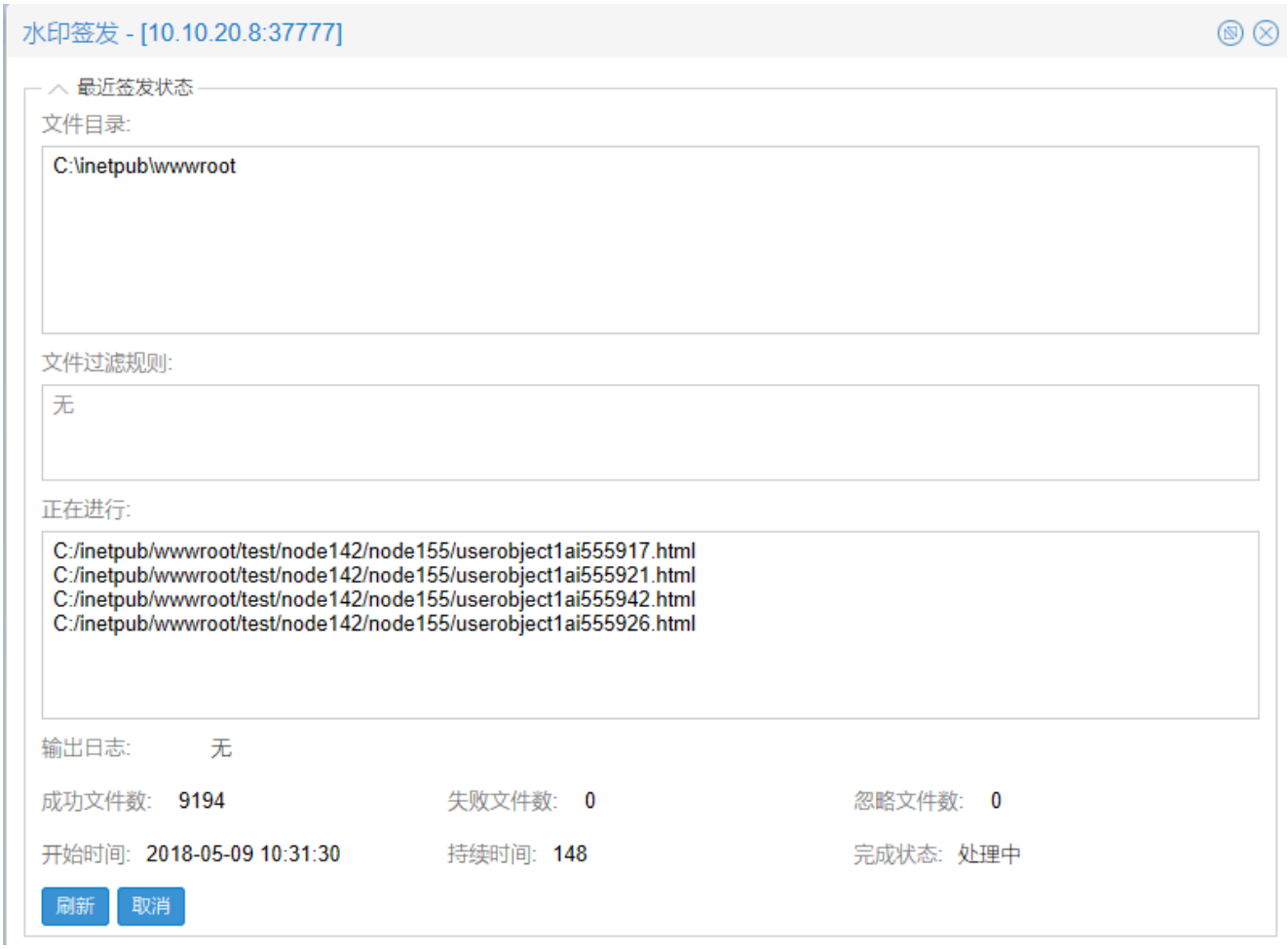


图示 3-4-12 水印签发

可以配置的信息包括：

- 目录列表：需要监视文件异常变化的目录列表，可以点击 按钮从关联站点的映射路径获取；
- 过滤规则：监视过程中需要排除的文件或目录；包含（+）即需要对满足条件的文件进行水印签发，排除（-）即不需要对满足条件的文件进行水印签发。默认值为在文件目录中的所有文件都受到实时防护。

点击【创建】后，界面上显示当前的签发进度，必要时点击【刷新】按钮查看最新状态。直至“完成状态”项中，标示为“已完成”，代表本次签发已执行完毕。

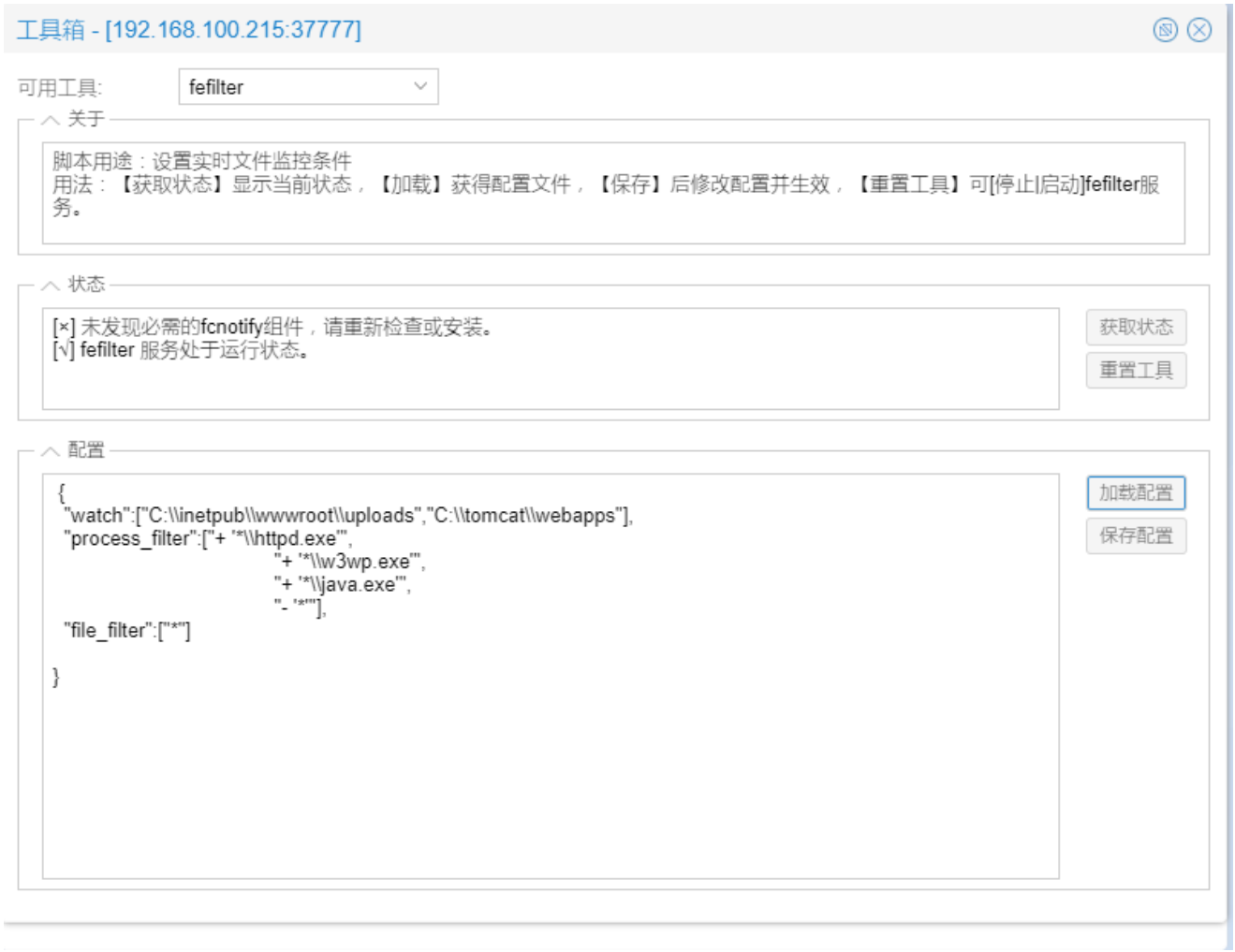


图示 3-4-13 水印签发的实时状态

3.4.7 工具箱

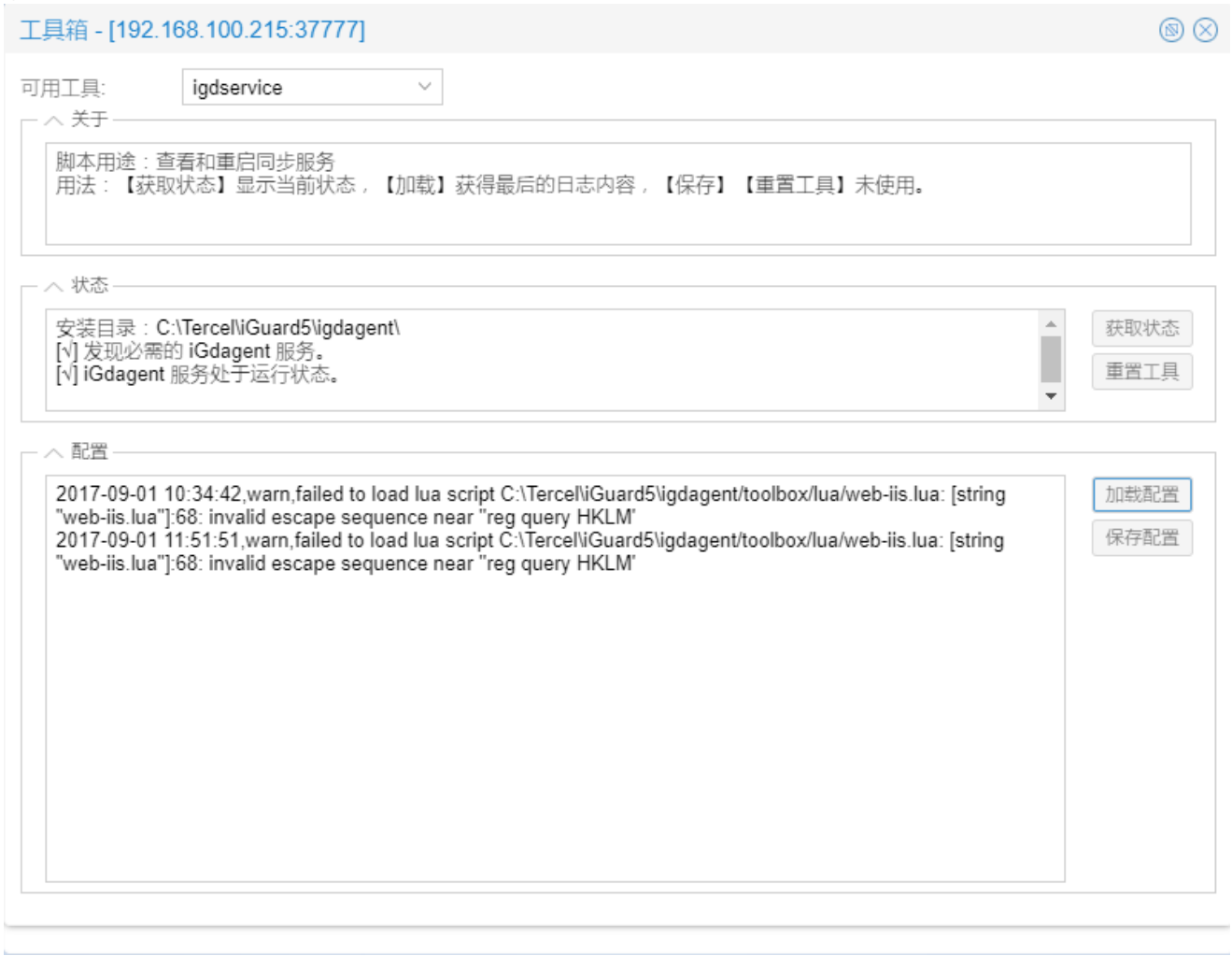
点击特定服务器记录的操作项，在页面右侧出现的配置区域选择“工具箱”配置选项页，在【可用工具】选项中选择需要查看的目标服务加载模块项，目前Windows支持可查看的加载项主要有fefilter、igdservice、managed-mods、web-tomcat、webserver-info，Linux支持可查看的加载项主要有iLocker。

- fefilter:查询当前fefilter文件监控模式的状态，配置和修改fefilter需要监控的目录和进程，需要点击【获取状态】和【加载】两个按钮才能看到截图里的内容（图示3-4-14）；



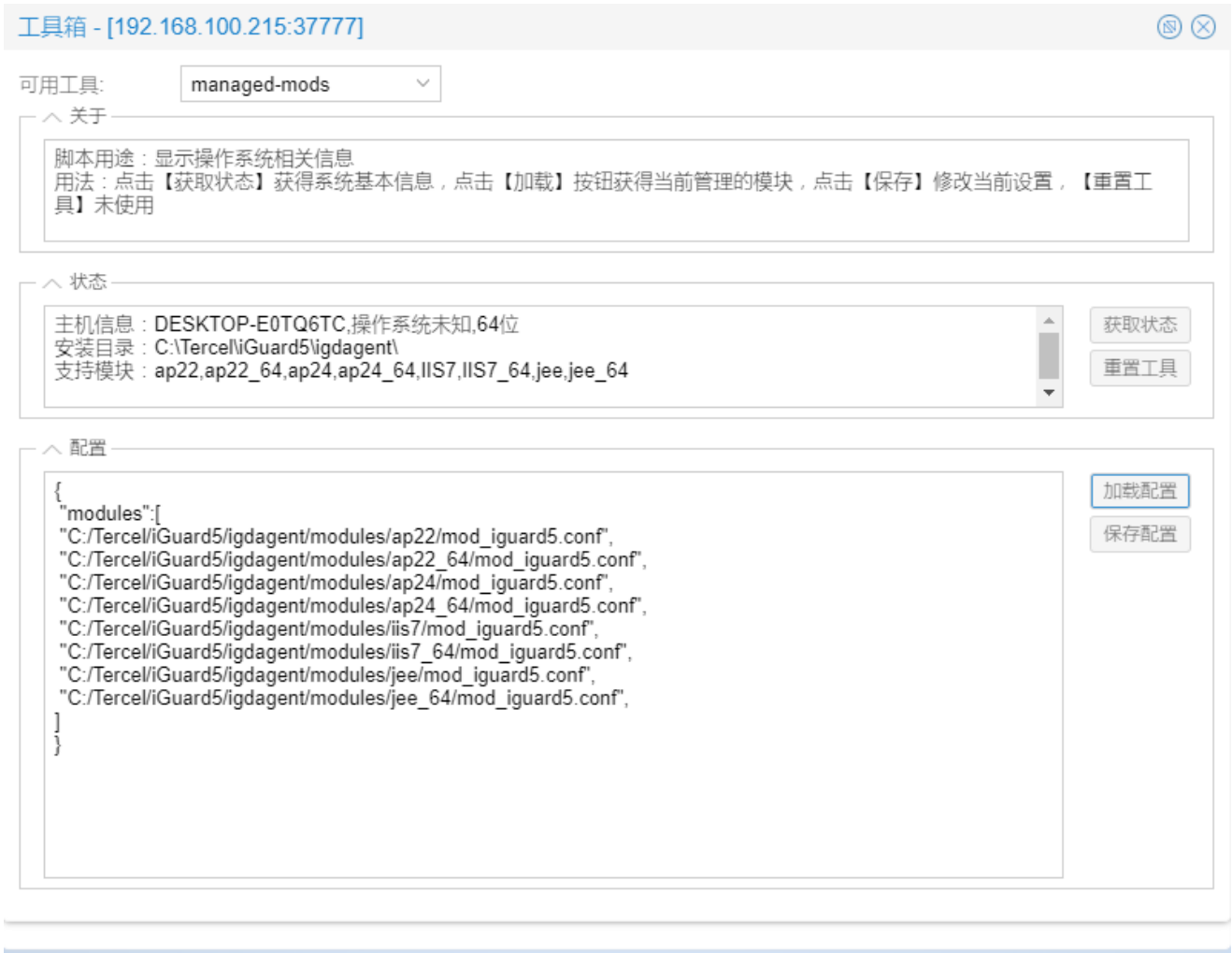
图示 3-4-14可用工具fefilter

- igdservice：查看和重启同步服务，需要点击【获取状态】和【加载】两个按钮才能看到截图里的内容（图示3-4-15）；



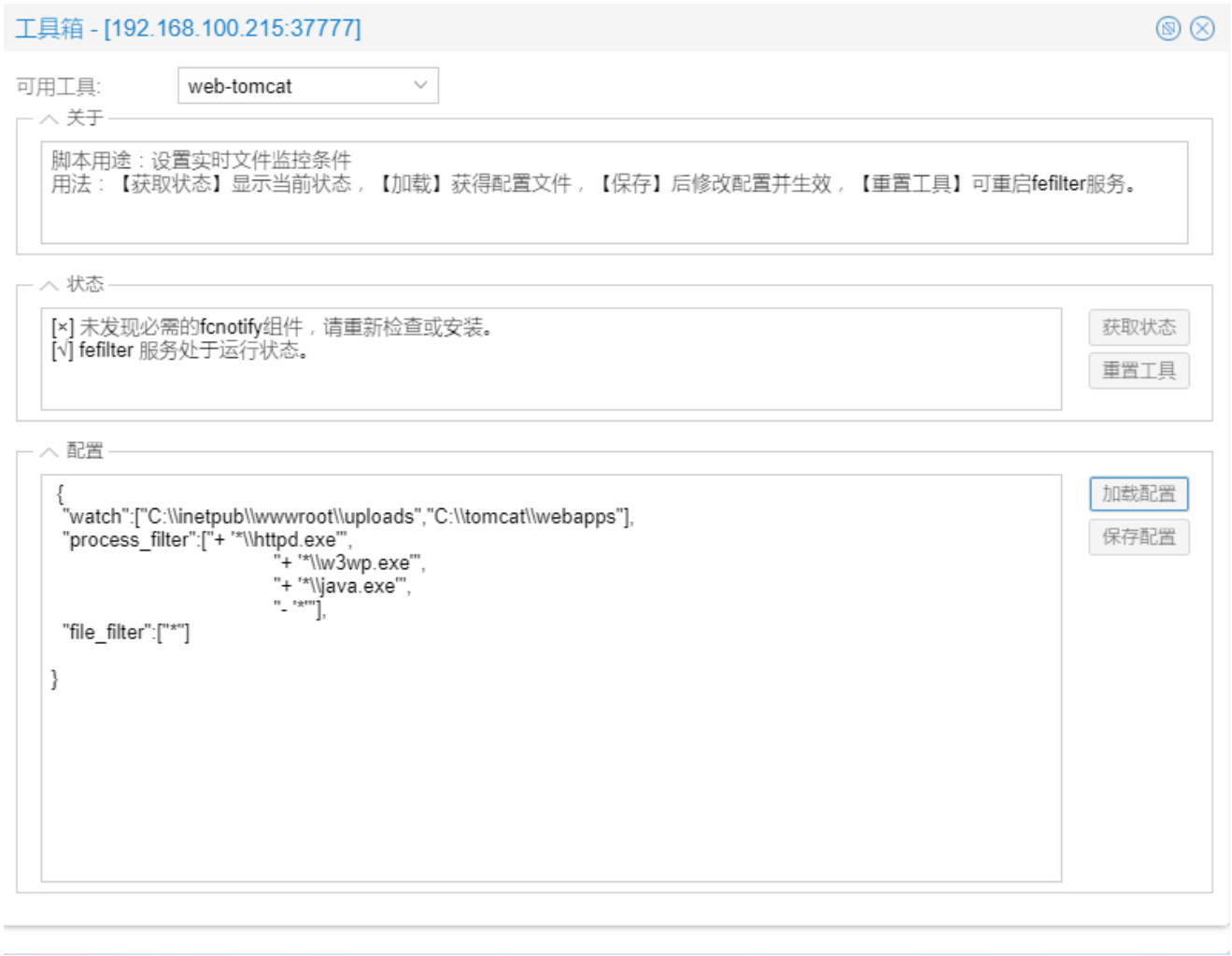
图示 3-4-15可用工具igdservice

- managed-mods：显示当前同步服务器操作系统支持模块的相关信息，需要点击【获取状态】和【加载】两个按钮才能看到截图里的内容（图示3-4-16）；



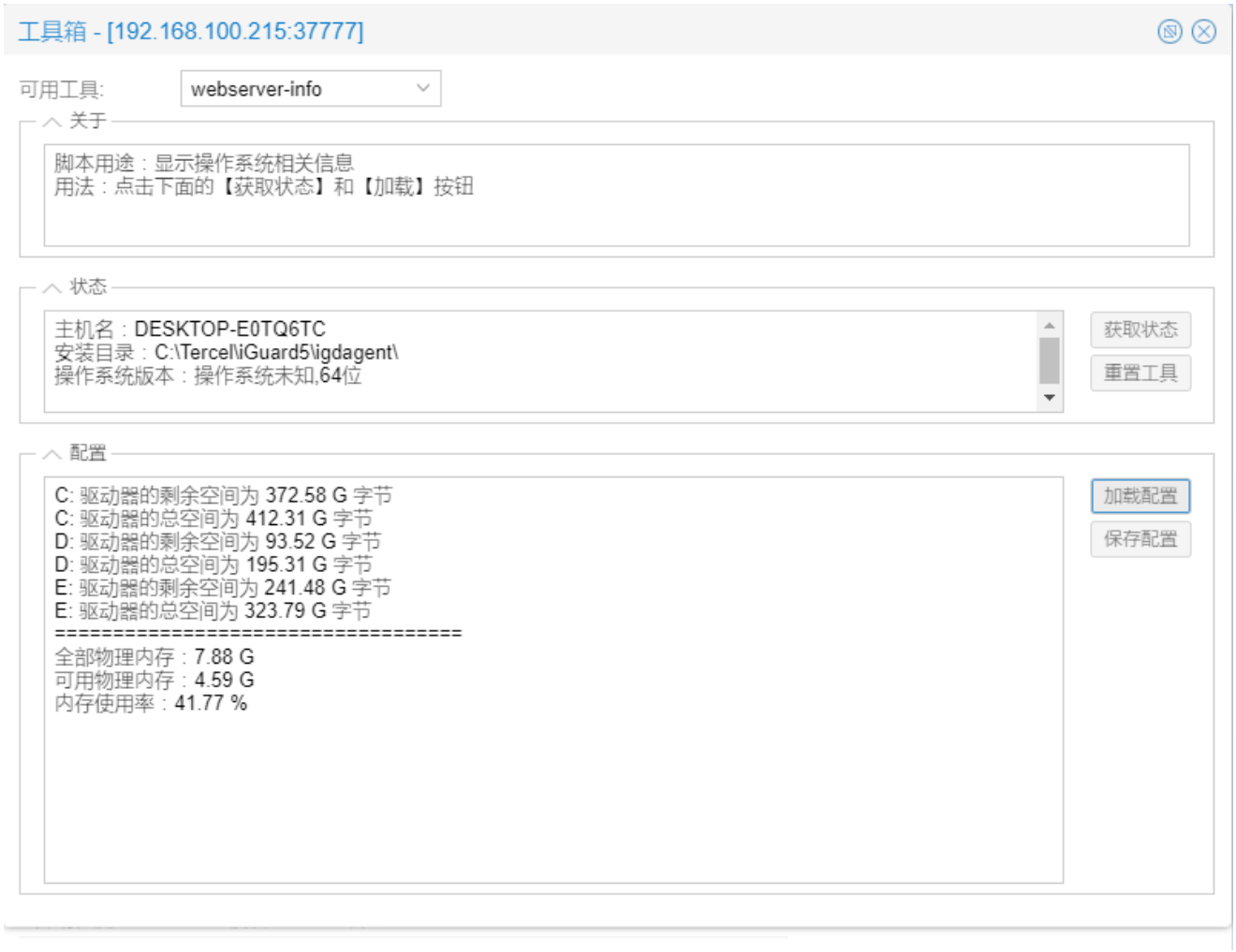
图示 3-4-16可用工具managed-mods

- web-tomcat：设置实时文件监控条件，需要点击【获取状态】和【加载】两个按钮才能看到截图里的内容（图示3-4-17）；



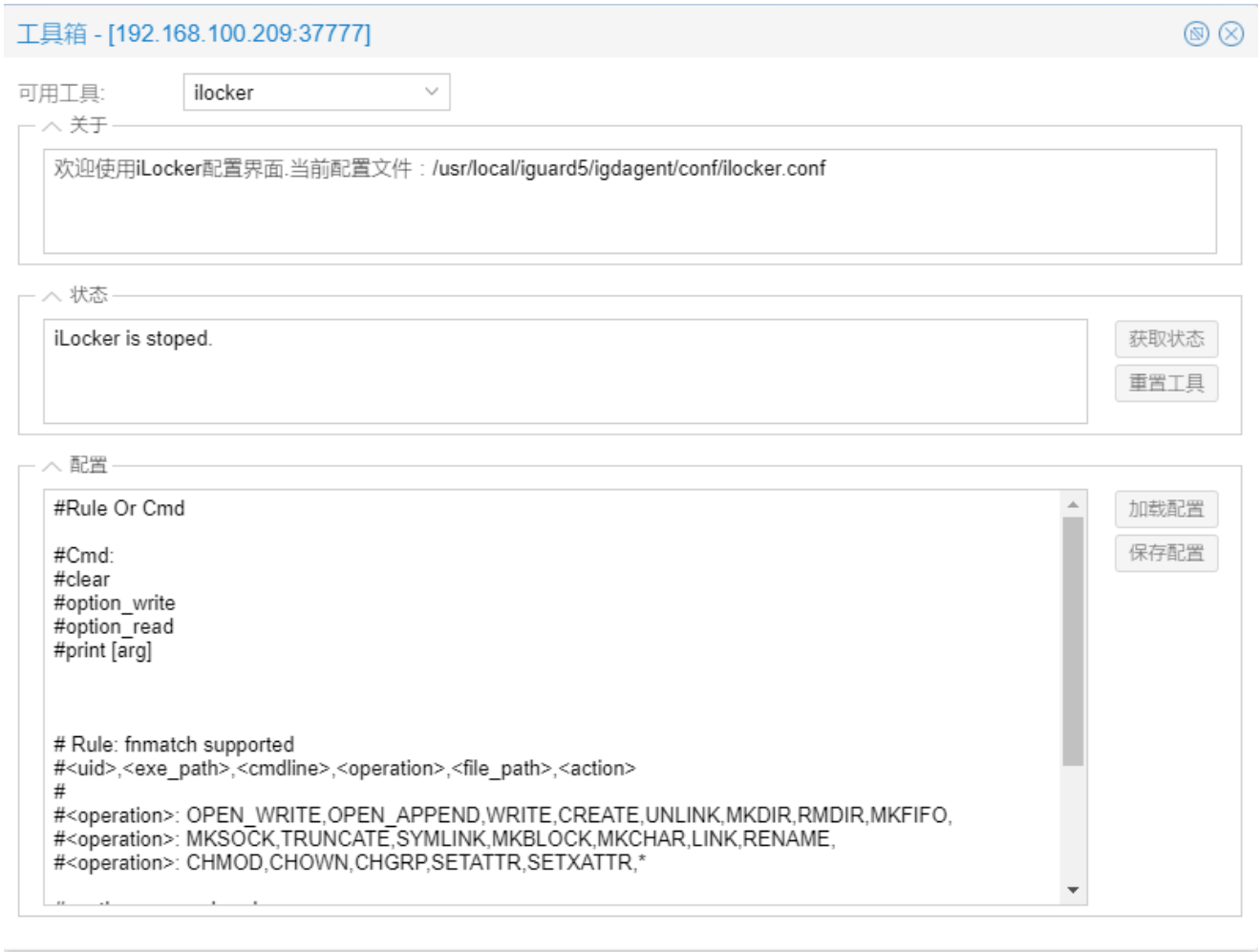
图示 3-4-17可用工具web-tomcat

- webserver-info：显示当前同步操作系统的版本和内存等相关信息，需要点击【获取状态】和【加载】两个按钮才能看到截图里的内容（图示3-4-18）；



图示 3-4-18可用工具webserver-info

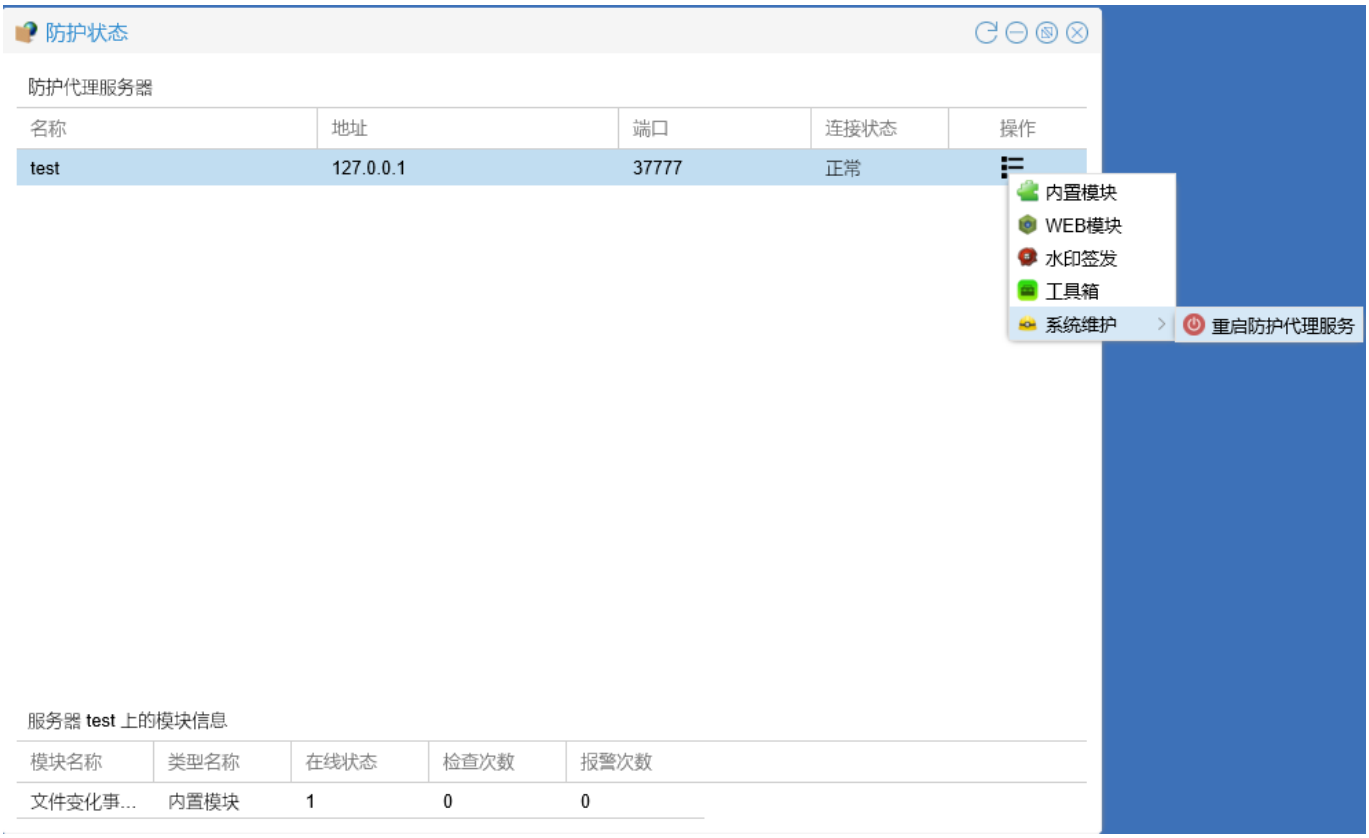
- iLocker：查询ilocker加载状态，配置和修改ilocker需要防护的目录，这个模块要目标服务器是Linux系统才能在工具箱中进行查看，需要点击【获取状态】和【加载】两个按钮才能看到截图里的内容（图示3-4-19）；



图示 3-4-19可用工具iLokcer

3.4.8 系统维护

点击特定服务器记录的操作项，在页面右侧出现的配置区域选择“系统维护”配置选项页，点击【重启防护代理服务器】按钮可以对服务器执行远程功能重启的操作（图示3-4-20）。这个重启操作的效果，是远程重启了目标服务器端的“igdagent”服务，使一些调整能及时生效。



图示 3-4-20 系统维护

3.5 同步管理

3.5.1 站点管理

点击左上角的【开始】菜单列表中的【同步管理】→【站点管理】，会弹出站点管理界面并显示当前站点的配置信息（图示3-5-1）。

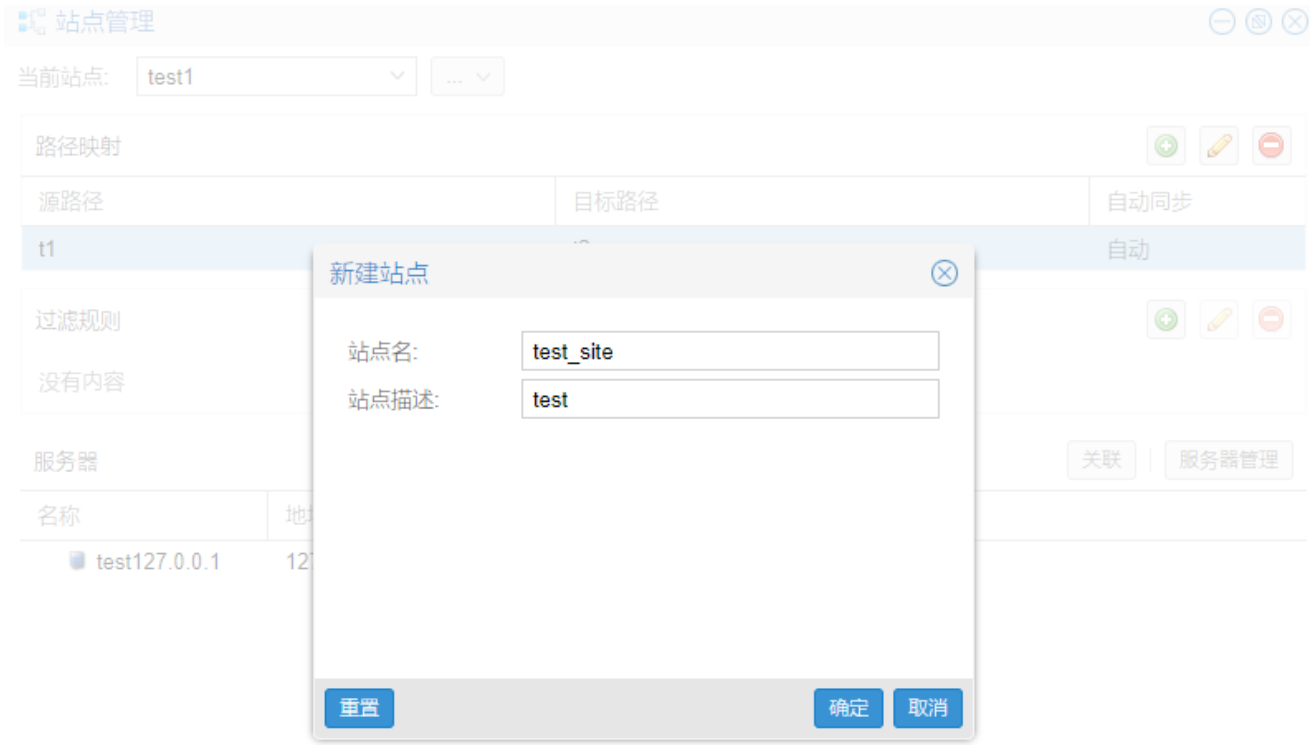
图示 3-5-1 站点配置

可以配置的信息包括：

- 路径映射：文件同步传输的源路径和目标路径的映射关系；
- 过滤规则：文件同步传输时需要进行过滤的规则条件；
- 服务器：站点所包含的服务器或服务器组。

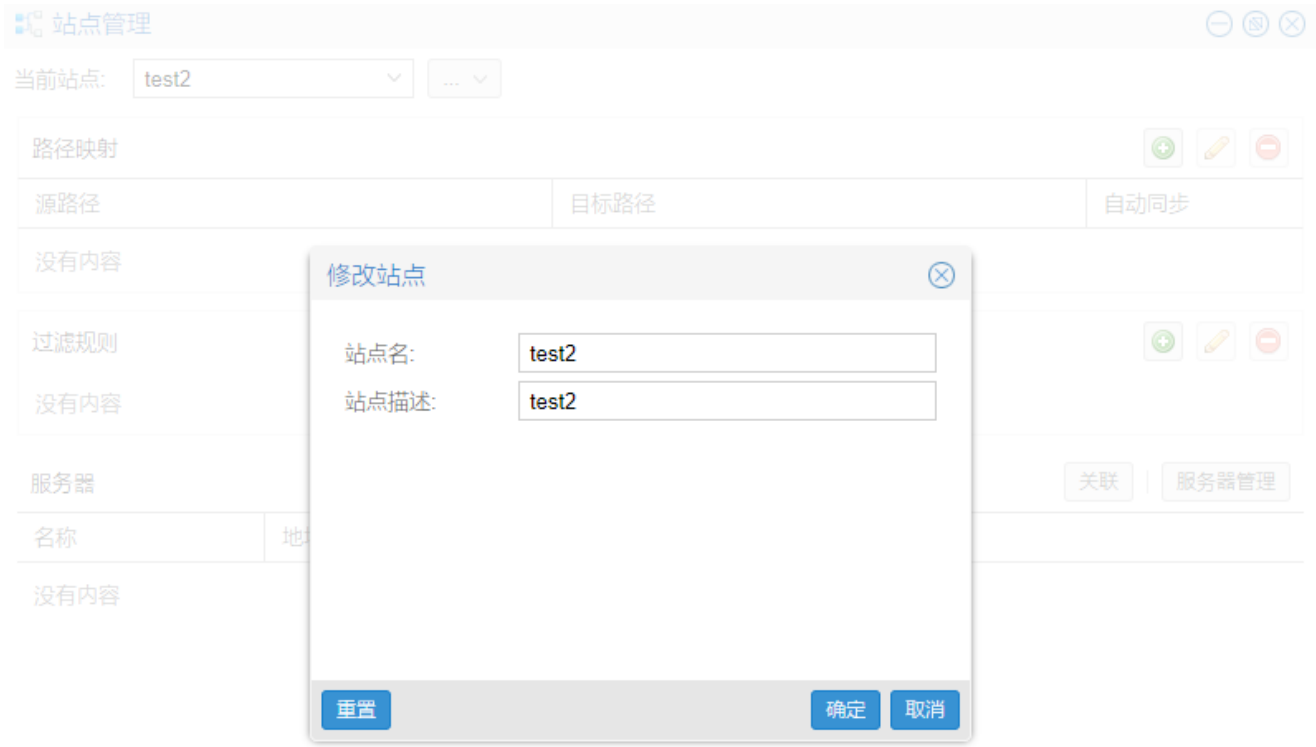
可以进行的操作包括：

- 添加站点： 点击当前站点最右侧的下拉列表中的【添加站点】，在弹出的新建站点设置框中进行操作，可以设置站点名、站点描述等信息，点击【确认】按钮完成站点的新建（图示3-5.-2）。



图示 3-5-2 新建站点

- 修改站点： 点击当前站点最右侧的下拉列表中的【修改站点】，在弹出的修改站点设置框中进行操咋，可以修改站点名、站点描述等信息，点击【确认】按钮完成站点的编辑（图示3-5-3）。



图示 3-5-3 编辑站点

- 删除站点： 点击当前站点最右侧的下拉列表中的【删除站点】，在弹出的删除站点设置框中确认中进行操作，点击【是】按钮完成站点的删除（图示3-5.4）。

图示 3-5-4 删除站点

- 新增路径映射： 点击路径映射字样右侧的 按钮，在弹出的编辑路径映射设置框中进行操作，可以配置源路径（即发布端）、目标路径（即同步端）、是否开启自动同步等信息，点击【确定】按钮完成路径映射的新增（图示3-5-5）。

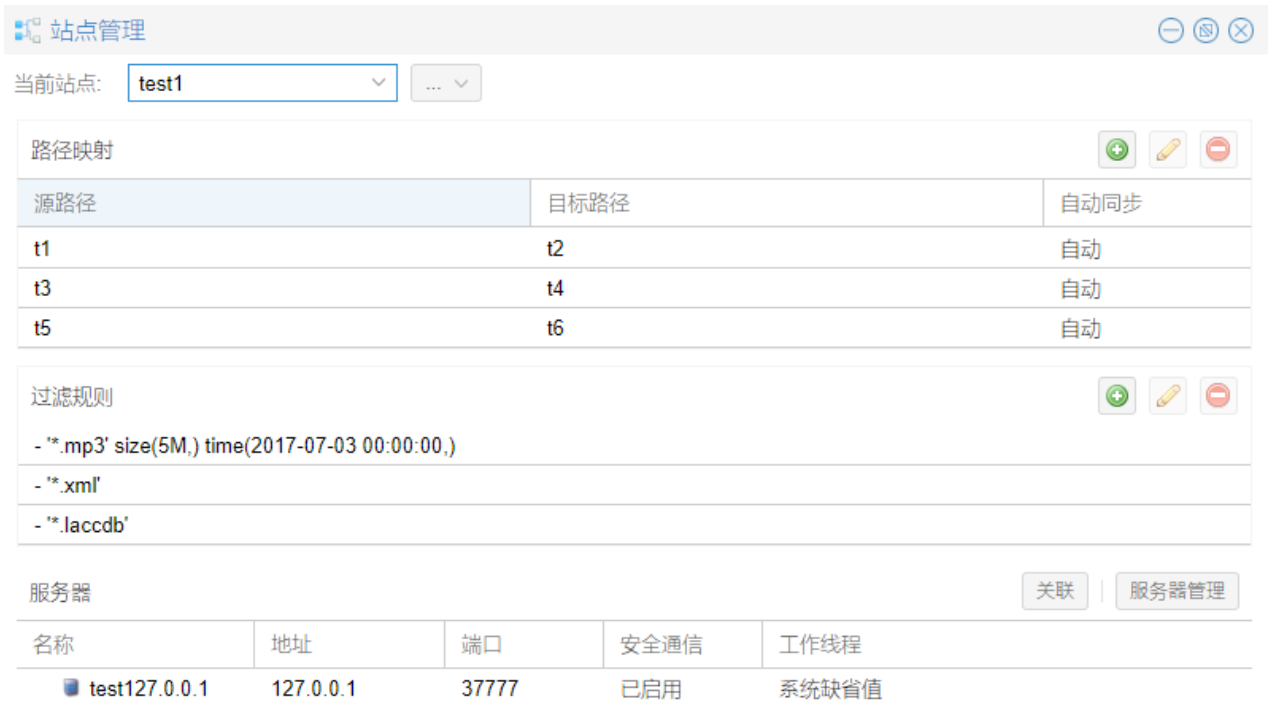
图示 3-5-5 新增路径映射

- 编辑路径映射： 选中当前需要调整的路径映射，点击路径映射字样右侧的 按钮，在弹出的编辑路径映射设置框中进行操作，可以修改源路径（即发布端）、目标路径（即同步端）、是否开启自动同步等信息，点击【确定】按钮完成路径映射的编辑。

- 删除操作： 选中当前需要删除的路径映射，单击路径映射字样右侧的⛔按钮，在弹出的编辑路径映射设置框中进行操作，点击【是】按钮完成对当前选中路径映射的删除。（图示3-5-6）。

图示 3-5-6 编辑路径映射

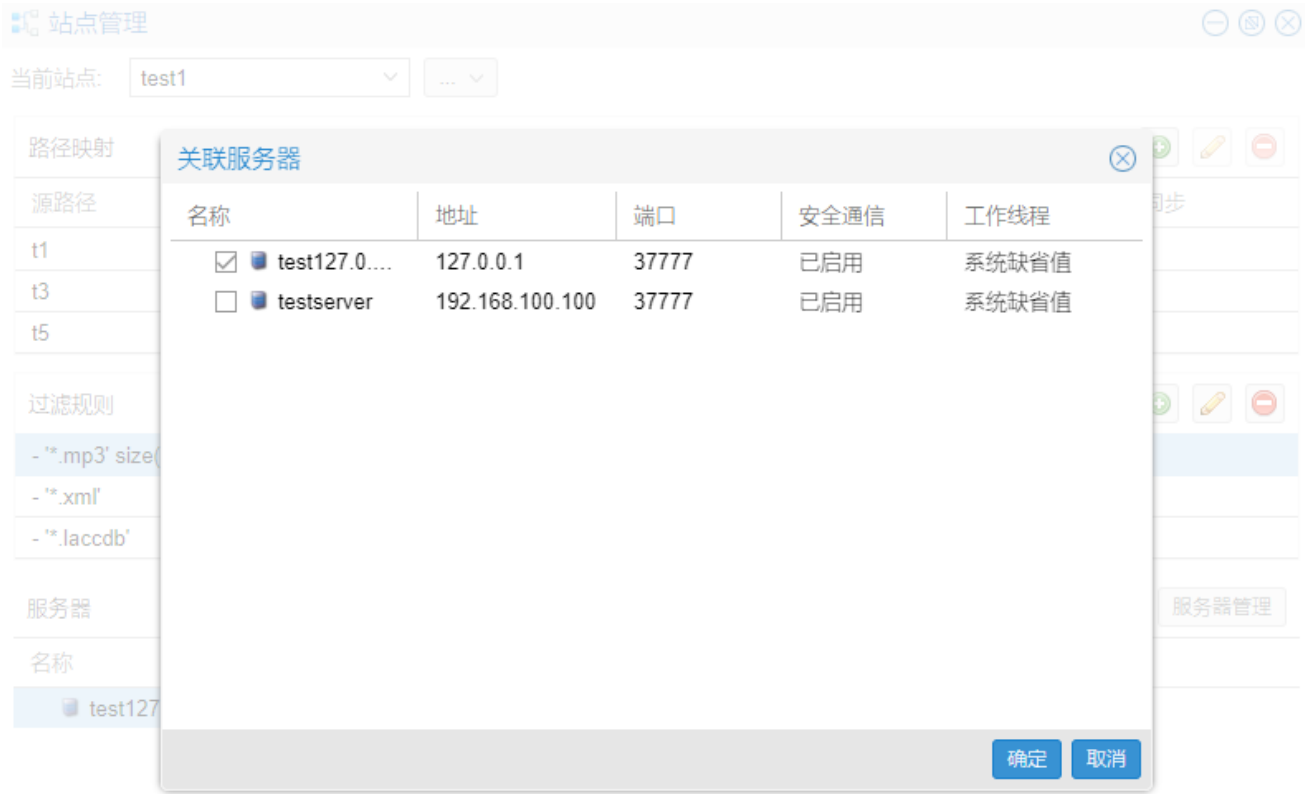
- 编辑过滤规则： 选中需要编辑的过滤规则条目，点击过滤规则字样右侧的✏按钮，在弹出的编辑过滤规则设置框中进行操作，点击【确定】按钮完成过滤规则的编辑（图示3-5-7），可以拖动过滤规则条目进行排序，或点击⛔按钮删除相应的过滤规则，点击➕按钮可以添加新的过滤规则，会弹出过滤规则配置框（图示3-5-8），可以配置的信息包括：
  - 过滤策略：包含即需要同步传输，排除即不需要同步传输；
  - 对匹配结果取反：若勾选，则对下述过滤条件进行取反操作；
  - 文件模式：对文件名的正则表达式匹配；
  - 文件类型：限制过滤文件的类型；
  - 文件尺寸：对文件大小的限制范围；
  - 时间范围：对文件创建时间的限制范围；
  - 特征数据：对特定文件内容的匹配，偏移即文件起始位置的偏移量，特征即特定的匹配数据，需以16进制格式表示。



图示 3-5-7 编辑过滤规则

图示 3-5-8 新增过滤规则

- 编辑关联服务器:
  点击服务器字样右侧的【关联】按钮，在弹出的关联服务器设置框中进行操作，选中需要进行关联的服务器记录前的复选框，点击【确定】按钮完成关联操作（图示3-5-9）。



图示 3-5-9 编辑关联服务器

3.5.2 服务器管理

点击左上角的【开始】菜单列表中的【同步管理】→【服务器管理】，会弹出服务器管理界面并显示所有服务器的配置信息（图示3-5-10）。

图示 3-5-10 服务器配置

可以查看的服务器信息包括：

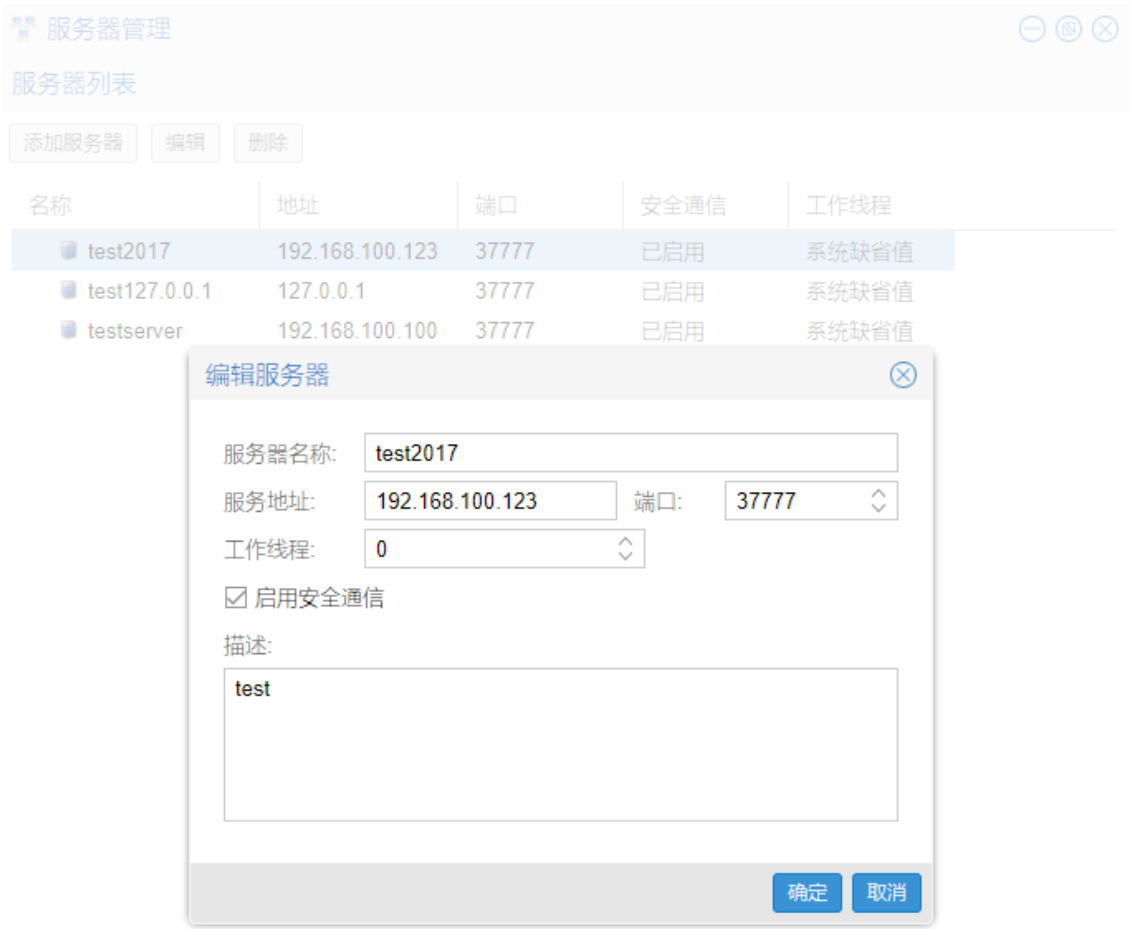
- 名称：服务器的显示名称；
- 地址：服务器的IP地址；
- 端口：服务器的通讯端口，默认为37777；
- 安全通信：是否启用SSL加密通讯；
- 工作线程：文件同步传输时的默认线程数量。

可以进行的操作包括：

- 新增服务器：
  点击服务器列表字样下方的操作项【新增服务器】，在弹出的新增服务器设置框中进行操作，可以设置服务器名、服务地址、端口、勾选是否启用安全通信（SSL）、工作线程、描述等信息，点击【确定】按钮完成服务器的新增（图示3-5-11）。

图示 3-5-11 新增服务器

- 编辑服务器： 选中特定的服务器记录，点击服务器列表字样下方的操作项【编辑】，在弹出的编辑服务器设置框中进行操作，可以修改服务器名、服务地址、端口、勾选是否启用安全通信（SSL）、工作线程、描述等信息，点击【确定】按钮完成服务器的编辑（图示3-5-12）。



图示 3-5-12 编辑服务器

- 删除服务器： 选中特定的服务器记录，点击服务器列表字样下方的操作项【删除】，在弹出的编辑服务器设置框中进行操作，可以修改服务器名、服务地址、端口、勾选是否启用安全通信（SSL）、工作线程、描述等信息，点击【确定】按钮完成服务器的编辑；可以点击【删除】按钮对当前的服务器进行删除操作

3.5.3 手工同步

点击左上角的【开始】菜单列表中的【同步管理】→【手工同步】，页面显示手工同步的相关选项（图示3-5-13），主要包括：

- 当前站点：选择需要进行手工同步的站点；
- 指定同步文件/目录：选中需要进行手工同步的源路径映射；
- 选择目标服务器：选择需要进行手工同步的服务器。

图示 3-5-13 手工同步

选项确定后，在【更多选项】配置区域，可以点击 按钮新增本次手工同步的过滤规则（图示3-5-14），具体配置方法请参见“3.5.1 站点”章节中对于【编辑过滤规则】的介绍。

图示 3-5-14 手工同步更多选项

可以选择勾选“尝试同步目录结构，包括空目录”和“精确同步”按钮，两者的功能分别是：

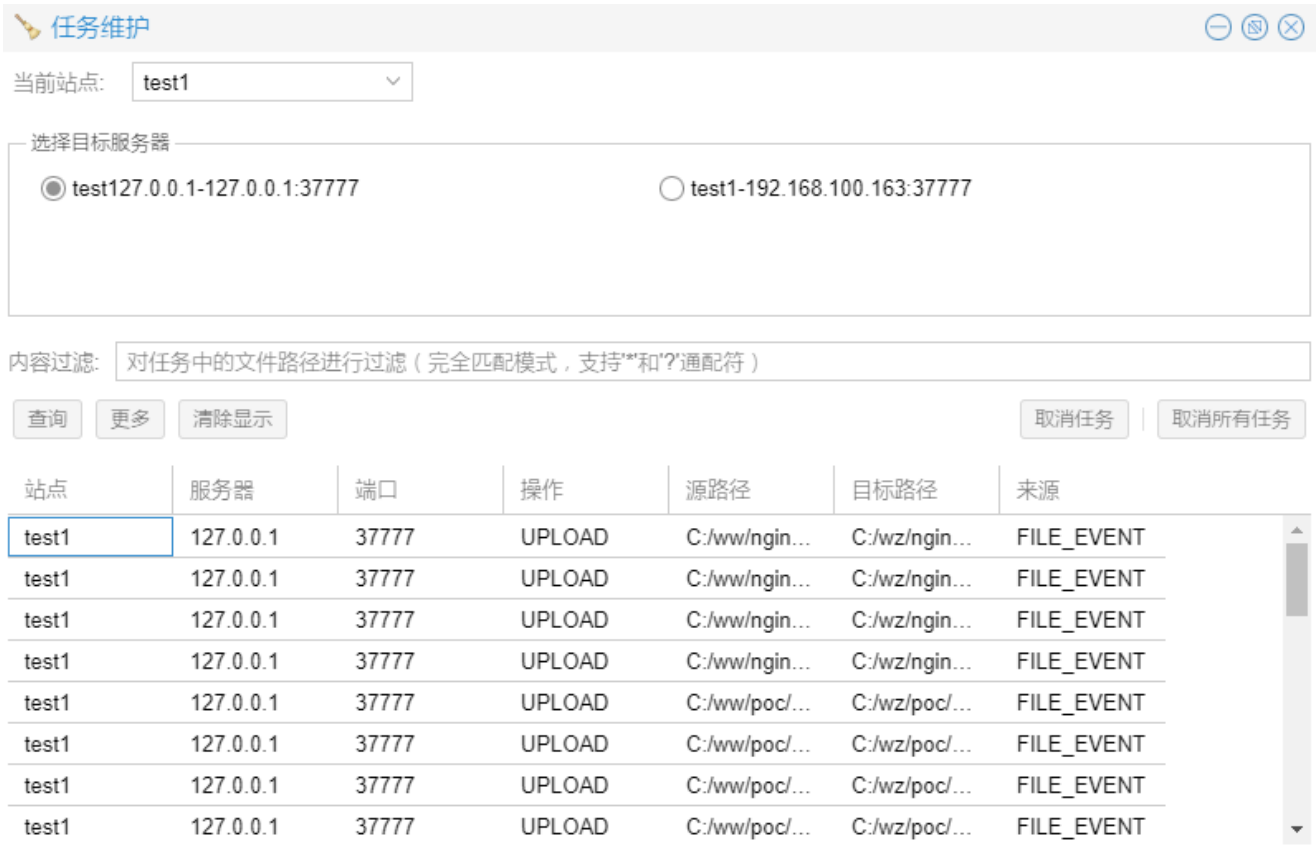
- 尝试同步目录结构，包括空目录：将源路径的所有文件目录（不管是否有内容），都同步到目标路径，并且保持与源路径相同的目录结构；
- 精确同步：将源路径的所有文件同步到目标路径，并且对目标路径原有的文件数量进行一致性比对，删除多余的旧文件，确保源路径和目标路径的文件数量和内容完全一致。

注意：手工同步的【附加过滤规则】仅对本次同步生效，而配置的【全站过滤规则】也同时生效，但优先级低于【附加过滤规则】，即在手工同步过程中，先应用【附加过滤规则】，再应用【全站过滤规则】。

3.5.4 任务维护

点击左上角的【开始】菜单列表中的【同步管理】→【任务维护】，可以根据选项来查看当前正在执行的同步任务（图示3-5-15），选项主要包括：

- 当前站点：选择需要进行手工同步的站点；
- 选择目标服务器：选择需要进行手工同步的服务器；
- 过滤内容：对任务中的文件路径进行过滤，采用完全匹配模式，支持'*'和'？'通配符。



图示 3-5-15 任务维护

可以查看的服务器信息包括：

- 站点：同步站点的显示名称；
- 服务器：服务器的IP地址；
- 端口：服务器的通讯端口，默认为37777；
- 操作：文件正在被执行的操作；
- 源路径：被同步文件的所在目录；
- 目标路径：被同步文件的目的目录；
- 来源：文件同步执行的动作来源。

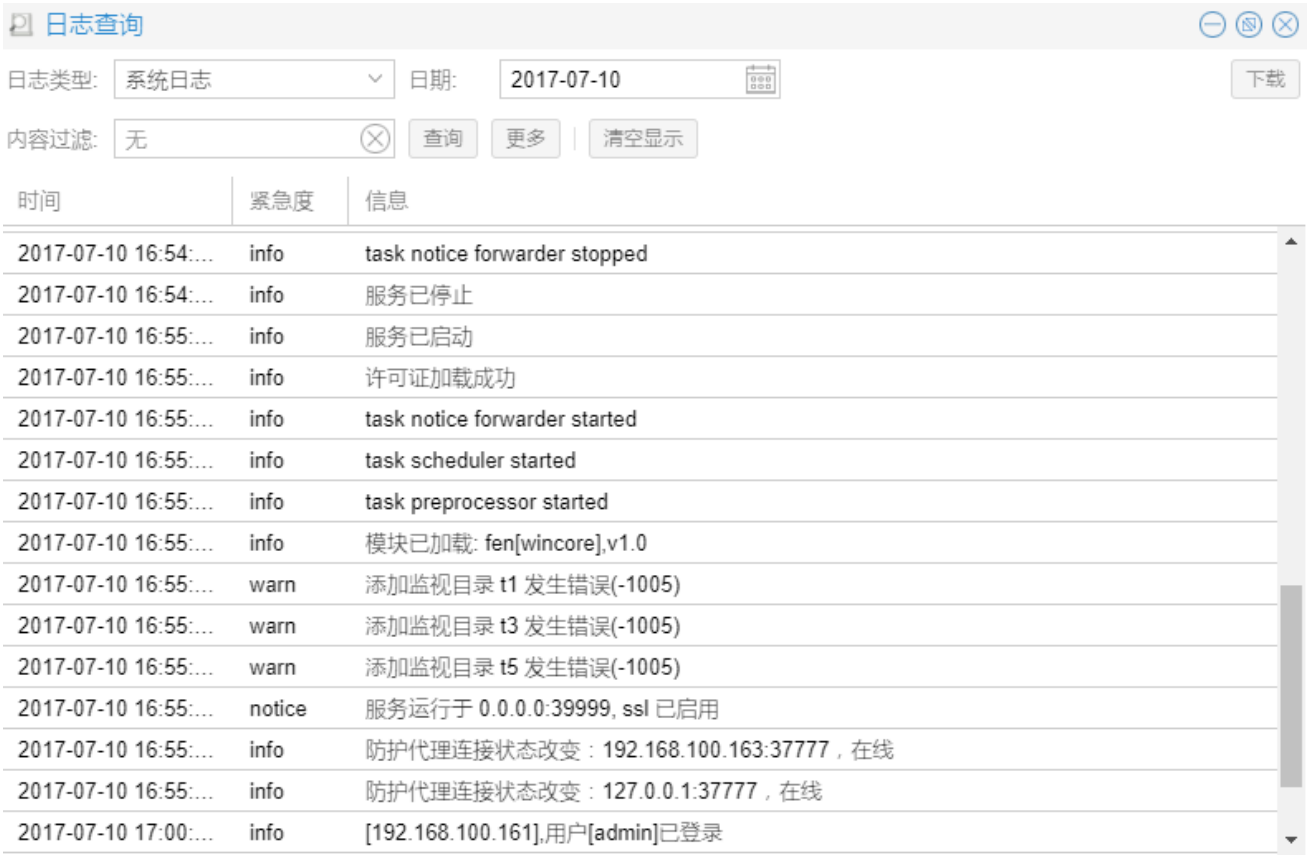
可以进行的操作包括：

- 查询： 点击【查询】按钮，可显示当前正在执行的同步任务。
- 更多： 当前任务数过多时，点击【更多】按钮可以继续加载显示；。
- 清除显示： 点击【清除显示】按钮，可以取消显示当前正在进行中的任务。
- 取消任务： 点击【取消任务】按钮，可取消当前选中的同步任务。
- 取消所有任务： 点击【取消所有任务】按钮，可取消当前正在进行的所有同步任务。

3.6 系统管理

3.6.1 日志查询

点击左上角的【开始】菜单列表中的【系统管理】→【日志查询】，会弹出日志查询界面，并显示各类操作日志记录列表，包括系统日志、报警日志、传输日志和失败任务日志（图示3-6-1）。



时间	紧急度	信息
2017-07-10 16:54:...	info	task notice forwarder stopped
2017-07-10 16:54:...	info	服务已停止
2017-07-10 16:55:...	info	服务已启动
2017-07-10 16:55:...	info	许可证加载成功
2017-07-10 16:55:...	info	task notice forwarder started
2017-07-10 16:55:...	info	task scheduler started
2017-07-10 16:55:...	info	task preprocessor started
2017-07-10 16:55:...	info	模块已加载: fen[wincore],v1.0
2017-07-10 16:55:...	warn	添加监视目录 t1 发生错误(-1005)
2017-07-10 16:55:...	warn	添加监视目录 t3 发生错误(-1005)
2017-07-10 16:55:...	warn	添加监视目录 t5 发生错误(-1005)
2017-07-10 16:55:...	notice	服务运行于 0.0.0.0:39999, ssl 已启用
2017-07-10 16:55:...	info	防护代理连接状态改变：192.168.100.163:37777，在线
2017-07-10 16:55:...	info	防护代理连接状态改变：127.0.0.1:37777，在线
2017-07-10 17:00:...	info	[192.168.100.161],用户[admin]已登录

图示 3-6-1 日志查询

可以进行的操作包括：

- 查询：输入日志类型、日期、过滤内容等条件，点击【查询】按钮，页面显示符合条件的日志记录列表；
- 更多：当日志记录过多时，点击【更多】按钮可以继续加载显示；
- 清空显示：点击【清空】按钮清除当前页面的日志显示，但此操作不会将日志从系统中删除；
- 下载：在配置区域选择“日志类型”和“日期”等筛选条件，点击【下载】按钮可以将符合条件的操作日志记录保存到本地。

注意：保存到本地的操作日志文件，目前仅支持纯文本格式（*.log）。

3.6.2 用户管理

点击左上角的【开始】菜单列表中的【系统管理】→【用户管理】，会弹出用户管理界面，并显示当前所有用户的列表（图示3-6-2）。

用户名	角色	电子邮箱	备注
admin	超级管理员		
user1	操作员	123@tcxa.com.cn	管理员1
user2	操作员	234@tcxa.com.cn	管理员2

图示 3-6-2 用户管理

可以查看的用户信息包括：

- 用户名：显示当前用户的名称；
- 角色：显示当前用户的具备的管理权限；

- 电子邮箱：显示当前用户的电子邮件地址；
- 备注：显示对当前用户的描述信息。

可以进行的操作包括：

- 新增用户： 点击页面左上方的操作项【 添加】按钮，在弹出的用户编辑设置框中进行操作，可以设置用户名、密码、电子邮箱、角色和备注等信息，点击【确定】按钮完成用户的新增（图示3-6-3）。

图示 3-6-3 新增用户

- 编辑用户： 选中需要修改的用户记录，点击页面左上方的操作项【 修改】按钮，在弹出的用户编辑设置框中进行操作，可以修改用户名、密码、电子邮箱、角色和备注等信息，点击【确定】按钮完成用户的编辑（图示3-6-4）。

图示 3-6-4 编辑用户

- 删除用户： 选中需要删除的用户记录，点击页面左上方的操作项【 删除】按钮，在弹出的确认设置框中进行操作，点击【是】按钮完成用户的删除（图示3-6-5）。

图示 3-6-5 删除用户

- 分配站点： 选中需要分配站点的用户记录，点击页面右上方的操作项【分配站点】按钮，在弹出的分配站点设置框中进行操作，勾选需要分配给当前用户进行管理的站点名称，点击【确认】按钮完成分配站点的操作（图示3-6-6）。

图示 3-6-6 分配站点

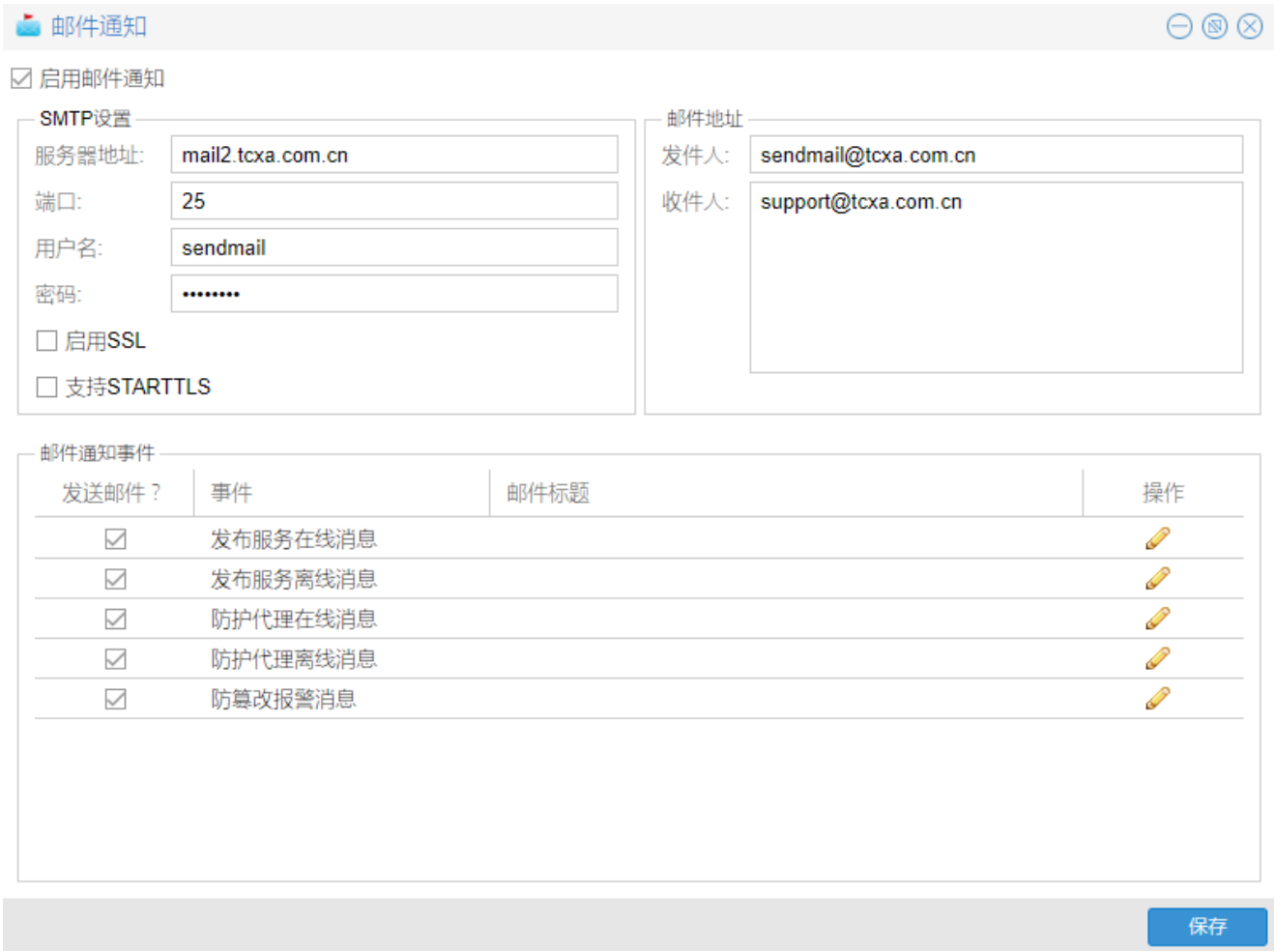
- 重置密码： 选中需要重置密码的用户记录，点击页面右上方的操作项【重置密码】按钮，在弹出的更改密码设置框中为该用户设置新的密码，点击【确定】按钮完成重置密码的操作（图示3-6-7）。

图示 3-6-7 重置密码

注意：只有具备“超级管理员”权限的用户，才能对“操作员”权限的人员进行【分配站点】和【重置密码】操作，反之不可。

3.6.3 邮件通知

点击左上角的【开始】菜单列表中的【系统管理】→【邮件通知】，页面显示邮件通知的配置选项，修改配置后，可以点击【保存】按钮完成对邮件通知配置修改的操作（图示3-6-8）。 在“开启”配置区域，可以选择是否启用邮件通知的功能。



图示 3-6-8 邮件通知

在“SMTP设置”配置区域，可以配置的信息包括：

- 服务器地址：用于发送的邮件服务器地址；
- 端口：用于发送的邮件服务器端口；
- 用户名：用于发送的邮箱用户名；
- 密码：用于发送的邮箱密码；
- 启用SSL：是否使用SSL方式连接；
- 支持STARTTLS：是否支持STARTTLS验证。

在“邮件地址”配置区域，可以配置的信息包括：

- 发件人：发送邮件的邮箱帐号；
- 收件人：接收邮件的邮箱帐号列表。

在“邮件通知事件”配置区域，可以勾选是否发送通知的信息包括：

- 发布服务在线消息：是否发送“发布服务在线”的邮件通知，并且可以设置特定的邮件标题；
- 发布服务离线消息：是否发送“发布服务离线”的邮件通知，并且可以设置特定的邮件标题；
- 防护代理在线消息：是否发送“防护代理在线”的邮件通知，并且可以设置特定的邮件标题；
- 防护代理离线消息：是否发送“防护代理离线”的邮件通知，并且可以设置特定的邮件标题；
- 防篡改报警消息：是否发送“防篡改报警”的邮件通知，并且可以设置特定的邮件标题。

3.6.4 控制面板

点击左上角的【开始】菜单列表中的【系统管理】→【控制面板】，会弹出控制面板操作框，并显示可以操作的内容，可以对文件事件、邮件通知、用户管理、文件传输、双机发布、产品注册及系统选项进行配置（图示3-6-9）。

图示 3-6-9 控制面板

可以进行的配置操作包括：

- 文件事件：具体步骤请见【3.6.4.1 文件事件 】章节。
- 邮件通知：具体步骤请见【3.6.3 邮件通知 】章节。
- 用户管理：具体步骤请见【3.6.2 用户管理 】章节。
- 文件传输：具体步骤请见【3.6.4.2 文件传输 】章节。
- 双机发布：具体步骤请见【3.6.4.3 双机发布 】章节。
- 产品注册：具体步骤请见【3.6.4.4 产品注册 】章节。
- 系统插件：具体步骤请见【3.6.4.5 系统插件 】章节。
- 系统选项：点击控制面板界面的【系统选项】操作项。可以对发布服务的端口做自定义设置，如把默认的39999端口调整为所需的其他端口。另外可以调整系统日志的级别，点击【保存】按钮完成对系统项的操作。

3.6.4.1 文件事件

点击控制面板界面的【文件事件】操作项，会跳转至文件事件操作框，可以对文件事件进行配置（图示3-6-10）。

图示 3-6-10 文件事件

在“文件变化监测”配置区域，可以配置的内容包括：

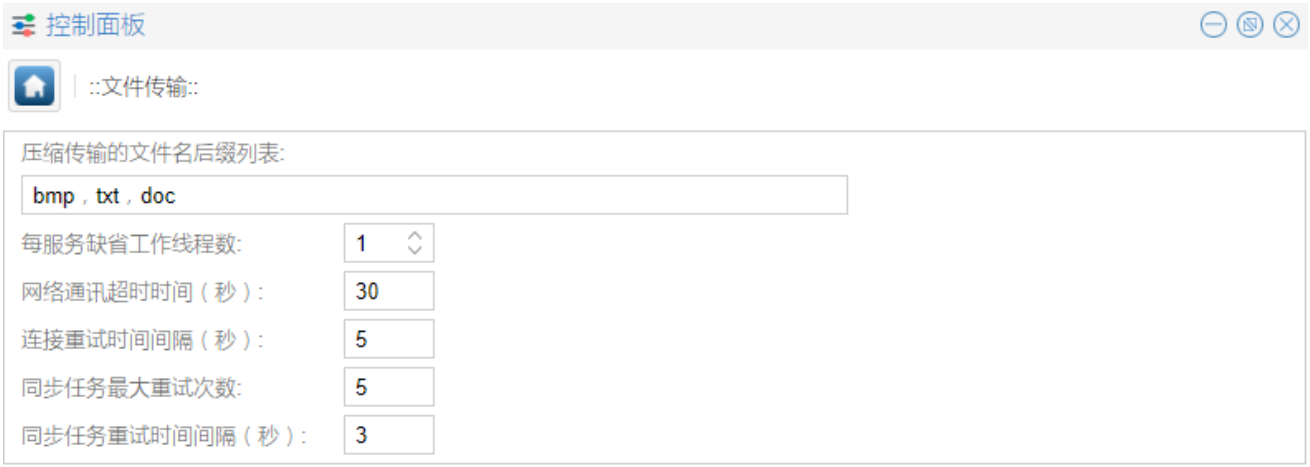
- 文件变化事件延后处理最小等待时间：默认为1s，可自行修改；
- 文件变化事件延后处理最大等待时间：默认为30s，可自行修改；
- 文件变化就绪检测的延迟时间：默认为3s，可自行修改；
- 文件变化预处理扫描间隔时间：默认为2s，可自行修改。

在“文件恢复”配置区域，若勾选“针对文件被篡改事件，进行文件恢复处理”，则会在文件被篡改之后进行文件的同步恢复；反之，则不进行恢复。

在“任务取消”配置区域，若勾选“手动取消的任务需要计入日志”，则会将手动取消的同步任务写入日志中；反之，则不会将取消的任务写入日志。

3.6.4.2 文件传输

点击控制面板界面的【文件传输】操作项，会跳转至文件传输操作框，并显示全局范围的文件传输配置参数信息（图示3-6-11）。



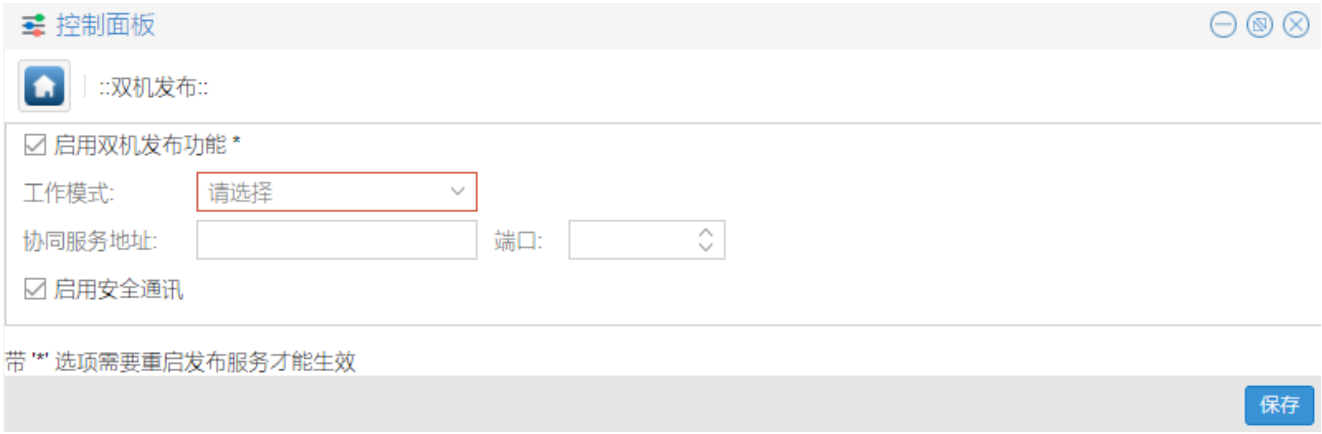
图示 3-6-11 文件传输

可以设置的配置参数包括：

- 压缩传输的文件名后缀列表：文件同步传输时，需要进行压缩的文件类型；
- 每服务缺省工作线程数：文件同步传输时，全局默认的线程数量；
- 网络通讯超时时间（秒）：超过默认时长无响应，视为超时，默认值为30s，可自行配置；
- 连接重试时间间隔（秒）：超时后的重试连接时间间隔，默认为5s，可自行配置；
- 同步任务最大重试次数：同步失败后的尝试重新同步次数，默认为5次，可自行配置；
- 同步任务重试时间间隔（秒）：同步失败后的尝试重新同步的时间间隔，默认为3秒，可自行配置。

3.6.4.3 双机发布

点击控制面板界面的【双机发布】操作项，会跳转至双机发布配置操作框，显示当前的发布模式（图示3-6-12），双机发布存在主备模式和先启先服务两种工作模式，主备模式需要设定一台发布服务器为主机，另外一台作为备机，通常情况下由主机进行发布等一系列工作，在主机服务停用后备机会接替主机继续工作；先启先服务模式不需要设置。



图示 3-6-12 双机发布

可以设置的配置内容包括：

- 启用双机发布功能：默认情况下不启用，需要使用的时候在前面的方框内进行勾选，需要重启发布服务才能生效；
- 工作模式：可以选择主机、备机或先启先服务中的一种；
- 协同服务地址：另外一台发布服务器的IP地址；
- 端口：与另外一台发布服务器进行通讯的端口号；
- 启用安全通讯：是否启用SSL加密通讯。

发布备机安装方法：将当前发布服务器中的StagingServer目录连同里面的所有内容拷贝至需要安装为备机的服务器，使用管理员权限运行发布备机上的cmd命令控制台，输入"C:\Tercel\iGuard5\StagingServer\stagingd.exe" -k install，按回车键完成注册（图示3-5-13）。

图示 3-5-13 注册stagingd5服务

注意：输入的"C:\Tercel\iGuard5\StagingServer\stagingd.exe"即为stagingd.exe所在的实际路径，因此需按照实际情况修改；注册完成后stagingd5服务处于停用状态，第一次启动需手工进行，之后随系统自动启动。

3.6.4.4 产品注册

点击控制面板界面的【产品注册】操作项，会跳转至产品注册操作框，显示当前系统的许可证信息（图示3-6-14）。

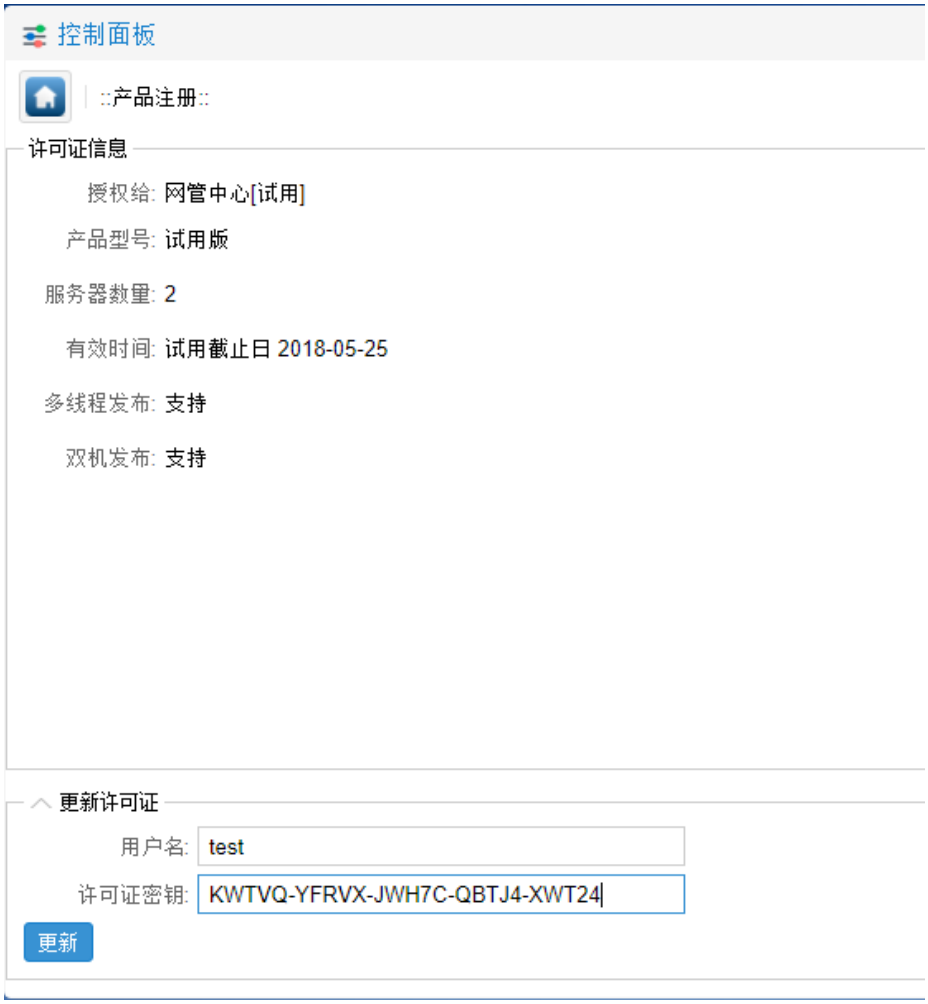
图示 3-6-14 许可证信息

可以查看的许可证信息包括：

- 授权给：显示当前许可证的用户名称；
- 产品型号：显示当前许可证对应的版本；
- 服务器数量：显示当前许可证支持的可添加服务器的最大数量；
- 有效时间：显示当前许可证的过期时间及提供技术支持的截止时间；
- 多线程发布：显示当前许可证是否支持文件同步传输的多线程机制；
- 操作系统：显示当前许可证是否对服务器的操作系统类型及版本进行限制；
- 双机发布：显示当前许可证是否支持发布服务器的双机部署；
- 激活状态：显示当前许可证是否已经激活；
- 证书编号：显示许可证的唯一编号。

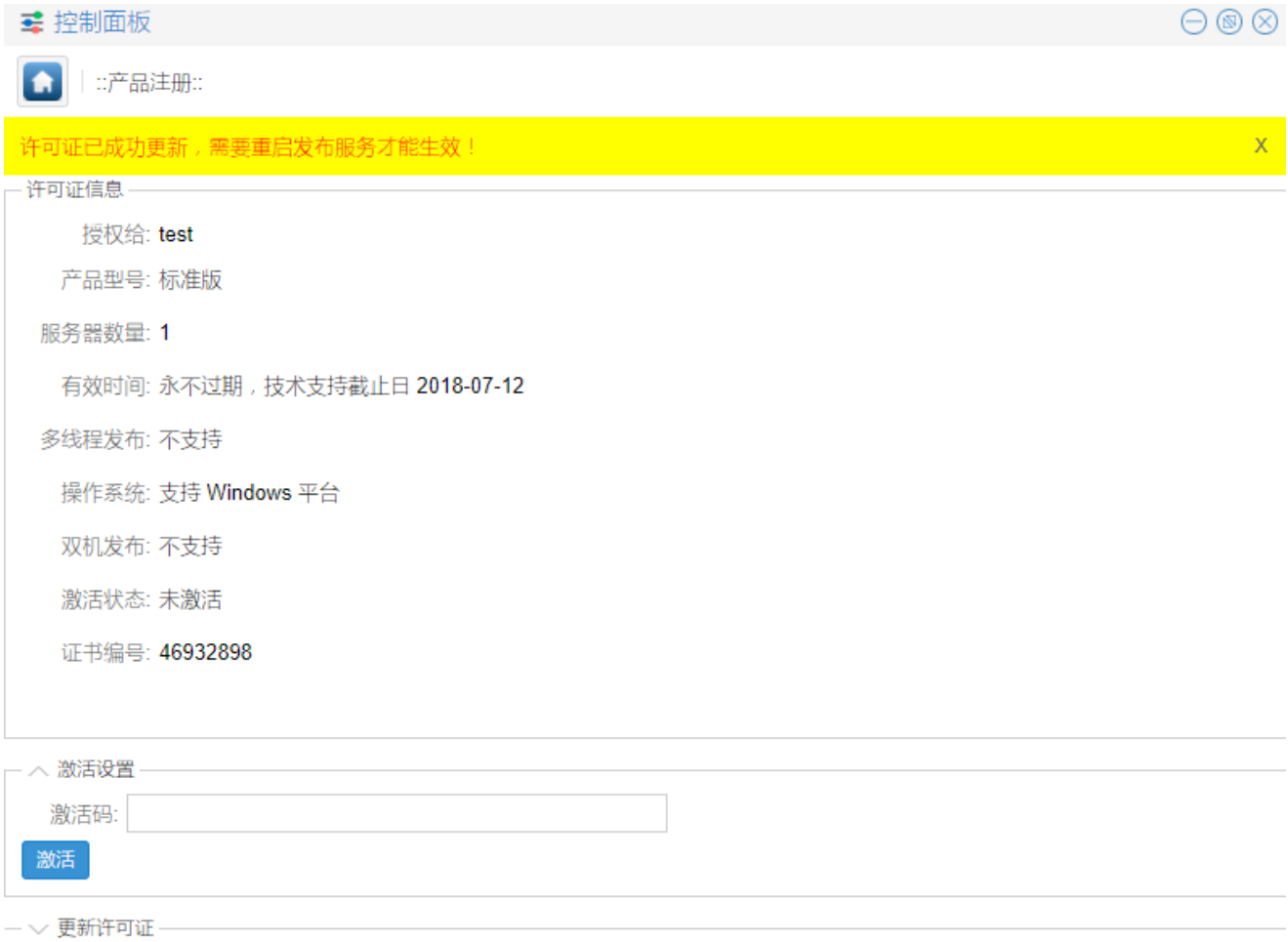
可以进行的操作包括：

- 更新许可证：点击产品注册页面中的“更新许可证”按钮，出现注册信息输入框（图示3-6-15）



图示 3-6-15 输入许可证信息

输入有效许可证的用户名和许可证密钥，点击【更新】按钮，完成许可证信息的更新操作（图示3-6-16）。



图示 3-6-16 显示输入的许可证信息

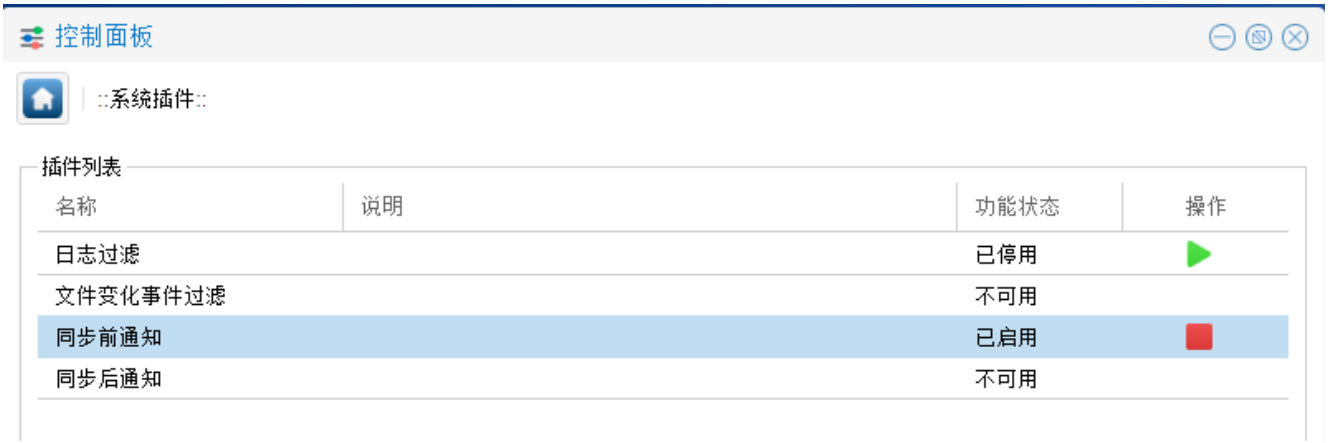
- 激活设置：只有输入正式许可证的时候才需要输入激活码。如果是测试许可证，可以忽略本步骤。在“激活设置”配置区域，输入有效许可证的产品激活码，点击【激活】按钮进行激活（图示3-6-17）；产品激活后该配置区域会自行隐藏。

图示 3-6-17 正式许可证信息

注意：在进行更新许可证或激活码后，需要重启发布服务才能生效；产品激活码具有时效性（许可证签发后的15天内），请在输入前检查激活码是否在有效期内。

3.6.4.5 系统插件

点击控制面板界面的【系统插件】操作项，会跳转至系统插件列表界面，显示当前系统插件列表设置信息（图示3-6-17）。



图示 3-6-17 系统插件列表

iGuard发布服务器上共有四种系统插件，分别在特定的时间节点上，调用指定的lua脚本，完成特定的任务。这类任务一般是特殊的根据用户需求个性化定制的。这四类插件必须配合指定的文件名固定的lua脚本使用。

以下是四种插件的功能和lua脚本说明：

- 日志过滤：对应脚本 “发布服务器安装目录/plugin/lua/log.lua"，在日志生成阶段实现特定任务。
- 文件变化事件过滤：对应脚本 “发布服务器安装目录/plugin/lua/filechange.lua"，对源目录下的文件变化监控时，实现特定任务。
- 同步前通知：对应脚本 “发布服务器安装目录/plugin/lua/presync.lua"，在源目录下的文件结束变化但还未开始上传时，实现特定任务。
- 同步后通知：对应脚本 “发布服务器安装目录/plugin/lua/postsync.lua"，在源目录下的文件已完成同步后，实现特定任务。

举例说明，如需要检查上传文件的内容是否有异样，需要做的步骤包括：

1. 把 “发布服务器安装目录/plugin/lua/_postsync.lua" 脚本文件，改名为postsync.lua；
2. 点击控制面板界面【系统插件】操作项，进入图示3-6-17配置界面；
3. 点击【同步后通知】对应的绿色三角形图标 ▶，启动该插件。
4. 点击红色方块图标 ■ 将停用该插件。

如果 plugin/lua 目录下没有该事件对应的lua脚本，界面上将不会出现绿色三角形启动图标，也就是无法启用该功能项；如果仅在 plugin/lua 目录下，把lua脚本按规定改了名，但没有在这个界面上启动该功能，对应的任务也不会生效。

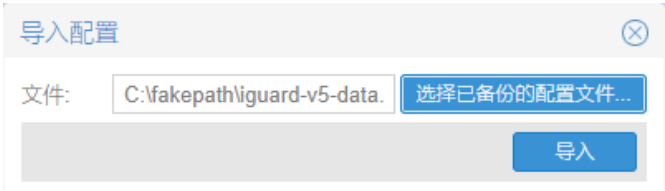
3.7系统维护

3.7.1导出配置

点击左上角的【开始】菜单列表中的【系统维护】→【导出配置】，产生以iguard-v5-data.backup命名的当前配置对应的配置文件，并且被保存到本地。

3.7.2导入配置

点击左上角的【开始】菜单列表中的【系统维护】→【导入配置】，在弹出的导入配置设置框中进行操作，点击【选择已备份的配置文件】按钮，选择对应的配置文件，最后点击【导入】按钮完成操作（图示3-7-1）。



图示 3-7-1 导入配置

3.7.3重启发布服务

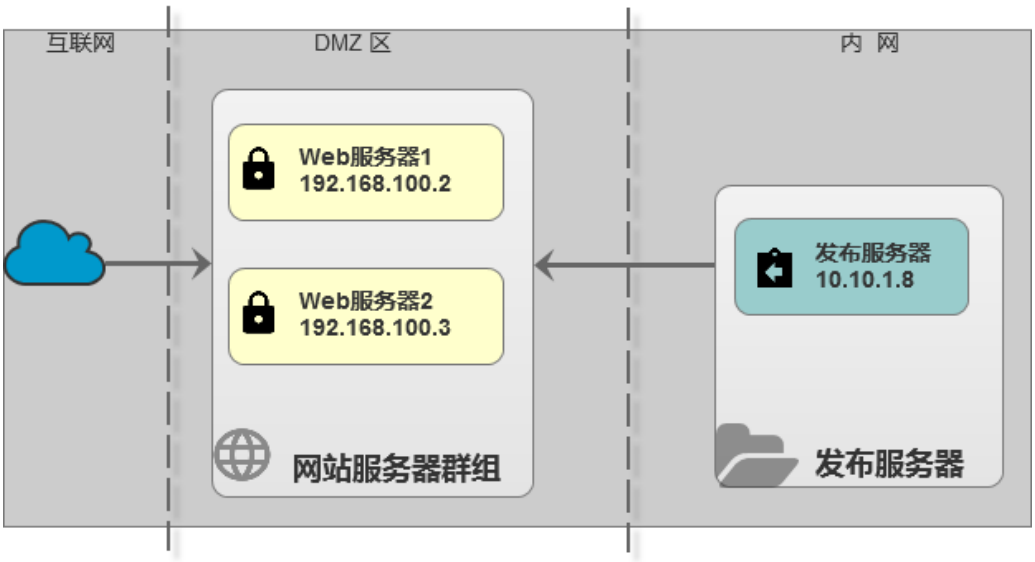
点击左上角的【开始】菜单列表中的【系统维护】→【重启发布服务】，对发布服务系统进行重启操作。

第四章 快速配置向导

4.1 Windows发布服务, Windows网站服务器

本章以下图的拓扑环境为例，介绍常规情况下，发布服务器和网站服务器同时为Windows操作系统的部署步骤。

假设的场景中，用户把发布服务器放在内网IP为10.10.1.8的Windows 2008服务器上；需要防护的两台网站服务器在DMZ区，中间有防火墙隔断，网站服务器也是Windows 2008操作系统。



图示 4-1 系统拓扑

4.1.1 网页备份

由于iGuard需要一份原始文件作为恢复的基准，所以在部署时，需要先把网站服务器（192.168.100.2或192.168.100.3）上的内容全部复制到发布服务器（10.10.1.8）上。备份的几个要点如下：

- 如果网站服务器曾被攻击，应先检查网站内容是否异常，是否仍有残留的网页木马。网站服务器的用户、服务和自启动等关键部位，是否有需要特别留意之处。如有，需要先做细致的清理和加固，再做页面备份。
- 备份到发布服务器的网页内容，可以放在任意目录下，但通常建议选择剩余空间较大的磁盘分区。
- 如果文件数量众多，可以使用FastCopy等工具协助复制。
- 网页备份的步骤并非强制在最开始时执行，但文件数量众多的情况下，强烈建议在安装程序之前首先执行文件备份。因为在文件备份期间，同时可以并行地安装程序。

4.1.2 安装发布服务器

在安装发布服务器前，需要先获得有效的许可证，并确保许可证支持的数量，大于等于当前需要保护的站点数。如在我们的示例中，则至少需要一份支持2套站点的许可。

获得许可证后，在发布服务器上，以管理员身份点击运行“iGuard5-Stagingd-5.XX.exe”。具体安装步骤见本文档【2.1.1发布服务器Windows安装】章节。在安装过程中，准确输入许可证信息。

发布服务器安装完成后，会在操作系统的服务里，新增一项名为“Stagingd5”的服务，确保该服务处于启动状态。

4.1.3 安装同步服务器

由于发布服务器和同步服务器需要进行身份验证，所以需要提前先把发布服务器安装目录（默认安装目录为C:\Tercel\iGuard5\StagingServer）下的staging.id验证文件，复制到两台网站服务器上去。

获得staging.id文件后，在网站服务器（192.168.100.2和192.168.100.3）上，以管理员身份点击运行“iGuard5-igdagent-5.XX.exe”。具体安装步骤详见本文档【2.2.1 同步服务器Windows安装】章节。在安装过程中，需要提供复制过来的staging.id文件的位置。安装同步服务器后的几个要点如下：

- 如果发布服务器和同步服务器不在同一网段，并且两个网段之间有防火墙分隔，需要在防火墙上，开通从发布服务器到同步服务器37777端口的TCP访问。如本例中，需要开通从10.10.1.8到192.168.100.2和192.168.100.3两服务器的37777端口访问。
- 还需要检查同步服务器自身的Windows操作系统是否开启了自带的系统防火墙。如果开启了自带的网络防火墙，还需要开放37777端口的对外服务。
- 同步服务器安装完成后，会在操作系统的服务里，新增两项名为“fcagent”和“igdagent”的服务，确保这两个服务处于启动状态。

4.1.4 登陆Web控制台做各种配置

在客户端机器（通常为管理员的桌面机），打开网页浏览器（建议IE8以上版本，Firefox、Chrome等），访问发布服务器上的Web控制台，具体路径为：https://[发布服务器IP]:39999/。

如本案例中，需要在浏览器中访问https://10.10.1.8:39999/。

如果浏览器无法访问 https://[发布服务器IP]:39999/：

- 请先检查发布服务器10.10.1.8上的Stagingd5服务是否处于启动状态；
- 再检查发布服务器自身操作系统所带的网络防火墙是否打开，如果是，则需要在防火墙中额外允许39999端口的访问；
- 地址栏里的地址是否为https://...开头，是否误为http://...
- 浏览器是否启动了访问代理，访问代理服务器是否可用，是否支持ssl；
- 必要时可以用ping, telnet等工具协助定位问题。

系统默认用户名为admin，密码为iguard。

在控制台里，推荐的初始操作步骤为：

1) 新增需要防护的服务器，具体步骤详见【3.5.2系统配置-服务器】章节的“”新增服务器。如本例中，新增的同步服务器IP为192.168.100.2和192.168.100.3。

2) 新增站点，具体步骤详见【3.5.1系统配置-站点】章节：

- 在站点【路径映射】的“源路径”里，写存放在发布服务器上的备份文件目录；在“目标路径”里，写需要防护的网站在同步服务器端的目录。如果有多条，则分别设定。
- 完成路径映射设定后，再到【关联服务器】里，设定要把这条映射分配给哪几个服务器。如本例中，需要关联上一步骤中设定的192.168.100.2和192.168.100.3服务器。

3) 保存。并在界面的【防护状态】中，查看上述两台服务器的状态是否为【Ok】。

同时，建议立刻修改管理员密码，换掉默认密码。

4.1.5 远程防护配置

iGuardV5.5 有三种防护模式（可以只选择使用其中一种或多种组合）。三种防护模式需要分别配置，要点如下：

4.1.5.1 文件异动检测

点击桌面上的“防护状态”，再选择需要配置的服务器对应【操作】列里的“内置模块”，在可用模块下拉列表里，选择“文件异动检测”。在目录列表框，选择“从站点中导入”按钮，把前面“路径映射”中设定的“目标目录”自动导入为防护目录。也可以不使用“导入”功能，而是手工指定需要防护的目录。该目录为网站服务器（同步服务器）端的物理路径。必须执行这一目录设定操作，否则文件异动检测无效。详见【3.4.2 文件异动检测）】章节。

4.1.5.2 核心内嵌防护

①首先需要对Web端受保护文件进行水印初始化工作，详见【3.4.6水印签发】章节。如果文件实在太多，可以使用命令行方式，效率更高，详见【2.3.1 文件水印初始化】章节。

② 如果有需要忽略的目录，可点击桌面上的“防护状态”，再选择需要配置的服务器对应【操作】列里的“Web模块”，详见【3.4.5 Web模块】章节。

③这一设置完成后，还需要在Web服务器端加载具体的防护模块，详见【2.3防护方式】章节里各种Web服务器的具体步骤。必须在网站服务器端额外地执行加载模块的动作，否则核心内嵌防护无效。

注意：如果上述步骤② 里，点击了“防护状态”->“Web模块”后，没有在系统默认Web服务器类型列表里，找到自己实际使用的Web服务器品种，需要到Web服务器上，编辑修改C:\tercel\iguard5\igdagent\conf\managed.conf 配置文件。如当前配置为：

```
{
"modules":[
 "C:/Tercel/iGuard5/igdagent/modules/iis7_64/mod_iguard5.conf",
 "C:/Tercel/iGuard5/igdagent/modules/jee_64/mod_iguard5.conf",
]
}
```

而实际需要使用的模块是32位的Apache 2.2，则需要修改该文件为： { "modules":["C:/Tercel/iGuard5/igdagent/modules/ap22/mod_iguard5.conf"] }

在Web服务器端保存该文件后，再返回控制台，点击“防护状态”->“Web模块”，重新做忽略配置。

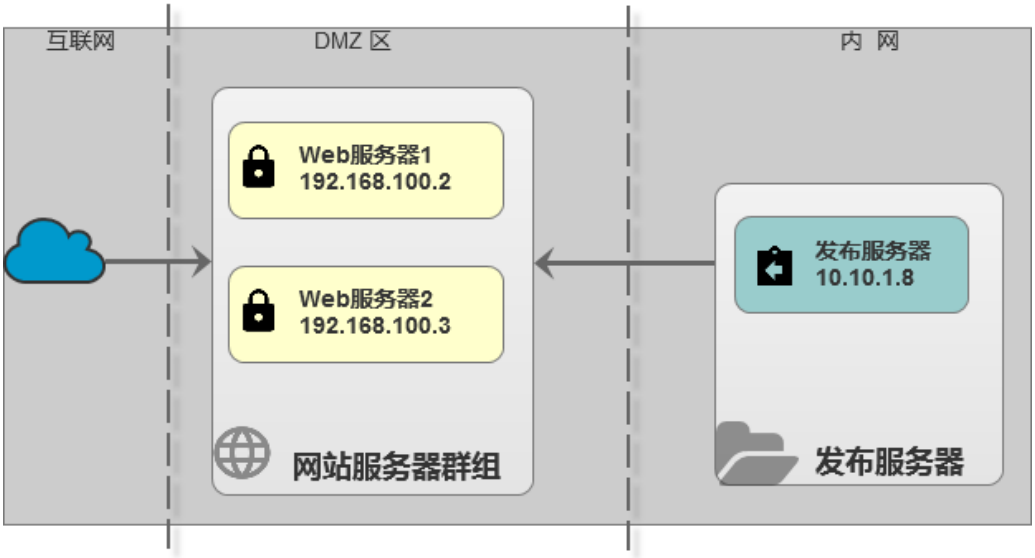
4.1.5.3 定时扫描防护

点击桌面上的“防护状态”，再选择需要配置的服务器对应【操作】列里的“内置模块”，在可用模块下拉列表里，选择“定时扫描计划”。点击 添加按钮，在目录列表框，选择“导入”，把前面“路径映射”中设定的“目标目录”自动导入为定时扫描目录，具体操作详见【3.4.1 内置模块（定时扫描计划）】章节。必须执行这步操作，否则定时扫描防护无效。

4.2 Linux发布服务, Linux网站服务器

本章以下图的拓扑环境为例，介绍常规情况下，发布服务器和网站服务器同时为 Linux 操作系统的部署步骤。

假设的场景中，用户把发布服务器放在内网IP为10.10.1.8的Linux 服务器上；需要防护的两台网站服务器在DMZ区，中间有防火墙隔断，网站服务器也是 Linux 操作系统。



图示 4-2 系统拓扑

4.2.1 网页备份

由于iGuard需要一份原始文件作为恢复的基准，所以在部署时，需要先把网站服务器（192.168.100.2或192.168.100.3）上的内容全部复制到发布服务器（10.10.1.8）上。备份的几个要点如下：

- 如果网站服务器曾被攻击，应先检查网站内容是否异常，是否仍有残留的网页木马。网站服务器的用户、服务和自启动等关键部位，是否有需要特别留意之处。如有，需要先做细致的清理和加固，再做页面备份。
- 备份到发布服务器的网页内容，可以放在任意目录下，但通常建议选择剩余空间较大的磁盘分区。 在选择具体位置之前， 可以先输入以下命令，查看各分区剩余空间，确定备份目录具体位置：

```
# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/VolGroup-lv_root 14G 11G 2.1G 85% /
tmpfs 940M 0 940M 0% /dev/shm
/dev/sda1 477M 40M 412M 9% /boot
```

- 如果需要先打包再备份，可以执行以下命令，获得打包后的文件 backup_file.tar，把该文件传到发布服务器即可 ：

```
# tar cvf backup_file.tar /备份目录
```

而在发布服务器端，则执行以下命令做解压：

```
# tar xvf backup_file.tar
```

- 网页备份的步骤并非强制在最开始时执行，但文件数量众多的情况下，强烈建议在安装程序之前首先执行文件备份。因为在文件备份期间，同时可以并行地安装程序。

4.2.2 安装发布服务器

在安装发布服务器前，需要先获得有效的许可证，并确保许可证支持的数量，大于等于当前需要保护的站点数。如在我们的示例中，则至少需要一份支持2套站点的许可。另外发布服务器是Linux操作系统时，一定要获得支持 Linux 发布功能的许可证。

获得许可证后，在发布服务器上，先确认操作系统版本和内核，再决定采用哪个安装程序。

获得内核版本的命令如下：

> **# uname -an**
> **Linux localhost.localdomain 2.6.32-358.el6.x86_64 #1 SMP Fri Feb 22 00:31:26 UTC 2013 x86_64 x86_64 x86_64 GNU/Linux**

获得发行版信息的命令如下：

> **# lsb_release -a**
> **LSB Version: :base-4.0-amd64:base-4.0-noarch:core-4.0-amd64:core-4.0-noarch:graphics-4.0-amd64:graphics-4.0-noarch:printing-4.0-amd64:printing-4.0-noarch**
> **Distributor ID: CentOS**
> **Description: CentOS release 6.8 (Final)**
> **Release: 6.8**
> **Codename: Final**

获得硬件架构位数的命令如下：

> **# arch**
> **x86_64**

如我们的例子中，结合内核版本数字和硬件架构位数，选用的安装程序为 iGuard5-stagingd-Linux-2.6.32-71.el6.x86_64-XXXXX.tar.gz。具体安装步骤见本文档【2.1.2 发布服务器Linux安装】章节，默认安装路径为 /usr/local/iguard5/stagingd 。

发布服务器安装完成后，还需要手工在自启动文件里添加自启动项。如编辑 /etc/rc.local 文件，加入以下这句：

```
/usr/local/iguard5/stagingd/admtool start
```

发布服务器安装完成后，执行以下命令启动服务：

> **# cd /usr/local/iguard5/stagingd**
>
> # ./admtool start

会在操作系统的服务里，新增两项stagingd进程，说明启动成功。

如果执行了以上启动命令，仍然无法访问 https://发布服务器ip:39999/ 控制台站点，则需要检查发布服务器自身 Linux 操作系统是否开启了自带的系统防火墙。如果开启了自带的网络防火墙，还需要开放37777端口的对外服务。具体步骤是，编辑 /etc/sysconfig/iptables，加入以下一行

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 39999 -j ACCEPT
```

然后重启系统防火墙：

> **# service iptables restart**

4.2.3 安装同步服务器

由于发布服务器和同步服务器需要进行身份验证，所以需要提前先把发布服务器 staging.id 验证文件（默认路径 /usr/local/iguard5/stagingd/staging.id），复制到两台网站服务器上去。

获得staging.id文件后，在网站服务器（192.168.100.2和192.168.100.3）上，也需要先确认内核版本数字和硬件架构位数，再选用合适的安装程序。具体安装步骤见本文档【2.1.2 发布服务器Linux安装】章节，默认安装路径为 /usr/local/iguard5/igdagent 。在安装过程中，需要提供复制过来的staging.id文件的位置。安装同步服务器后的几个要点如下：

- 如果发布服务器和同步服务器不在同一网段，并且两个网段之间有防火墙分隔，需要在防火墙上，开通从发布服务器到同步服务器37777端口的TCP访问。如本例中，需要开通从10.10.1.8到192.168.100.2和192.168.100.3两服务器的37777端口访问。

- 需要检查同步服务器自身 Linux 操作系统是否开启了自带的系统防火墙。如果开启了自带的网络防火墙，还需要开放37777端口的对外服务。具体步骤是，编辑 /etc/sysconfig/iptables，加入以下一行

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 37777 -j ACCEPT
```

然后重启系统防火墙：

> **# service iptables restart**

- 同步服务器安装完成后，执行以下命令启动服务：

> **# cd /usr/local/iguard5/igdagent**
> **# ./admtool start**

- 会在操作系统的服务里，新增两项igdagent进程，说明启动成功。
- 另外也需要手工在自启动文件里添加自启动项。如编辑 /etc/rc.local 文件，加入以下这句：

```
/usr/local/iguard5/igdagent/admtool start
```

4.2.4 登陆Web控制台做各种配置

在客户端机器（通常为管理员的桌面机），打开网页浏览器（建议IE8以上版本，Firefox、Chrome等），访问发布服务器上的Web控制台，具体路径为：https://[发布服务器IP]:39999/。

如本案例中，需要在浏览器中访问 https://10.10.1.8:39999/。

如果浏览器无法访问 https://[发布服务器IP]:39999/：

- 请先检查发布服务器10.10.1.8上的Stagingd5服务是否处于启动状态；
- 再检查发布服务器自身操作系统所带的网络防火墙是否打开，如果是，则需要在防火墙中额外允许39999端口的访问；
- 地址栏里的地址是否为https://...开头，是否误为http://...
- 浏览器是否启动了访问代理，访问代理服务器是否可用，是否支持ssl；
- 必要时可以用ping, telnet等工具协助定位问题。

系统默认用户名为admin，密码为iguard。

在控制台里，推荐的初始操作步骤为：

1) 新增需要防护的服务器，具体步骤详见【3.5.2系统配置-服务器】章节的“新增服务器”。如本例中，新增的同步服务器IP为192.168.100.2和192.168.100.3。

2) 新增站点，具体步骤详见【3.5.1系统配置-站点】章节：

- 在站点【路径映射】的“源路径”里，写存放在发布服务器上的备份文件目录；在“目标路径”里，写需要防护的网站在同步服务器端的目录。如果有多条，则分别设定。
- 完成路径映射设定后，再到【关联服务器】里，设定要把这条映射分配给哪几个服务器。如本例中，需要关联上一步骤中设定的192.168.100.2和192.168.100.3服务器。

3) 保存。并在界面的【防护状态】中，查看上述两台服务器的状态是否为【Ok】。

同时，建议立刻修改管理员密码，换掉默认密码。

4.2.5 远程防护配置

iGuardV5.5 有三种防护模式（可以只选择使用其中一种或多种组合）。三种防护模式需要分别配置，要点如下：

4.2.5.1 核心内嵌防护

①首先需要对Web端受保护文件进行水印初始化工作，详见【3.4.6水印签发】章节。如果文件实在太多，可以使用命令行方式，效率更高，详见【2.4.1 文件水印初始化】章节。

② 如果有需要忽略的目录，可点击桌面上的“防护状态”，再选择需要配置的服务器对应【操作】列里的“Web模块”，详见【3.4.5 Web模块】章节。

③这一设置完成后，还需要在Web服务器端加载具体的防护模块，详见【2.3防护方式】章节里各种Web服务器的具体步骤。必须在网站服务器端额外地执行加载模块的动作，否则核心内嵌防护无效。

注意：如果上述步骤② 里，点击了“防护状态”->“Web模块”后，没有在系统默认Web服务器类型列表里，找到自己实际使用的Web服务器品种，需要到Web服务器上，编辑修改/usr/local/iguard5/igdagent/conf/managed.conf 配置文件。如当前配置为：

```
{
"modules":[
 "/usr/local/iguard5/igdagent/modules/ap22/mod_iguard5.conf",
 "/usr/local/iguard5/igdagent/modules/jee/mod_iguard5.conf",
]
}
```

而实际需要使用的模块是Nginx模块，则需要修改该文件为：

```
{
"modules":[
 "/usr/local/iguard5/igdagent/modules/nginx/mod_iguard5.conf"
]
}
```

在Web服务器端保存该文件后，再返回控制台，点击“防护状态”->“Web模块”，重新做忽略配置。

4.2.5.2 iLocker防护模式

详见【2.4.6 Linux iLocker 拦截模式）】章节和【2.4.7 Linux iLocker 自动恢复）】章节。

4.2.5.3 定时扫描防护

点击桌面上的“防护状态”，再选择需要配置的服务器对应【操作】列里的“内置模块”，在可用模块下拉列表里，选择“定时扫描计划”。点击 添加按钮，在目录列表框，选择“导入” ，把前面“路径映射”中设定的“目标目录”自动导入为定时扫描目录，具体操作详见【3.4.1 内置模块（定时扫描计划）】章节。必须执行这步操作，否则定时扫描防护无效。

4.3 各种自定义微调

4.3.1 特定文件/目录的自动上传过滤

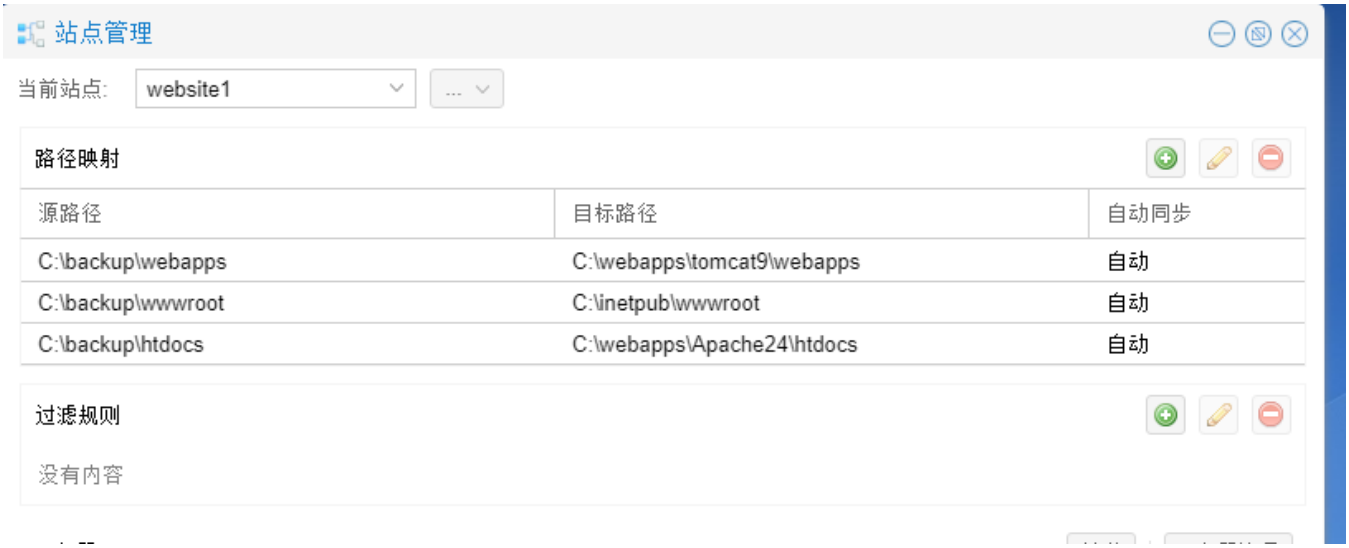
iGuardV5可以根据文件名模式，灵活地设定哪些文件无需自动上传至网站服务器端。文件名模式可以匹配到单个具体文件、单个目录下的所有文件以及不同目录下的相似规律文件。再通过多条策略的灵活组合，能实现各种不同需求。

场景1：不需要自动上传特定目录下的某些文件

如最常见的情况是，网站目录下的某些临时文件、日志文件和计数器文件，并不需要自动上传到网站端。他们的物理路径如下：

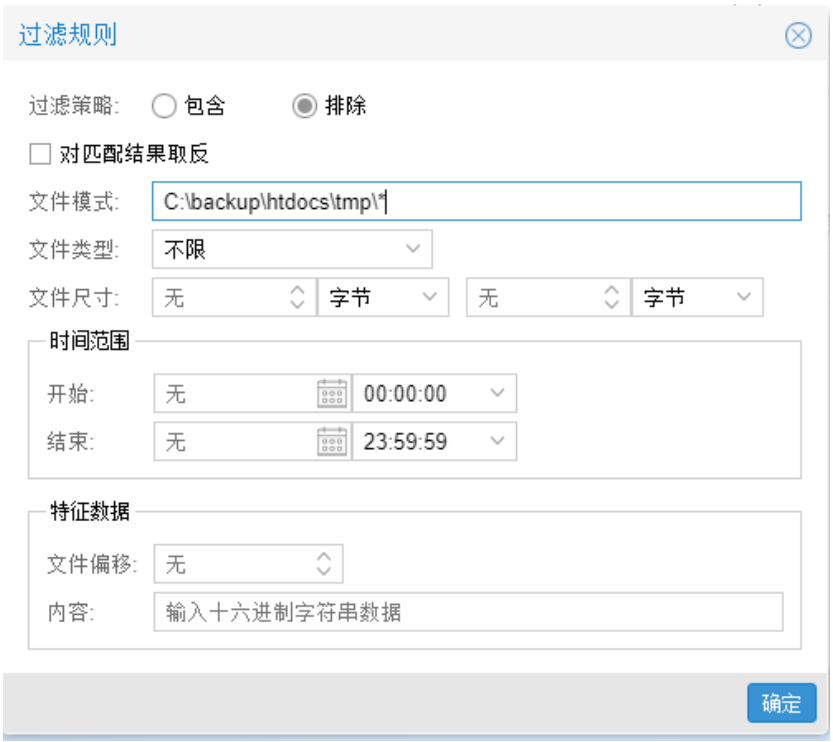
- C:\backup\htdocs\tmp 目录下的所有文件都是临时文件，不需要上传
- C:\backup\htdocs\logs 目录下后缀为.log的日志文件
- C:\backup\wwwroot\count.dat 固定的计数器文件

操作为：首先点击【开始】->【同步管理】->【站点管理】，在相应站点的【过滤策略】里（如图示4-2）



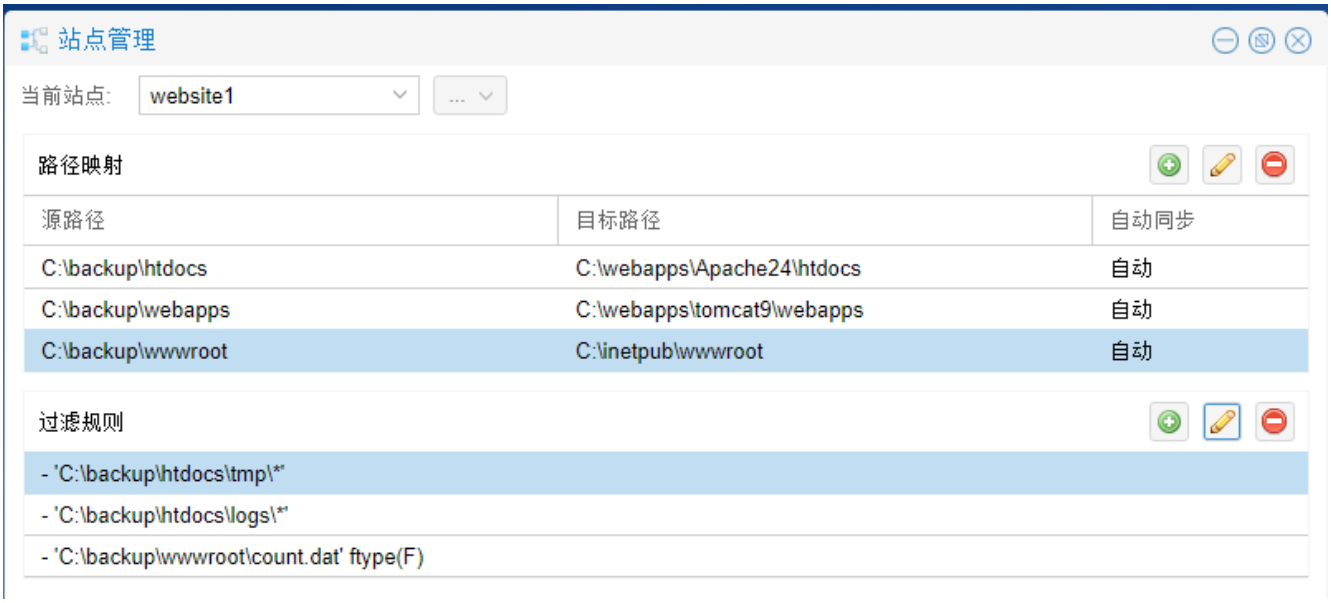
图示 4-2 设置全站过滤策略

在右侧的一排快捷图标 里，选择【新增】 图标，在“过滤策略”里，选择“排除”，文件模式里填入具体文件名，可以使用*和?符号做文件名模式匹配，如图示。



图示 4-3 设置单条过滤策略

根据以上具体需求，逐一填入需要忽略3条过滤策略，得到最后的过滤列表，如图示。



图示 4-4 各种文件名过滤策略组合

最后点击【保存】即可。这3类模式的文件将不会再自动上传。

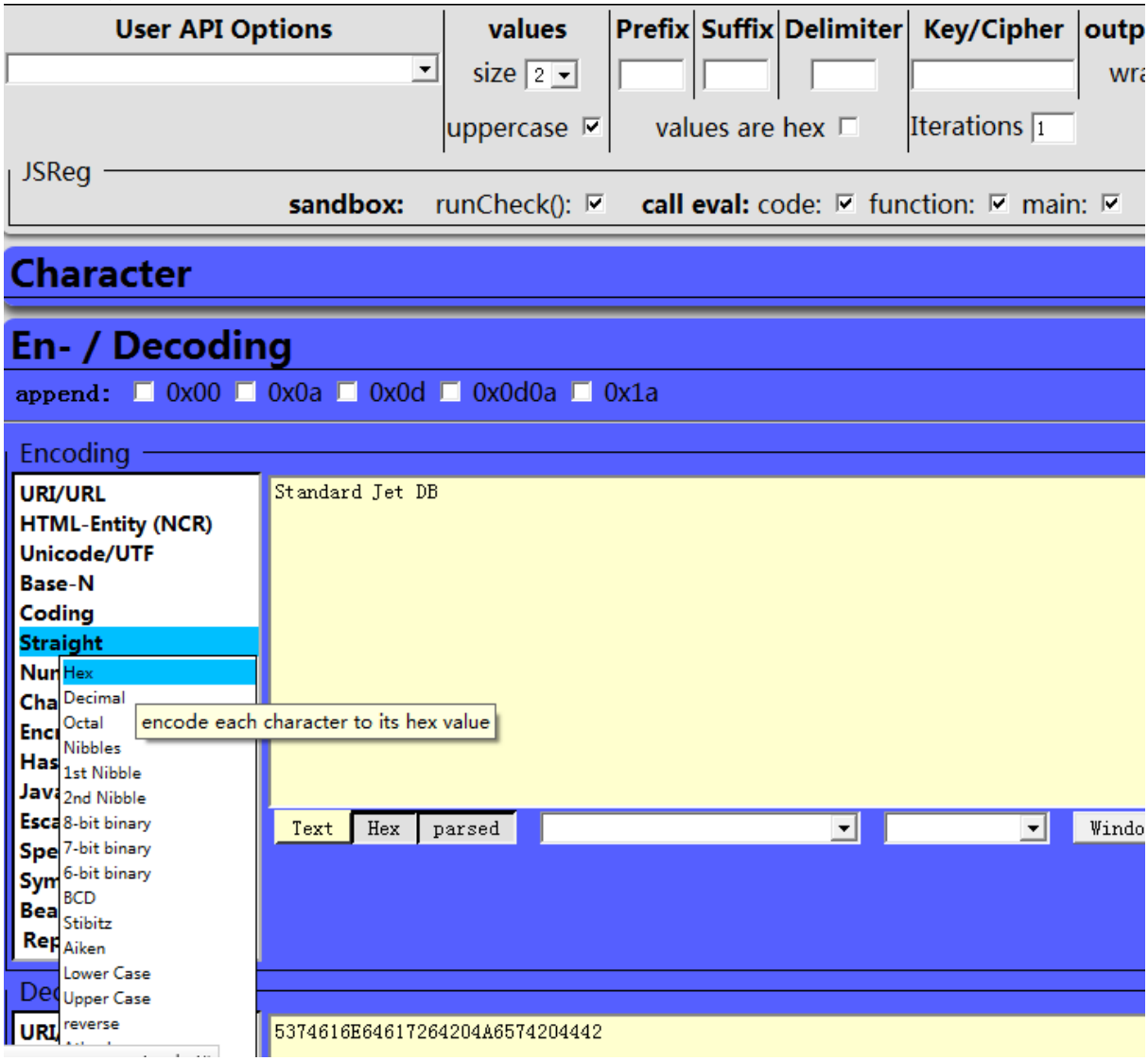
场景2：不需要上传有特定内容模式的文件

如最常见的情况是，某些Microsoft Access数据库格式的文件，原本后缀名为.mdb，但为了防止被下载，已改名为.asa文件。而且这类文件分布在网站的各个子目录下，并无特定规律，无法用文件名模式匹配出来，这时候就需要根据文件的具体内容进行过滤了。

这类.mdb文件的特点为，在文件开头的第5个字节开始，必然包含着“Standard Jet DB”字符串。由于iGuardV5的内容过滤是16进制编码的，所以需要先把这段字符串转成16进制编码。方法如下：

- 用浏览器访问http://app.tcxa.com.cn/ende/；

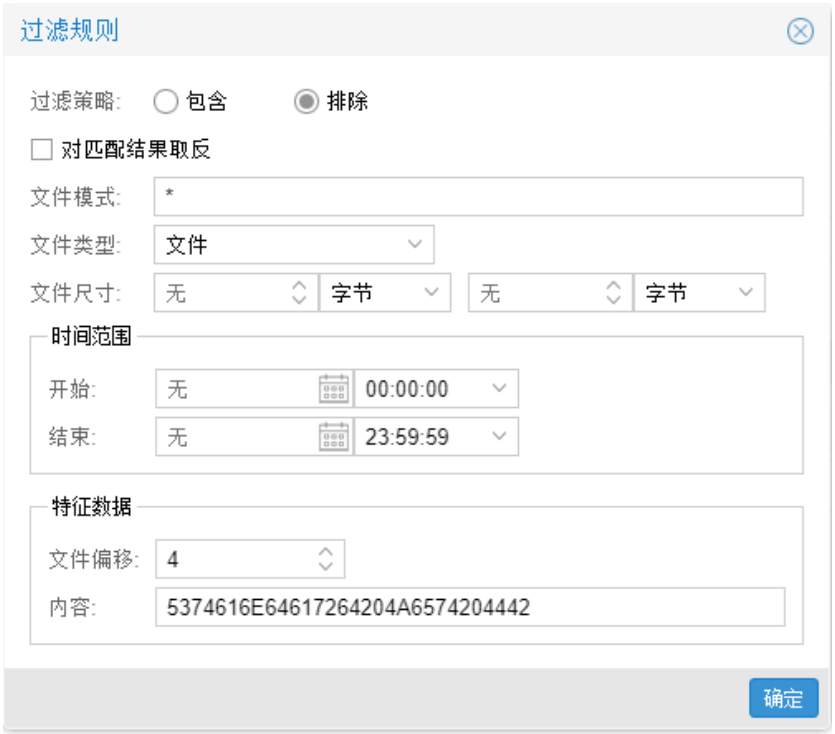
- 在Encoding框内填入“Standard Jet DB” （图示4-5）；



图示 4-5 获得字符串的16进制编码值

- 在页面上方的“Use API Options”中，“User API Options”为空；“values”为2；“Prefix”、“Suffix”和“Delimiter”全部为空；
- 在左侧Encoding里选择“Straight“->“Hex” 16进制编码；
- 最后，在下方的“Decoding”框内，出现了该字符串的完整16进制编码：“5374616E64617264204A6574204442”。

把这段编码复制下来。回到iGuardV5控制台中。首先点击【开始】->【同步管理】->【站点管理】，在相应站点的【过滤策略】里，再点击“新增”图标，按以下内容填入具体的过滤策略。“过滤策略”为“排除”；文件模式“*”代表所有文件；“偏移”值为“4”（从第5个字节开始匹配）；“特征”为这串16进制特征码，如图示4-6。最后点击“保存”。

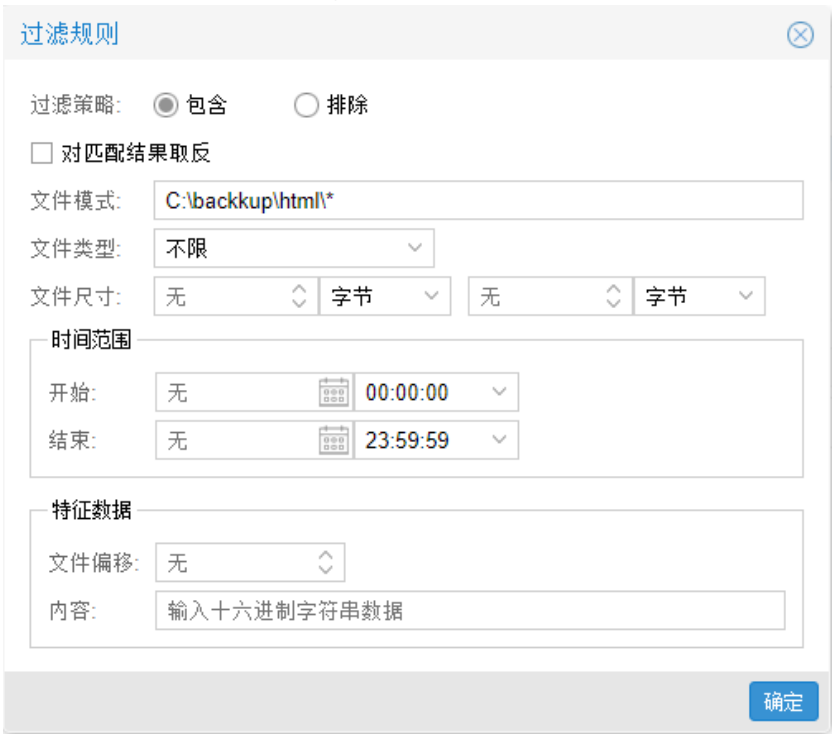


图示 4-6 根据文件内容配置过滤策略

场景3：在整个大目录下，只有部分文件需要自动上传，其他文件全部不要自动上传

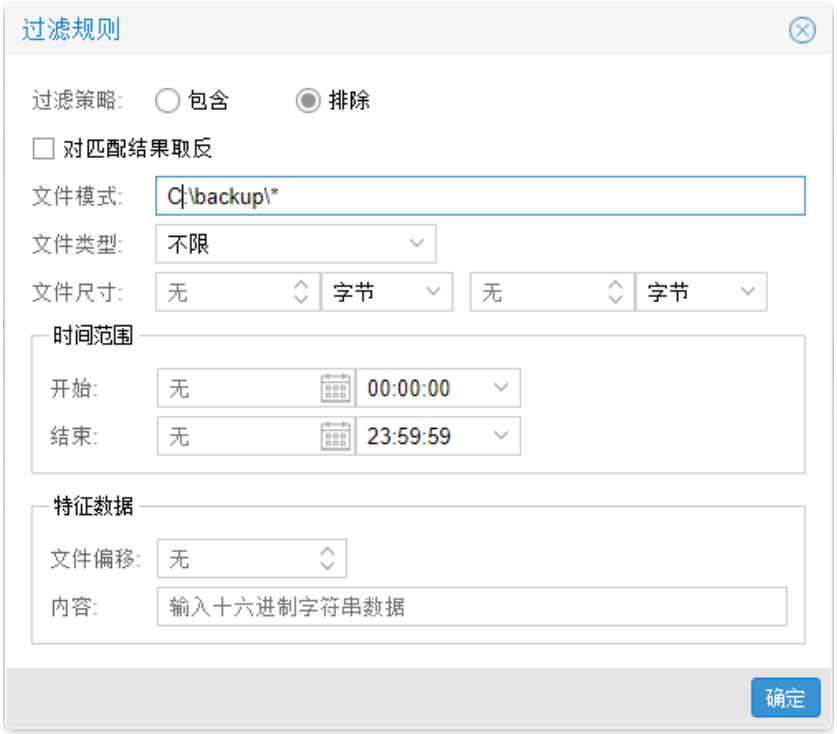
源目录为C:\backup，在这个总的目录下，有许多二级子目录，其中只有html和images两个子目录需要自动同步，其他一律不需要自动同步。

首先点击【开始】->【同步管理】->【站点管理】，在相应站点的过滤选项里，选择过滤策略为“包含”，在文件模式里，分别填入“C:\backup\html*”和“C:\backup\images*”，代表这两个目录需要做自动同步，如图示4-7。



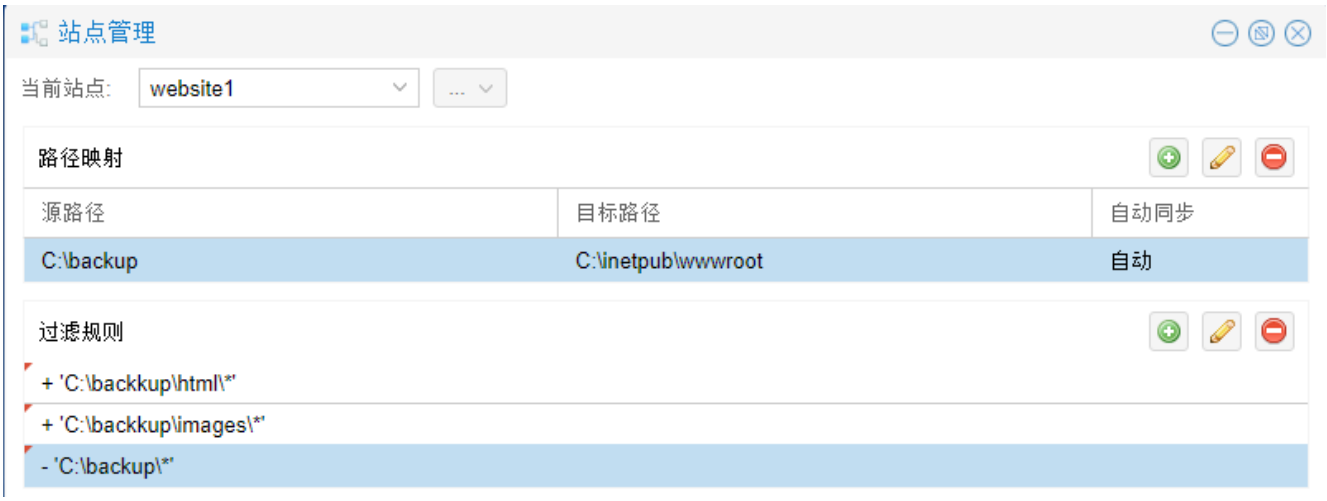
图示 4-7 设置子目录的自动上传

最后，再多加一条“过滤策略”为“排除”的选项，设置最上一级的目录不需要做自动上传，如图示4-8。



图示 4-8 去除最上层目录的自动上传

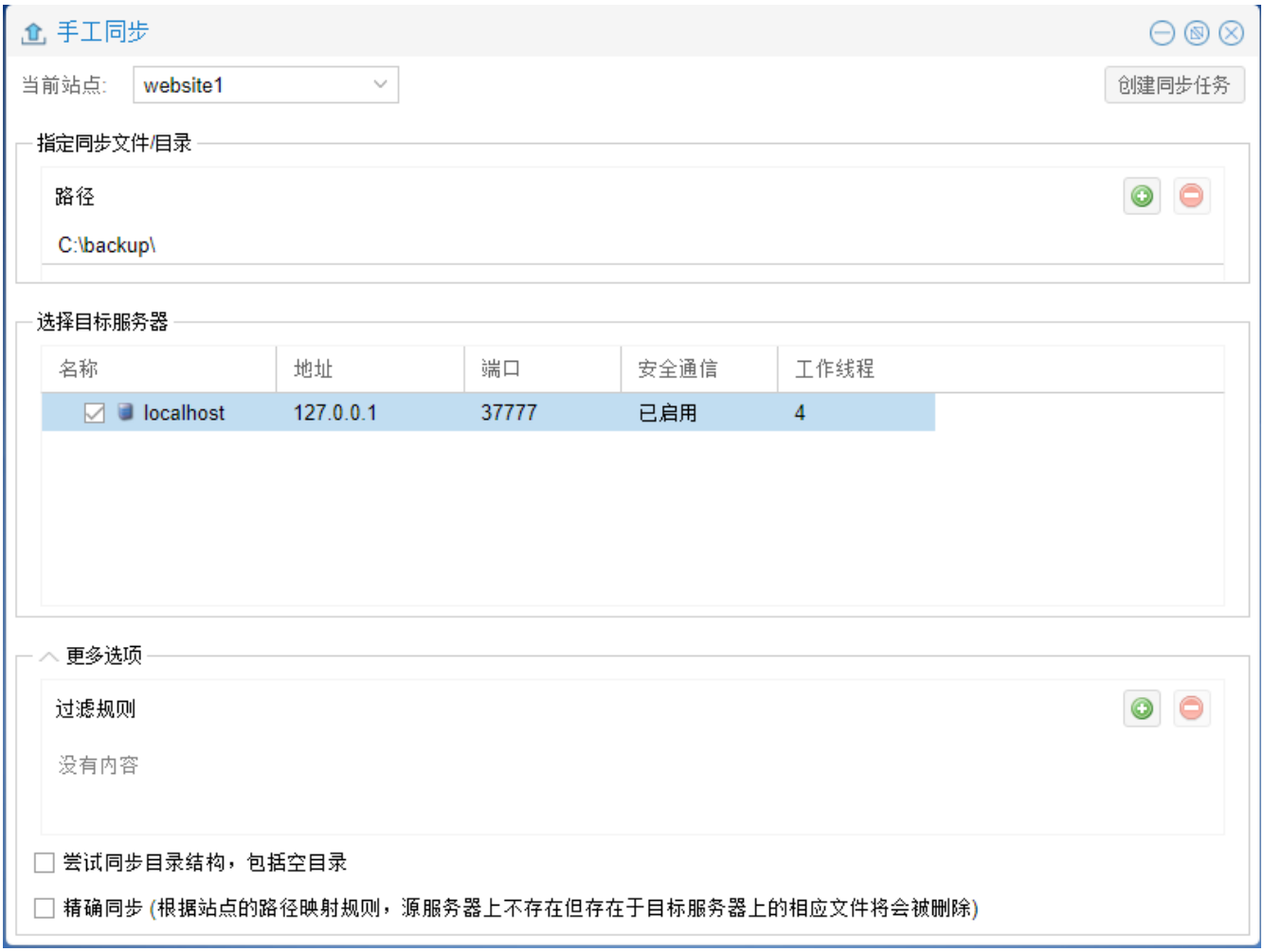
最后得到完整的过滤列表如图示4-9，点击“保存”完成设置。由于过滤策略遵照从上到下的优先级匹配，所以最长最深的目录级别应该写在最上面，最短的写在最底层。过滤策略里，前面为“+” 加号的，为需要自动同步的目录，前面为“-”减号的，则不需要同步。



图示 4-9 完整的过滤策略列表

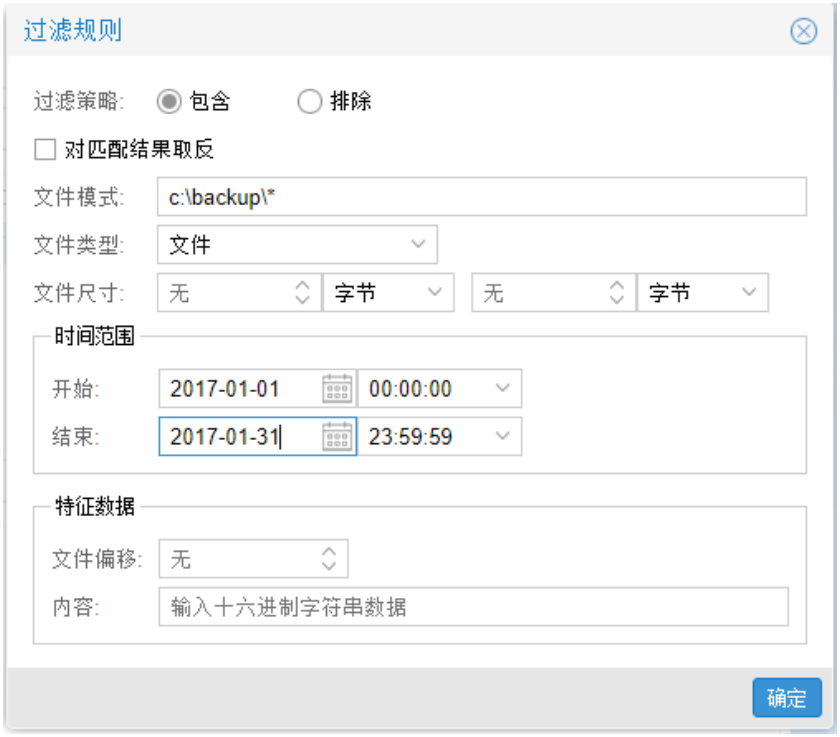
4.3.2 特定文件/目录的手工上传过滤

场景1：选择只上传特定时间段内产生的文件 如对源目录C:\backup，只希望手工上传该目录下2017年1月份内产生的全部文件。 首先点击【开始】->【同步管理】->【手工同步】，先选定相关的站点，再选择【指定同步文件/目录】里的需要手工同步的路径，再选择【选择目标服务器】，最后点击下方的【更多选项】下拉菜单，展示详尽选项的设置，如图示4-10：



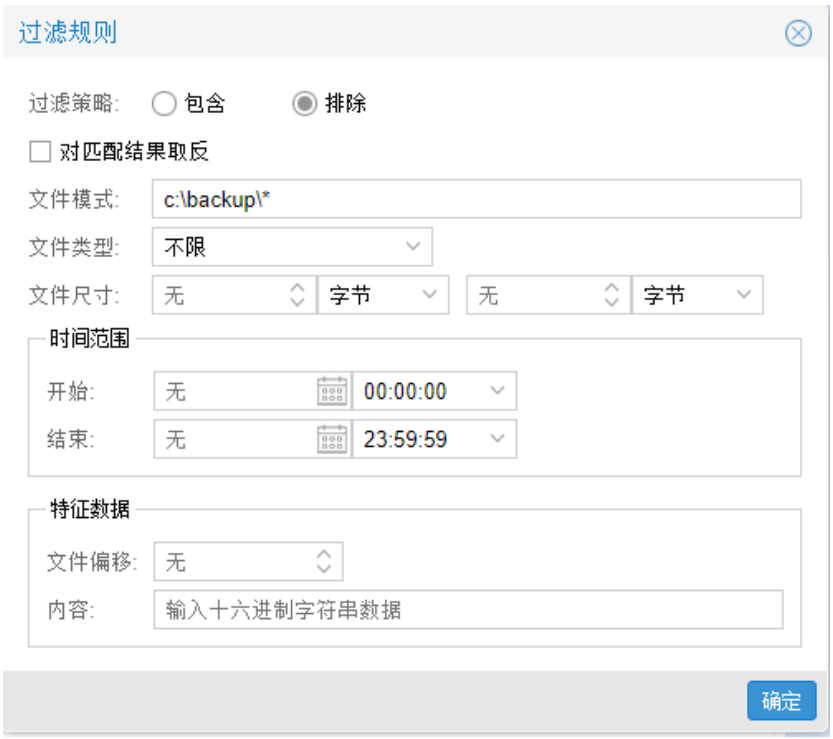
图示 4-10 手工同步的【更多选项】

在【更多选项】的【过滤策略】里，根据需求增加额外的过滤策略。如设定只同步2017年1月份时段的文件，先点击“新增”图标，过滤策略设为【包含】，“文件类型”里选择“文件”，再设定“时间节点”范围，具体如图示4-10。



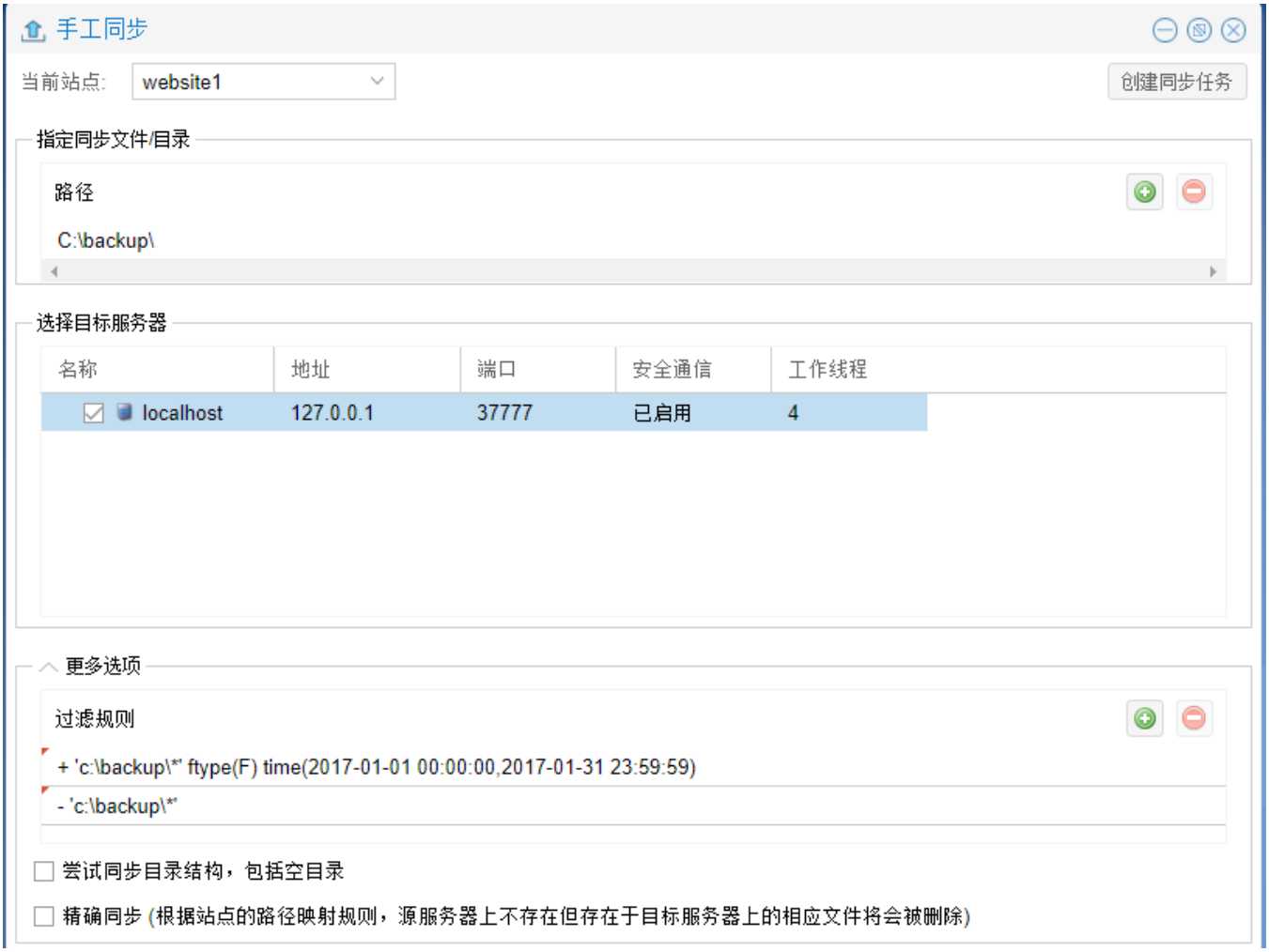
图示 4-10 只同步特定时段的文件上传

由于默认是同步全部文件的，所以还需要额外设置一条排除其他所有文件上传的规则。点击“新增”图标，过滤策略设为【排除】，如图示4-11。



图示 4-11 排除其他文件的上传

这样总体的规律规则如图示4-12。完成后点击右上方的【创建同步任务】按钮即可。



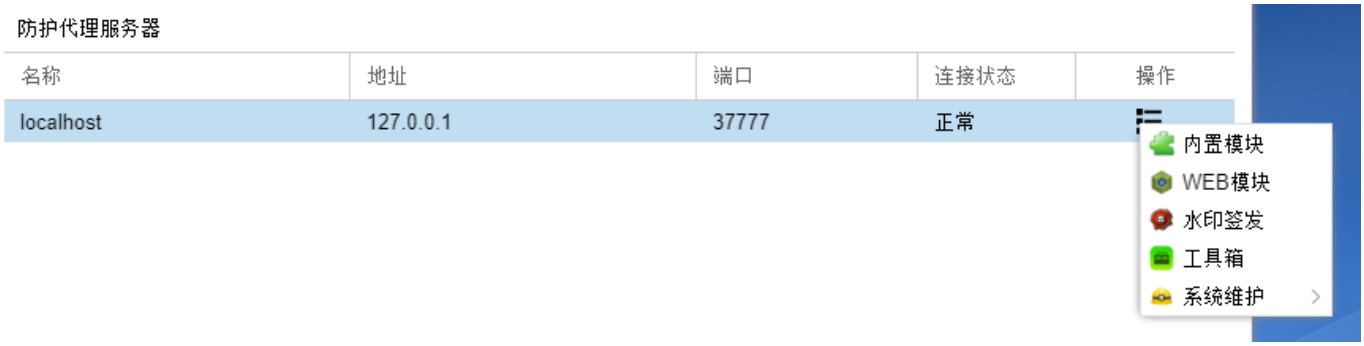
图示 4-12 过滤特定时间段内的文件上传

4.3.3 对文件异动检测，放开对特定文件/目录的防护

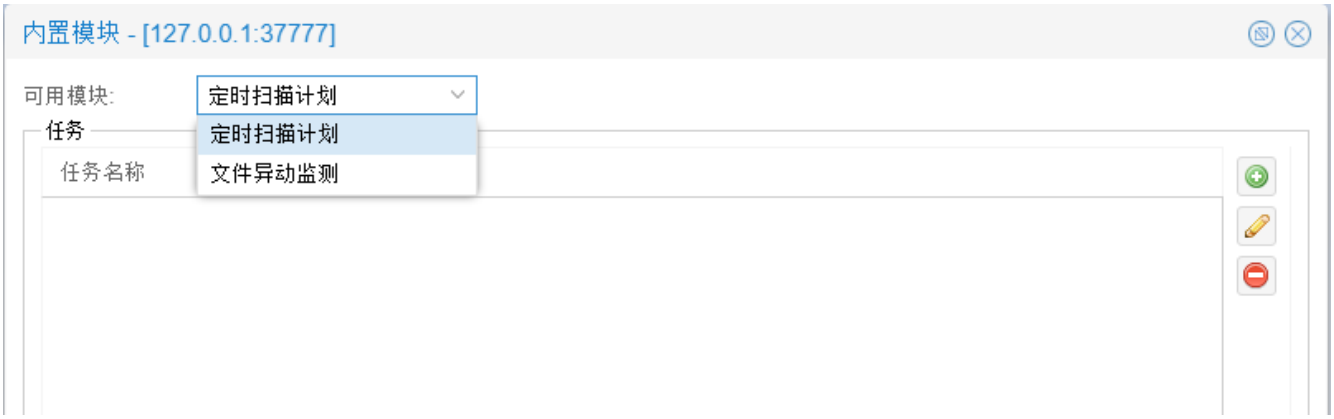
场景1：不需要保护特定的目录/文件

最常见的情况是，网站目录下的某些上传目录需要直接更新特定类型的文件，如jpg、gif和zip等，但这类目录往往也是藏污纳垢之所，所以只能放开特定类型文件的访问，而对敏感的脚本类型文件，如asp、php、asa和jsp等，则不应允许访问。

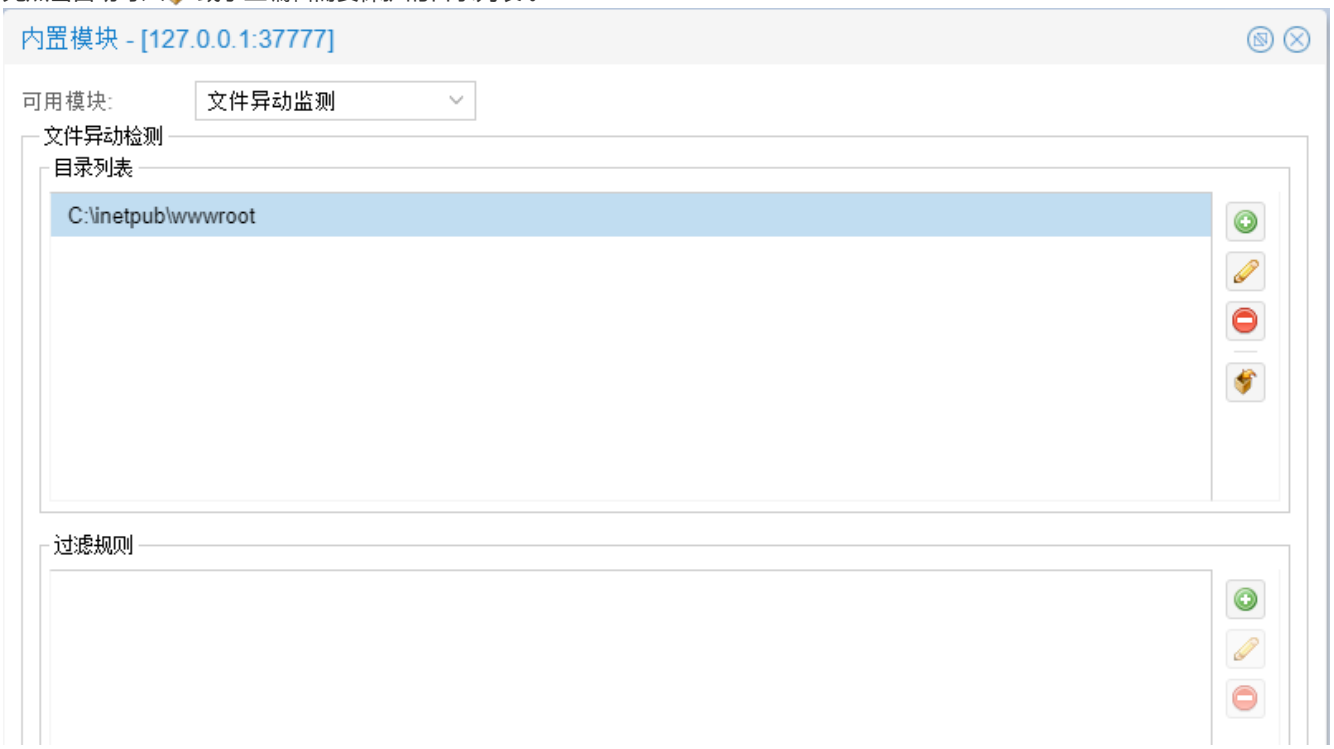
根据此需求，点击桌面上的快捷【防护状态】，再选择需要配置的服务器对应的“内置模块”



在内置模块列表里，再选择【文件异动监测】。



先点击自动导入 或手工编辑需要保护的目录列表 。



再点击“新增”按钮，在【过滤策略】项目中，设置“过滤策略”为“包含”，限定上传目录下的asp*文件是需要防护的，其他相似的脚本文件也类似地处理，如图4-13。

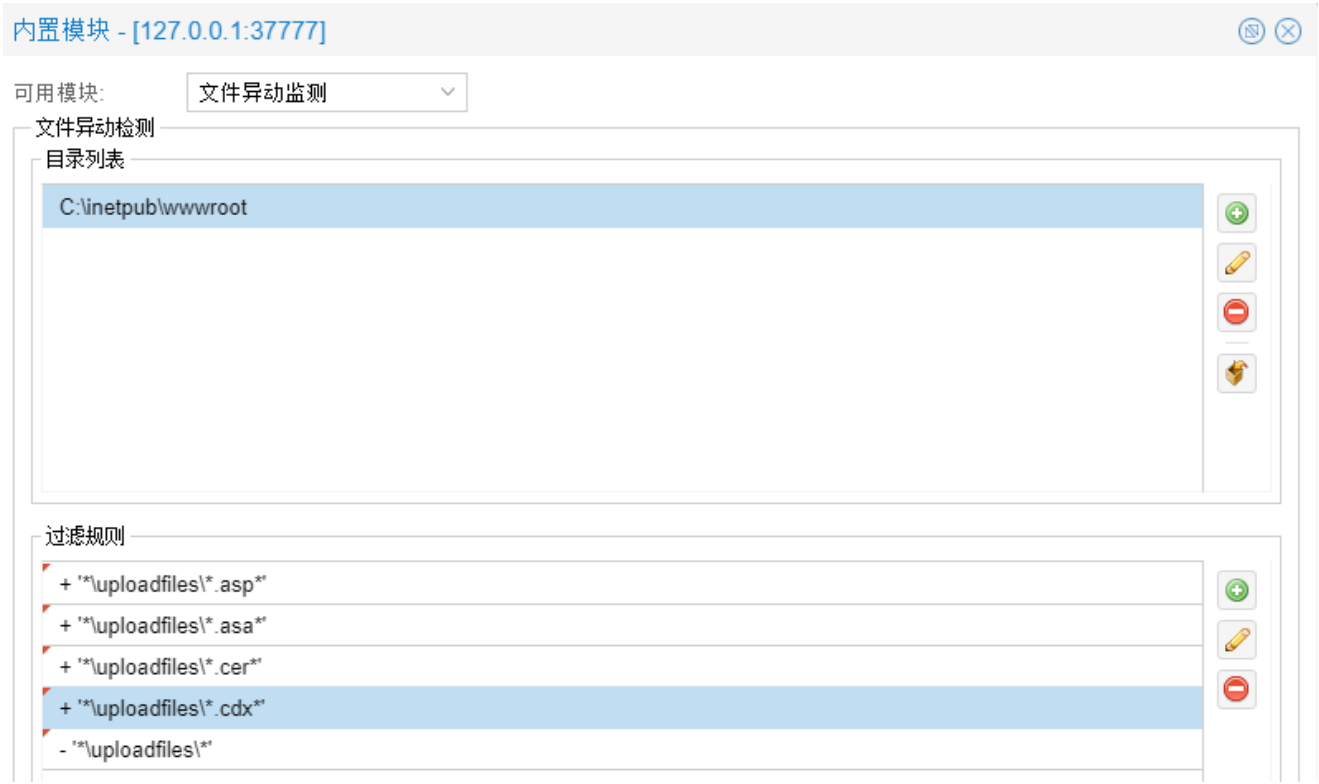
图示 4-13 需要进行文件异动检测防护的特定文件（受保护）

一般而言，在同一个目录下，既需要限制某类文件的生成，又需要放开另一类文件时，一定要先设置“受保护”的文件过滤，安全性更高些。

完成“受保护”类型文件的设置后，再对除普通文件做例外设置（注意：此时“过滤策略”应选择“排除”），如图示4-14。这类过滤策略为“排除”的文件，将不受文件异动检测防护，即可以随意产生，无需从源端上传。

图示 4-14 不需要进行文件异动检测防护的特定文件（不受保护）

总的过滤策略列表如图示4-15。前面符号为加号“+”的，是选择了“过滤策略”为“包含”的文件模式（受保护）；前面符号为减号“-”的，则是“过滤策略”为“排除”的文件模式（不受保护）。



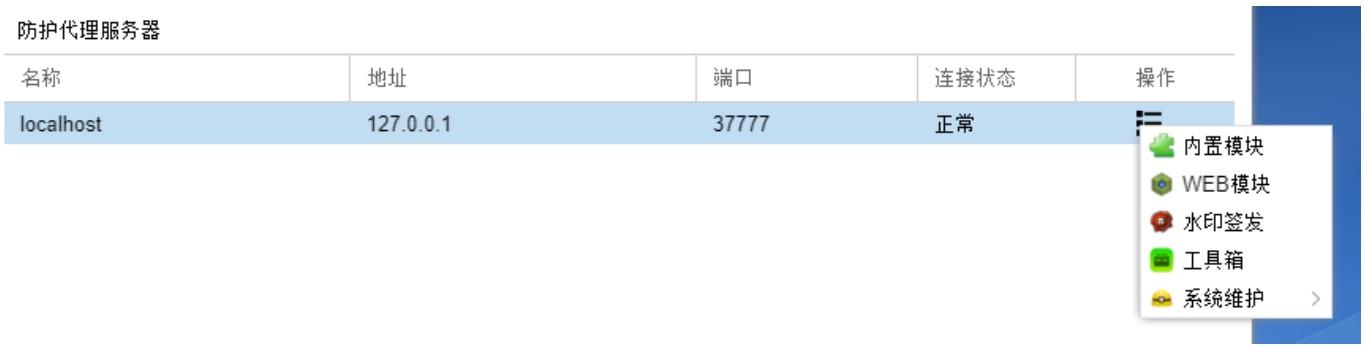
图示 4-15 完整的过滤策略列表

4.3.4 对核心内嵌模块，放开对特定文件/目录的防护

场景1：不需要保护特定的目录/文件 默认情况下，Web服务器里加载了防篡改模块后，将只认可从发布服务器传到Web服务器相应目录的文件。这一途径之外的任何修改都会被认为是非法的。如果确实有必要，如一些临时文件、计数器文件和Access数据库文件等，确实不需要防护的，可以做例外忽略。他们的物理路径如下：

- D:\webroot\tmp 目录下的所有文件都是临时文件
- D:\webroot\logs 目录下后缀为.log的日志文件
- D:\webroot\db\count.dat 固定的计数器文件

根据此需求，点击桌面上的快捷【防护状态】，再选择需要配置的服务器对应的“Web模块”，如图示4-16。



图示 4-16 选择服务器对应的Web模块项

根据自己的实际情况，在【可用模块】里，选择合适的Web模块，如图示中的“IIS7-x86_64”模块。

在【关于受保护的文件过滤规则】分类中，依次分别点击 “新增”按钮  ，如下设置每一条“排除”策略，得到如图示4-17列表，最后点击“保存”。

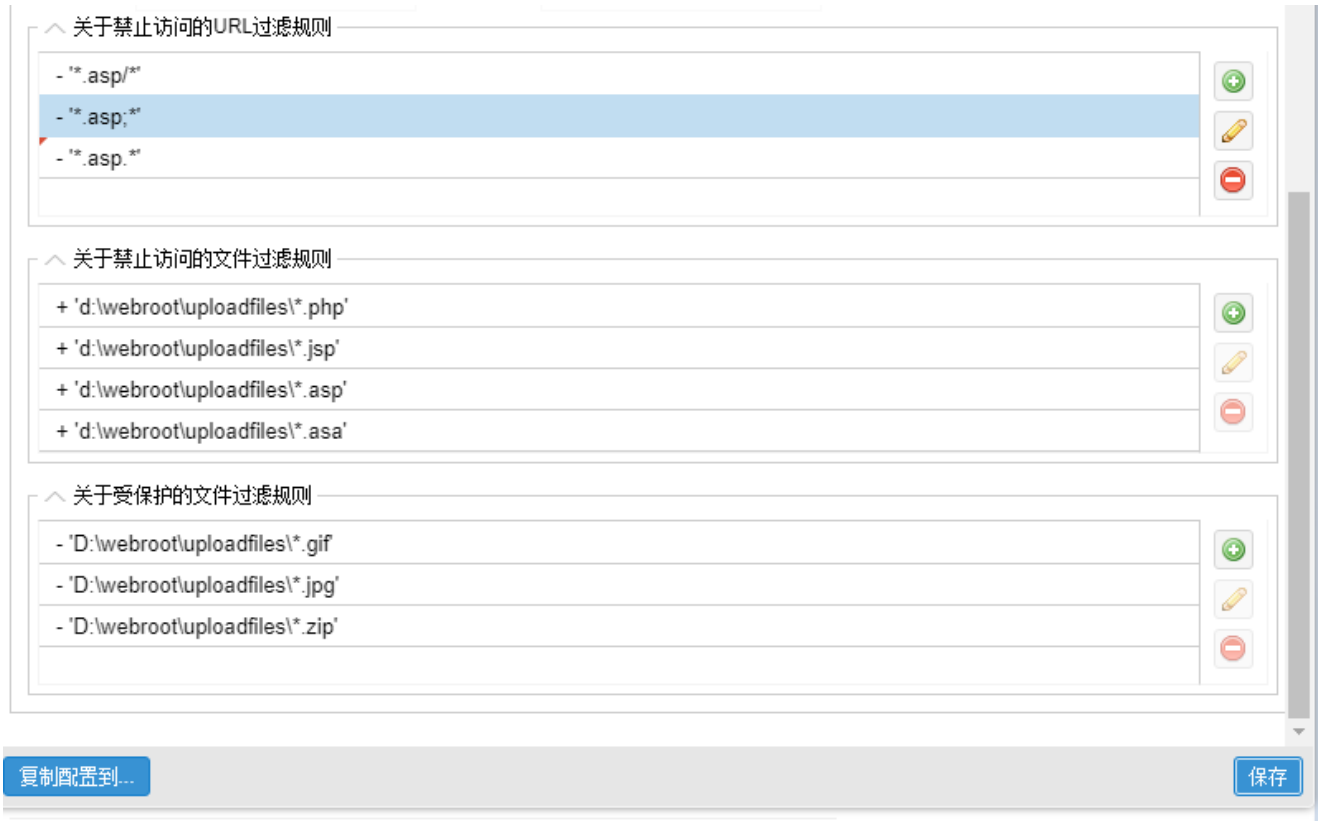
图示 4-17 无需保护的文件规则列表

场景2：同一个目录下，既有不需要保护的文件，也有绝对不应该出现的文件。

典型场景如网站的上传目录。这部分目录下的文件一般无法从源端的相应目录上传，而这类上传目录又是最容易出现问题的位置，所以应该做好充分的防护。这些上传目录下存放的文件一般分两类：

- 无害的纯静态文件：如gif,jpg,zip,mp3,rar等类型；
- 有害的脚本文件：如asp,aspx,php,jsp等；
- 有害的伪造成静态文件的脚本文件：如.asp;.gif，/2.asp/3.jpg等模式的文件。

根据此需求，点击【防护状态】->具体服务器的【Web模块】列表中，在【可用模块】里，选择合适的Web模块，如“IIS7-x86_64”模块，再按以下内容设置：



图示 4-18 完整的上传目录防护规则列表

最后点击“保存”即可。

第五章 附 录

5.1 术语

- 发布服务器
  iGuard V5用于进行网页变更和发布的服务模块，与Web服务器上的网页文件具有完全相同的目录结构
- 同布服务器
  iGuard V5用于进行网页文件同步和篡改防护的服务模块，运行于Web服务器上
- 管理服务器
  iGuard V5用于进行规则和策略统一配置的服务器
- 站点
  表示一个具体的Web应用系统
- 服务器
  表示一台物理设备或者虚拟机
- 服务器组
  表示一组物理设备或者虚拟机的集合
- 关联
  是指站点和服务器之间的对应关系，一个站点可以分布在多台服务器上，一台服务器也可以同时部署和运行多个站点
- 路径映射
  是指某个Web应用系统在发布服务器上配置的文件路径，与真实Web服务器上的文件路径的对应关系，以确保能够准确地进行网页文件同步

5.2 清理网页木马

通常判断网页木马的方法有以下几种。这些方法的使用不是固定的，需要根据具体的场景，选择最合适的组合，以达到高效而不漏判误判的效果：

- 特殊的文件名模式：如明显偏离原有命名模式的脚本类型文件，如diy.aspx、hacker.php、1.asp;.gif、spy.jsp等，为高度可疑的网页木马；
- 较新的文件产生时间：如整个目录下的文件创建时间均为一年前，此时出现零星的创建时间非常近期的脚本型文件则为高度可疑的网页木马文件；
- 特殊的文件属性：如文件被设置为隐藏属性、只读属性等，也是高度可疑的标志；
- 访问日志里特别的Post操作：可以通过检查Web服务器的访问日志，配合grep（Linux系统）和findstr（Windows系统）的参数组合，过滤出特定时间段所有的Post操作，根据时间段、具体URL、提交参数、访问者IP等多项组合，判断是否为可疑的木马文件；
- 文件内容：查看网页文件的内容，如果为全文加密、过多超高权限的操作组合（可以操作文件、数据库、命令行等）、包含了一个额外的特殊文件（可以为本地或远程），都表明该文件可能是网页木马。

iGuardV5自带一个基本功能的网页木马检查工具（Webshell tool）。该工具为命令行方式，可协助检查指定目录内，是否有可疑的网页木马文件。但需要注意的是，这个工具只是**一种辅助手段，**它检查的结果需要再做人工甄别，才能避免出现误判。也就是说，该工具依然是自动检查+人工判断的综合。

5.2.1 Windows系统检查Webshell

在同步服务器端，执行cmd返回命令行方式。再输入以下命令：

```
cd C:\Tercel\iGuard5\igdagent\plugin\tools\bin
lua scanner.lua [网页目录] [ .|php|asp|aspx|jsp]
```

如：

```
#对c:\webroot下的文件做全类型网页木马检查（请注意命令里最后一个“.”点号字符）
lua scanner.lua c:\webroot .
#对c:\apache\htdocs下的文件做php类型网页木马检查
lua scanner.lua c:\apache\htdocs php
```

如下图例子中，执行以后得到5个可疑文件列表：

```
C:\Tercel\iGuard5\igdagent\plugin\tools\bin>lua scanner.lua c:\inetpub\wwwroot2
asp
-----
c:\inetpub\wwwroot2/editor.aspx:eval.-request:eval(request
-----
c:\inetpub\wwwroot2/test/home.asp:execute.-request:execute request
-----
c:\inetpub\wwwroot2/test/tools/123.asp:vbscript.encode:vbscript.encode
-----
c:\inetpub\wwwroot2/test/uploadfiles/2010914153117hack.asp:vbscript.encode:vbscr
ipt.encode
-----
c:\inetpub\wwwroot2/test/uploadfiles/hac.asp;.gif:vbscript.encode:vbscript.encod
e
total files scanned : 29
matched  files      : 5
matched / total     : 0.17241379310345
```

这个工具仅是帮助使用者缩小检查的范围，所以排查出来的这5个可疑文件仍需要人工验证，也就是需要使用文本工具，打开这些文件，查看具体代码，确定它们是否为Webshell。

5.2.2 Linux 系统检查Webshell

在同步服务器端，输入以下命令：

```
cd /usr/local/iguard5/igdagent/plugin/tools/
./lua scanner.lua [网页目录] [ .|php|asp|aspx|jsp]
```

如：

```
#对/usr/local/apache2/htdocs下的文件做全类型网页木马检查（请注意命令里最后一个.点号字符）
./lua scanner.lua /usr/local/apache2/htdocs .
#对/usr/local/tomcat/webapps下的文件做jsp类型网页木马检查
./lua scanner.lua /usr/local/tomcat/webapps jsp
```

如下图例子中，执行以后得到1个可疑文件列表：

```
[root@10.10.20.62/24] [/usr/local/iguard5/igdagent/plugin/tools]$ ./lua scanner.lua /usr
/local/apache22/htdocs/ .
-----
/usr/local/apache22/htdocs//xiaom.php:xiaom.php matches ./php-special.hash:xiaom.php (10
0):
==================================
total files scanned : 5
matched  files      : 1
matched / total     : 0.2
[root@10.10.20.62/24] [/usr/local/iguard5/igdagent/plugin/tools]$
```

但仍需要手工用文本编辑器查看该文件，确认是否为有害的Webshell。

□