



链滴

# Windows+Linux 服务器登录报警，编写脚本实现钉钉群机器人报警通知

作者: [HJTGit](#)

原文链接: <https://ld246.com/article/1642991194491>

来源网站: [链滴](#)

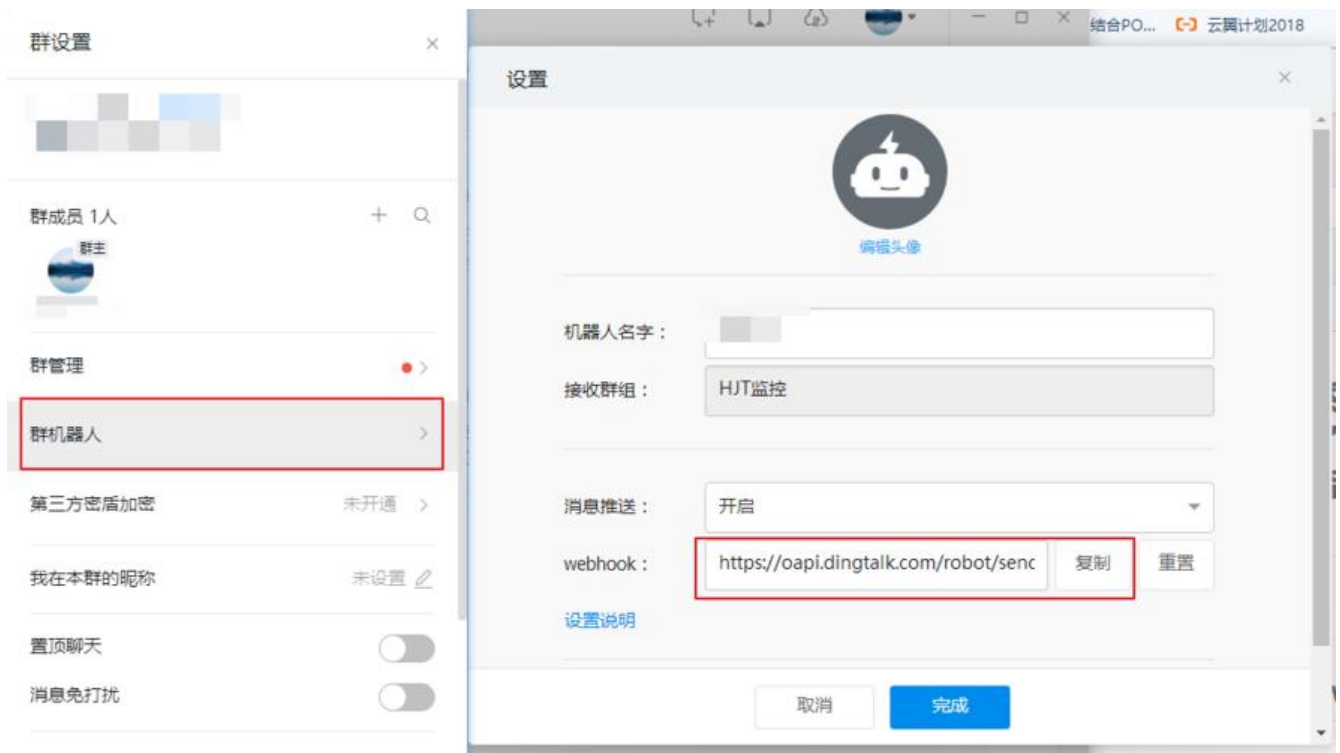
许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)



服务器有时不知道谁登录了系统，出了问题也无法找到责任人，谁动了服务器无从得知。不如在服务器安装个盘，监视下每天登录服务器的用户。

## Linux系统

### 注册钉钉机器人，获取机器人的webhook地址



## 登录服务器编写以下代码

```
#!/bin/bash
#获取登录者的用户名
user=$USER
#获取登录者的IP地址
ip=${SSH_CLIENT%% *}
#获取登录的时间
time=$(date +%F%t%k:%M)
#服务器的IP地址
server='xxxxxxx.xxxxxx.xxxxxx.xxxx'

function SendMessageToDingding(){
#你钉钉机器人的地址。
local url="https://oapi.dingtalk.com/robot/send?access_token=你钉钉机器人的token"

local UA="Mozilla/5.0(WindowsNT6.2;WOW64)AppleWebKit/535.24(KHTML,likeGecko)Chrom
/19.0.1055.1Safari/535.24"

local res=`curl -XPOST -s -L -H"Content-Type:application/json" -H"charset:utf-8" $url -d"{\"m
gtype\": \"text\", \"text\": {\"content\": \"$1\n$2\"}}`
}
SendMessageToDingding "服务器登录告警" "时间 $time,用户 $user,用户地址 $ip,服务器地址 $se
ver"
```

写入文件 `/etc/ssh/sshr` 即可。

**之后就可以放心了，有任何登录，都会收到消息。再也不用心吊胆了。**



[参考文章](#)

## Windows系统

获取机器人链接步骤与以上相同

## windows下编写bat脚本

首先创建脚本文件.bat执行推送钉钉功能 登录推送文件in.bat 退出登录out.bat

简单推送代码参考如下：

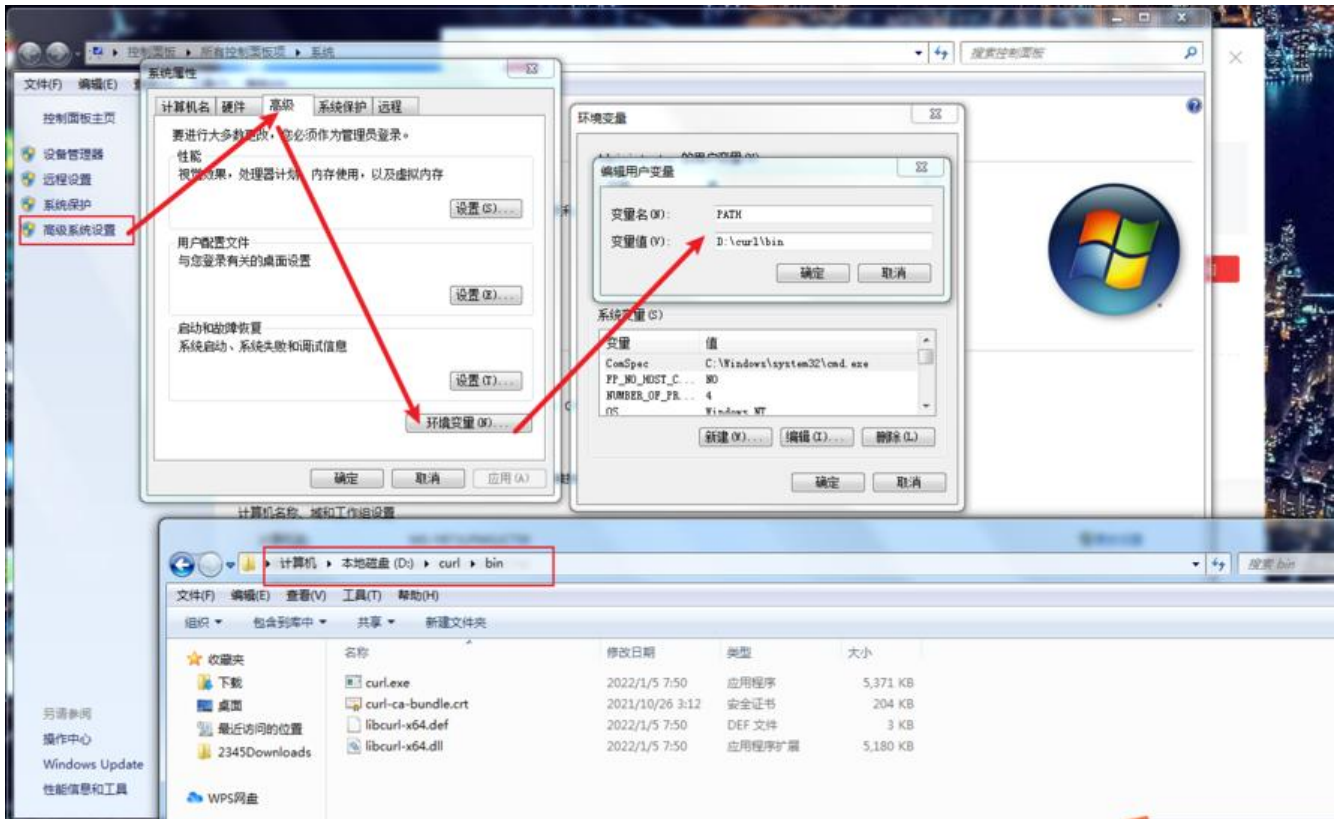
```
curl "https://oapi.dingtalk.com/robot/send?access_token=你钉钉机器人的token" -H "Content-
```

```
ype: application/json" -d "{\"msgtype\": \"text\", \"text\": {\"content\": \"login IN %date:~0,10 %time:~0,5%\"}}\" -X POST
```

```
curl "https://oapi.dingtalk.com/robot/send?access_token=你钉钉机器人的token" -H "Content-type: application/json" -d "{\"msgtype\": \"text\", \"text\": {\"content\": \"login OUT %date:~0,1 % %time:~0,5%\"}}\" -X POST
```

由于windows系统不自带curl功能无法直接访问接口推送消息 需要下载一个curl工具[curl.zip](#)

下载后解压，并配置解压后的目录到系统PATH，之后CMD中输入curl --help测试是否成功



```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation. 保留所有权利。

C:\Users\Administrator>curl --help
Usage: curl [options...] <url>
-d, --data <data>          HTTP POST data
-f, --fail                 Fail silently (no output at all) on HTTP errors
-h, --help <category>    Get help for commands
-i, --include              Include protocol response headers in the output
-o, --output <file>       Write to file instead of stdout
-O, --remote-name         Write output to a file named as the remote file
-s, --silent              Silent mode
-T, --upload-file <file> Transfer local FILE to destination
-u, --user <user:password> Server user and password
-A, --user-agent <name>  Send User-Agent <name> to server
-v, --verbose             Make the operation more talkative
-U, --version             Show version number and quit

This is not the full help, this menu is stripped into categories.
Use "--help category" to get an overview of all categories.
For all options use the manual or "--help all".

C:\Users\Administrator>
```

现在设置监控就可以实现推送，但是.bat文件执行时会出现一个黑框，让人很是害怕，所以经过查询到了一种方法

编写vbs文件里边执行.bat文件，就不会出现黑框，创建.vbs文件in.vbs out.vbs代码如下：

```
createobject("wscript.shell").run "这里填对应bat存放的位置",0
```

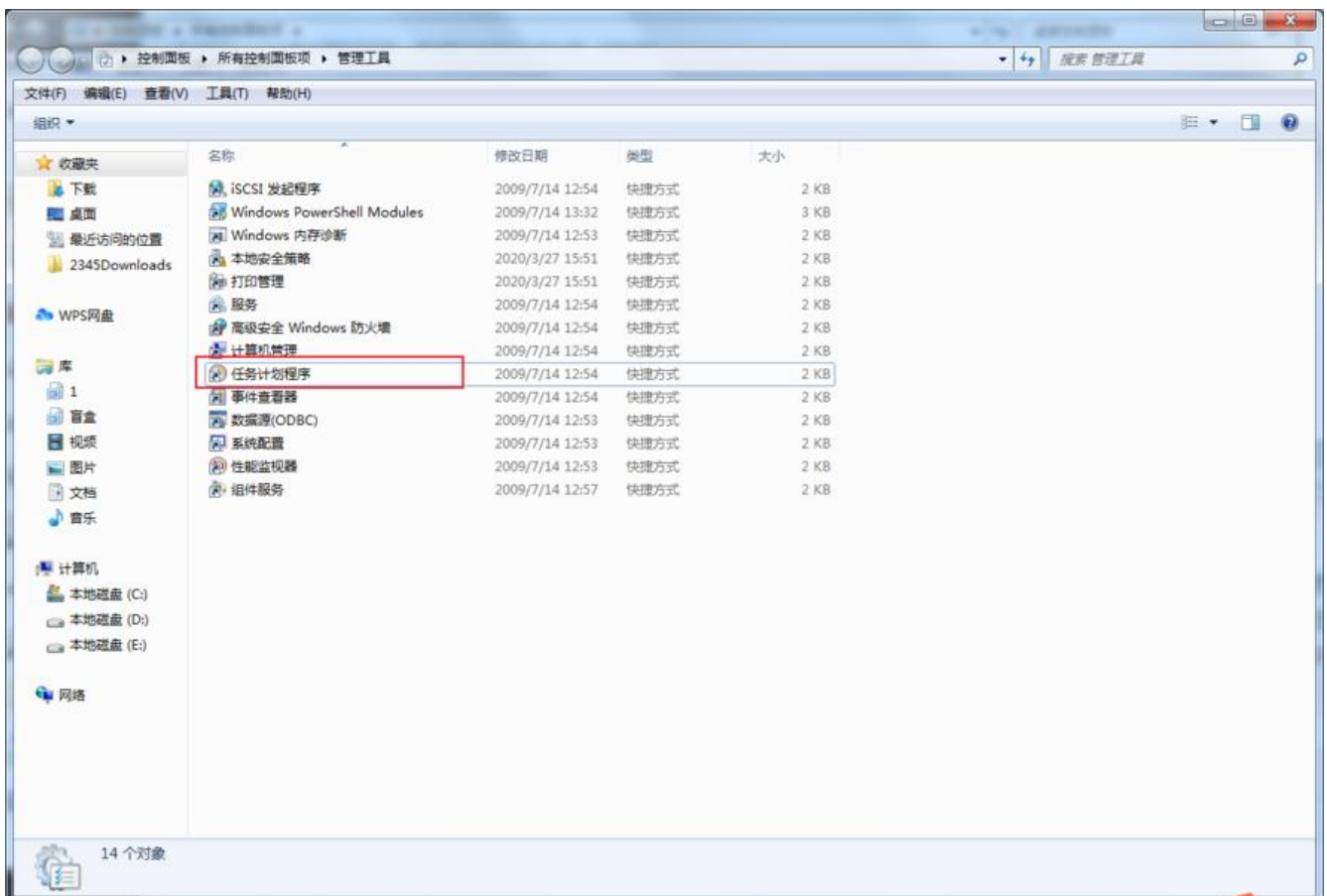
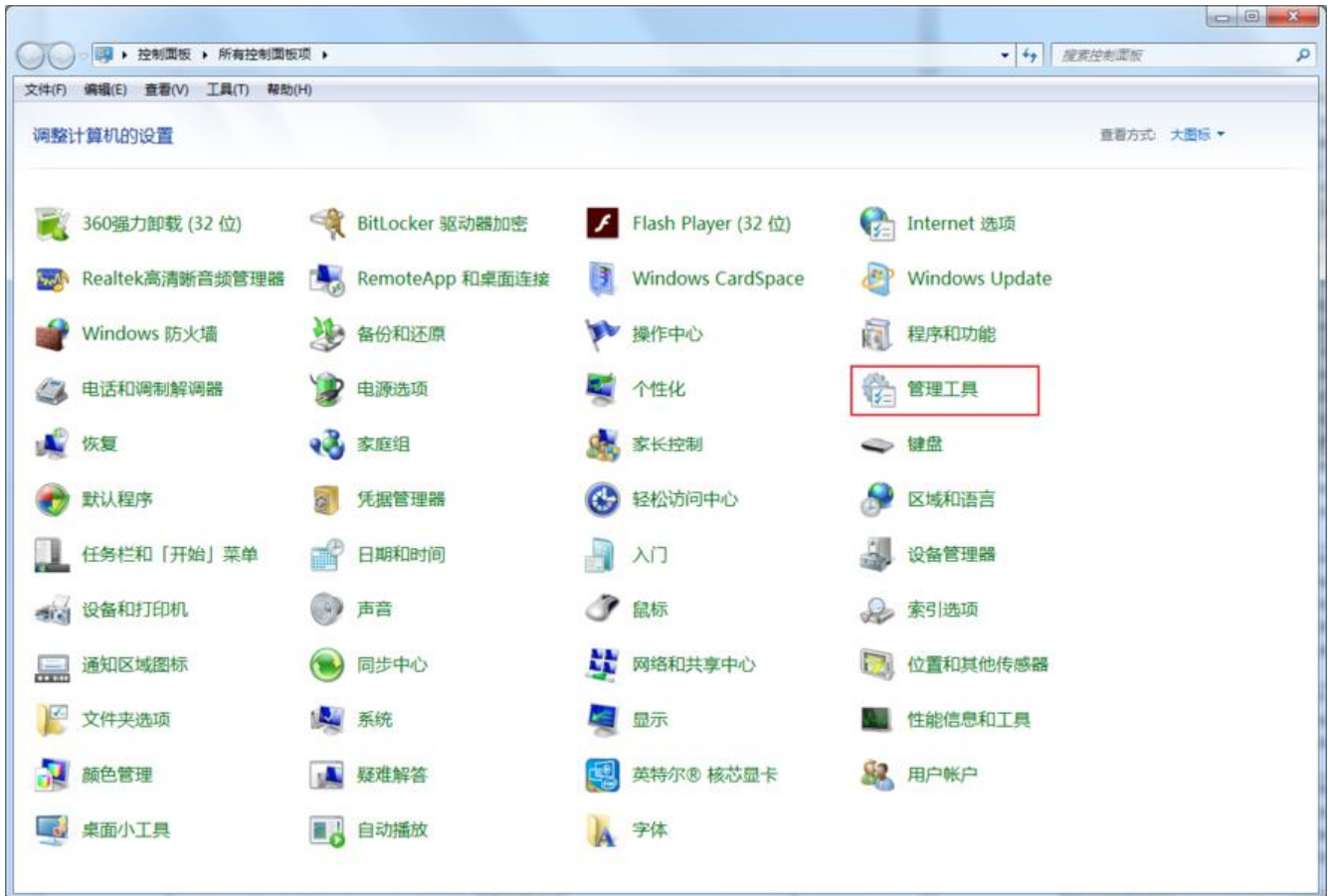
```
createobject("wscript.shell").run "C:\IN.bat",0
```

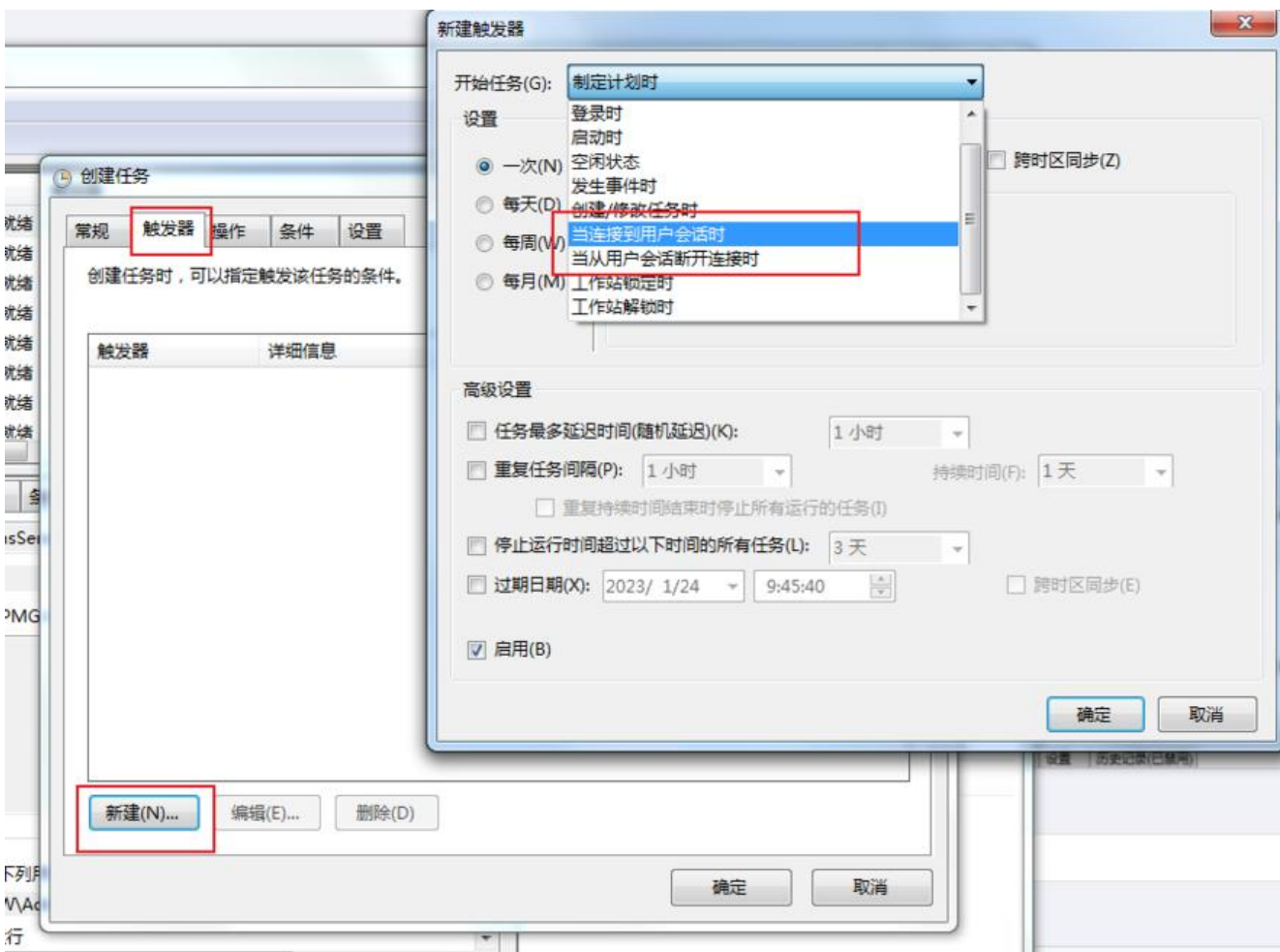
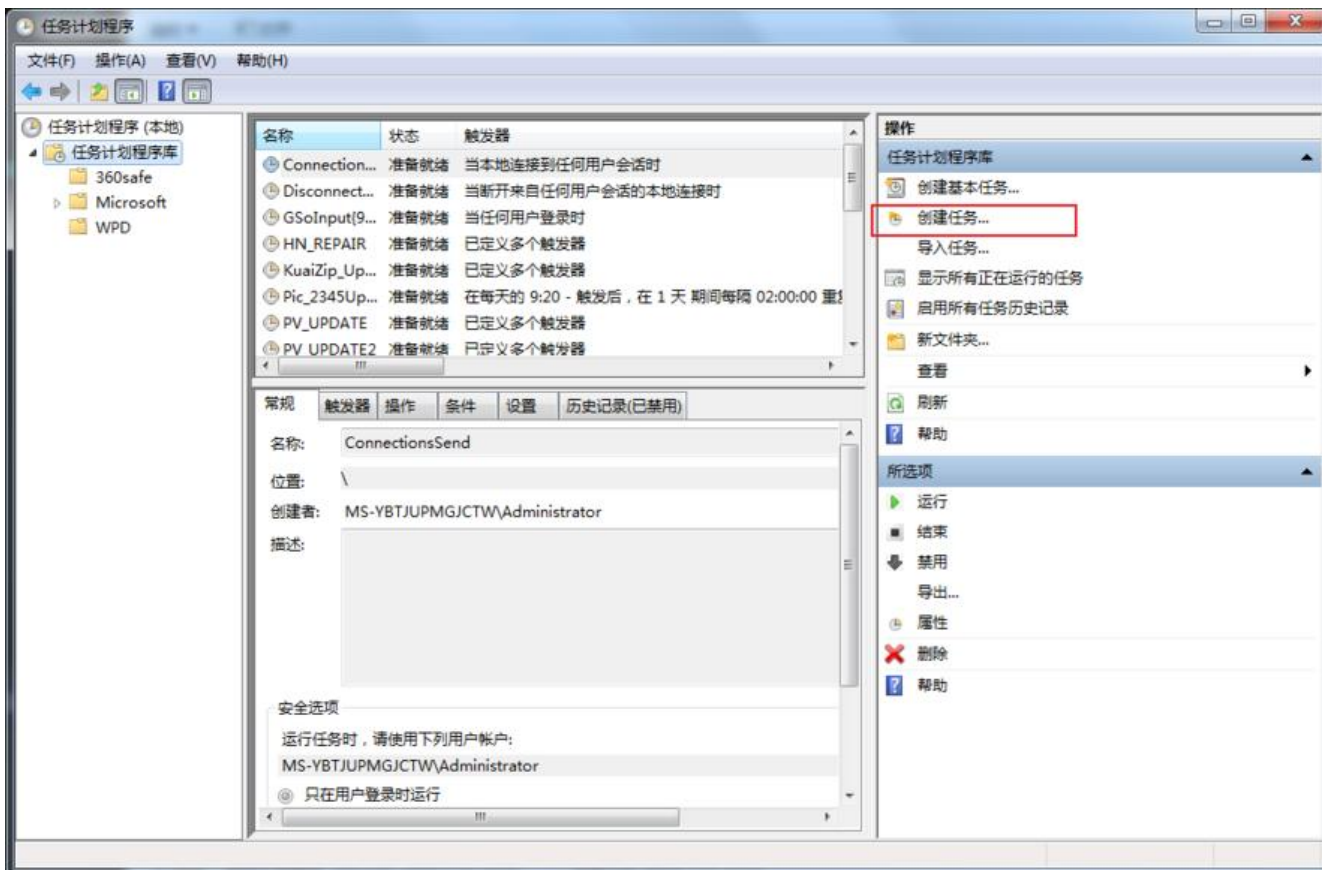
```
createobject("wscript.shell").run "C:\OUT.bat",0
```



## 设置登录断开监控

- 1.登录windows服务器 打开控制面板中的管理工具
- 2.打开任务计划程序
- 3.点击创建任务 名称自定义in
- 4.点击触发器，点击新建 开始任务下拉框选择“当连接到用户会话时”下方出现对应设置选“远程计算机连接”确定
- 5.点击操作，点击新建 操作下拉框选择“启动程序”下方程序或脚本选择自己创建的那个in.vbs文件：  
vbs文件与bat文件最好不要存放在有空格的文件夹下
- 6.相同操作创建out任务 触发器选择“当从用户会话断开连接时” 脚本选择自己创建的那个out.vbs文件





这样就实现了简单监控登录退出功能

