# tcp\_monitor布署说明

## 配置说明

### 刷新间隔

tcp\_monitor.pl文件中，

# 刷新间隔

my $\_refresh\_rate = 300; #Refresh rate of the netstat data

单位为秒，决定脚本多少秒取一次结果。

### 报警阈值配置文件

tcp\_monitor.pl文件中，

my $cfg\_file = "$Bin/../etc/tcp\_monitor.conf";

$Bin代表脚本所在目录，假设系统为linux，脚本目录为/openimis/SysChk/bin，则配置文件路径为/openimis/SysChk/etc/ tcp\_monitor.conf

tcp\_monitor.conf文件为报警阈值配置文件，内容如下：

###################################################

# this is the configure file of tcpcount.pl

###################################################

#NAME warning alarm on/off

ESTABLISHED 30000 50000 off

LISTEN 30000 50000 off

TIME\_WAIT 1000 2000 on

CLOSE\_WAIT 30000 50000 off

SYN\_SENT 30000 50000 off

SYN\_RECV 30000 50000 off

SYN\_WAIT 30000 50000 off

FIN\_WAIT1 30000 50000 off

FIN\_WAIT2 30000 50000 off

CLOSED 30000 50000 off

LAST\_ACK 30000 50000 off

CLOSING 30000 50000 off

UNKNOWN 30000 50000 off

Recv-Q 8192 10240 on

Send-Q 8192 10240 on

第1列为报警项名称，第2列为一般报警阈值，第3列为严重报警阈值，第4列为报警开关；缺省的项不会发出报警；如果不存在配置文件，或者配置文件中缺少对应的报警项配置，则遵循程序内部的默认配置。

### debug日志

tcp\_monitor.pl文件中，

# debug开关，debug日志文件名

my $debug = 0;

my $debuglog = "$Bin/../log/tcp\_monitor.log";

前者为debug日志开关，置为0表示关闭，置为1表示开启；后者为debug日志保存路径，$Bin代表脚本所在目录，假设系统为linux，脚本目录为/openimis/SysChk/bin，则debug日志文件路径为/openimis/SysChk/log/ tcp\_monitor.log

### 报警发送配置

tcp\_monitor.pl文件中，

my $alarm\_switch = 1;

my $alarm\_ip = "10.237.128.195";

my $alarm\_port = 31820;

第一个值为报警开关，置为1表示发送报警，置为0则不发送报警；第二个值为报警发送到的地址，第三个值为报警发送到的端口。

### tcp连接信息发送配置

tcp\_monitor.pl文件中，

my $report\_switch = 1;

my $report\_ip = "10.237.128.195";

my $report\_port = 31830;

第一个值为开关，置为1表示发送，置为0则不发送；第二个值为发送到的地址，第三个值为发送到的端口，一组31830，二组31831，三组31832，其他31833，请根据各组接收监控信息的服务器地址和端口配置。

## 各平台布署说明

### Linux

1、将tcp\_monitor.pl、check\_tcp\_monitor.sh、restart\_tcp\_monitor.sh拷贝到/openimis/SysChk/bin目录，tcp\_monitor.conf拷贝到/openimis/SysChk/etc目录；

2、切换到root用户，输入crontab –e 命令，添加以下内容：

\*/5 \* \* \* \* /openimis/SysChk/bin/check\_tcp\_monitor.sh #每5分钟检查进程是否存在,不存在则启动

2 12 \* \* \* /openimis/SysChk/bin/restart\_tcp\_monitor.sh #每天中午重启一次脚本

**可以通过附带的add\_cron\_tcp\_monitor.sh脚本自动完成第2步操作**

### Aix

1、安装lsof到/openimis/SysChk/bin目录下（如果关闭了tcp连接信息发送则可以不安装）

2、将tcp\_monitor.pl、check\_tcp\_monitor.sh、restart\_tcp\_monitor.sh拷贝到/openimis/SysChk/bin目录，tcp\_monitor.conf拷贝到/openimis/SysChk/etc目录；

3、切换到root用户，输入crontab –e 命令，添加以下内容：

0,5,10,15,20,25,30,35,40,45,50,55 \* \* \* \* /openimis/SysChk/bin/check\_tcp\_monitor.sh #每5分钟检查进程是否存在,不存在则启动

2 12 \* \* \* /openimis/SysChk/bin/restart\_tcp\_monitor.sh #每天中午重启一次脚本

**可以通过附带的add\_cron\_tcp\_monitor.sh脚本自动完成第3步操作**

### Windows

1、安装perl运行环境

2、tcp\_monitor.pl文件中，$cfg\_file 和$debuglog的值改为如下值

my $cfg\_file = "$Bin/tcp\_monitor.conf";

my $debuglog = "$Bin/log/tcp\_monitor.log";

3、将tcp\_monitor.pl、check\_tcp\_monitor.sh、restart\_tcp\_monitor.sh tcp\_monitor.conf拷贝到C:\OSAC目录；

4、添加一个计划任务，计划任务执行的命令为：

perl C:\openimis\SysChk\bin\tcp\_monitor.pl -c 3

其中， -c 3 表示每次运行脚本会收集3次信息。