# tcp\_monitor布署说明

## 配置说明

从1.6版本开始，配置文件改为ini格式，文件名tcp\_monitor.conf.ini。

### 主配置

主配置在配置的文件的main部分，以 [main] 引导的配置项:

#### refresh\_rate

采集信息间隔时间，单位为秒，默认为300秒

#### errorlog

错误日志保存路径，以相对脚本所在目录的相对路径表示

#### debug

debug开关，on/off表示打开/关闭，默认为off

#### debuglog

debug日志保存路径，以相对脚本所在目录的相对路径表示

#### alarm\_switch

报警监控总开关，on/off表示打开/关闭，默认为on

#### alarm\_ip

报警发送目的地址的IP，请根据各组接收监控信息的服务器地址和端口配置。

alarm\_port

报警发送目的地址的端口，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。

report\_switch

TCP连接信息发送的开关，on/off表示打开/关闭，默认为on

report\_ip

TCP连接信息发送目的地址的IP

#### report\_port

TCP连接信息发送目的地址的端口

#### action\_script

有报警触发时自动执行此命令，可以带参数。

上一次执行的命令如果尚未退出，不会再次触发。即保持永远只有一个实例在执行。

请不要使用 & 符号结尾等方法让命令后台执行，因为这样会立即获得命令正常结束的信号（bash会立即返回0），而真正的命令可能仍在执行中，此时再次触发报警会再次执行命令，极端情况下可能会带起大量的后台进程，消耗cpu资源。

### 连接状态计数报警配置

连接状态计数报警配置在配置的文件的alarm部分，以 [alarm] 引导的配置项:

#### **ESTABLISHED\_warning**

ESTABLISHED一般报警阈值,数字代表当前处于此连接状态的个数

#### **ESTABLISHED\_alarm**

ESTABLISHED严重报警阈值,数字代表当前处于此连接状态的个数

#### ESTABLISHED\_switch

ESTABLISHED单项报警开关，on/off表示打开/关闭

#### ESTABLISHED\_trigger

ESTABLISHED报警触发是否要自动执行[main] –> action\_script里配置的命令的开关，on/off表示打开/关闭

#### 其他

SYN\_SENT、SYN\_RECV、FIN\_WAIT1、FIN\_WAIT2、TIME\_WAIT、CLOSE、CLOSE\_WAIT、LAST\_ACK、LISTEN、CLOSING、UNKNOWN、Recv-Q、Send-Q 的配置与ESTABLISHED类似

### 连接状态计时报警配置

连接状态计数报警配置在配置的文件的timeout部分，以 [timeout] 引导的配置项:

#### **ESTABLISHED\_warning**

ESTABLISHED一般报警阈值,数字代表当前处于此连接状态的个数

#### **ESTABLISHED\_alarm**

ESTABLISHED严重报警阈值,数字代表当前处于此连接状态的个数

#### ESTABLISHED\_switch

ESTABLISHED单项报警开关，on/off表示打开/关闭

#### ESTABLISHED\_trigger

ESTABLISHED报警触发是否要自动执行[main] –> action\_script里配置的命令的开关，on/off表示打开/关闭

#### 其他

SYN\_SENT、SYN\_RECV、FIN\_WAIT1、FIN\_WAIT2、TIME\_WAIT、CLOSE、CLOSE\_WAIT、LAST\_ACK、CLOSING、UNKNOWN的配置与ESTABLISHED类似

## 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.ini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.ini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运行环境到C:\osac 目录，最终perl可执行文件路径应该为C:\osac\Perl\bin\perl.exe

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

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

3、tcp\_monitor.pl文件中，errorlog的值改为如下值

# 错误日志保存路径

errorlog=tcp\_monitor\_error.log

3、将tcp\_monitor.pl、srvany.exe、checkservice.vbs、 tcp\_monitor.conf.ini拷贝到C:\OSAC\tcp\_monitor\ 目录；

4、执行addnetworkservice.bat 脚本，脚本会自动添加一个Tcp\_monitor 服务到系统中并运行