触发器、报警

触发器 Trigger

作用：报警

由监控项获取数据，针对某个或者多个监控项为其设置触发器

设置监控项阈值，触发监控项状态的变化

一个监控项可以设置多个触发器

触发器的语法：

{<server>:<key>.<function>(<parameter>)}<operator><constant>

{<主机名称>:<键值名称>.<函数名称>(参数)}<操作符><常量[数字]>

{node01:net.if.in[eth0].sum(5m)}>100K

操作符：

+， -， \*， /

=， <>, >, >=, <, <=

and or not

函数：

avg( )

sum( )

max( )

min( )

last(#2 ) //获取后面的值

count( )

date() dayofmoney( ) dayofweek( )

diff( ) 判断两个值是否不相同

函数使用示例：

|  |  |  |
| --- | --- | --- |
| **sum(600)** | 600秒内所有值的总和 |  |
| **sum(#5)** | 最后5个值的总和  Avg(#5) | |

函数last当以#作为前缀使用时，值具有不同的含义，所以给定值3、7、2、6、5（按照时间顺序，第一个值3为最新值），last(#2) 将返回值为7 ，last(#5) 将返回值为5。 last()

https://www.zabbix.com/documentation/3.4/zh/manual/config/triggers/expression

{www.zabbix.com:system.cpu.load[all,avg1].last()}>5

{www.zabbix.com:system.cpu.load[all,avg1].last()}>5 or {www.zabbix.com:system.cpu.load[all,avg1].min(10m)}>2

{www.zabbix.com:vfs.file.cksum[/etc/passwd].diff()}=1

{www.zabbix.com:net.if.in[eth0,bytes].min(5m)}>100K

{smtp1.zabbix.com:net.tcp.service[smtp].last()}=0 and {smtp2.zabbix.com:net.tcp.service[smtp].last()}=0

{zabbix.zabbix.com:icmpping.count(30m,0)}>5

表示今天同一个时间的CPU负载和昨天同一个时间的CPU负载相比

{server:system.cpu.load.avg(1h)}/{server:system.cpu.load.avg(1h,1d)}>2

示例：为node01的磁盘分区剩余容量设置触发器

1) 为node01添加一个监测磁盘分区剩余容量的监控项、图形



2) 创建触发器





在node01上创建一个100M的文件

[root@node01 ~]# dd if=/dev/zero of=/data/1.txt bs=1M count=100

if=/dev/zero 源文件 input file

of=/data/1.txt 目的文件名称

bs=1M block size 数据块大小

count=100 次数

报警

报警方式：

邮件报警

微信报警

短信报警

电话报警

大体步骤：

1、创建报警媒介media

定义邮件服务器地址

定义发送人

2、定义收件人

3、关联触发器创建动作

示例：关联触发器，实现本地用户邮件报警

1) 添加主机名解析

[root@zabbix\_server ~]# cat /etc/hosts

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

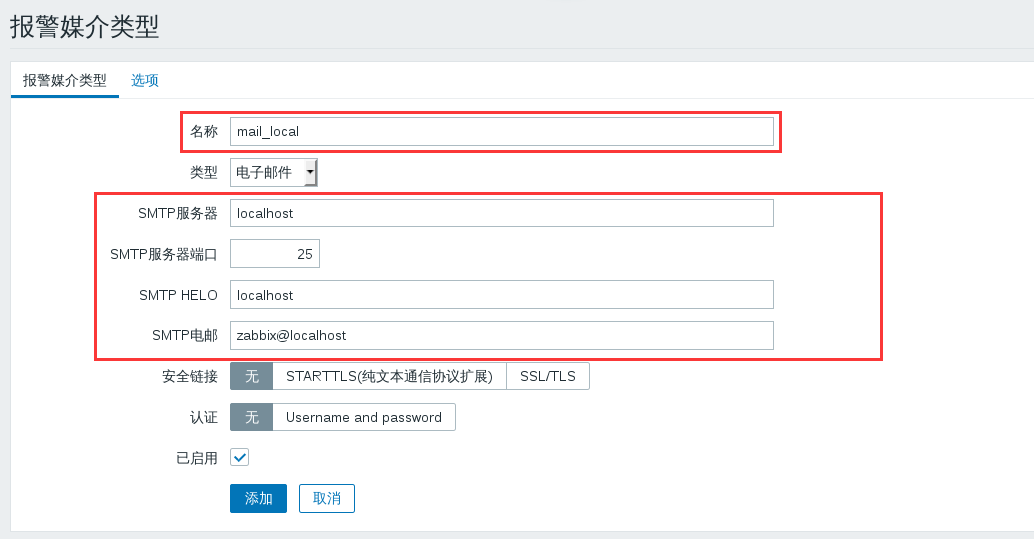
192.168.122.101 zabbix\_server.uplooking.com

[root@zabbix\_server ~]# yum install -y mailx

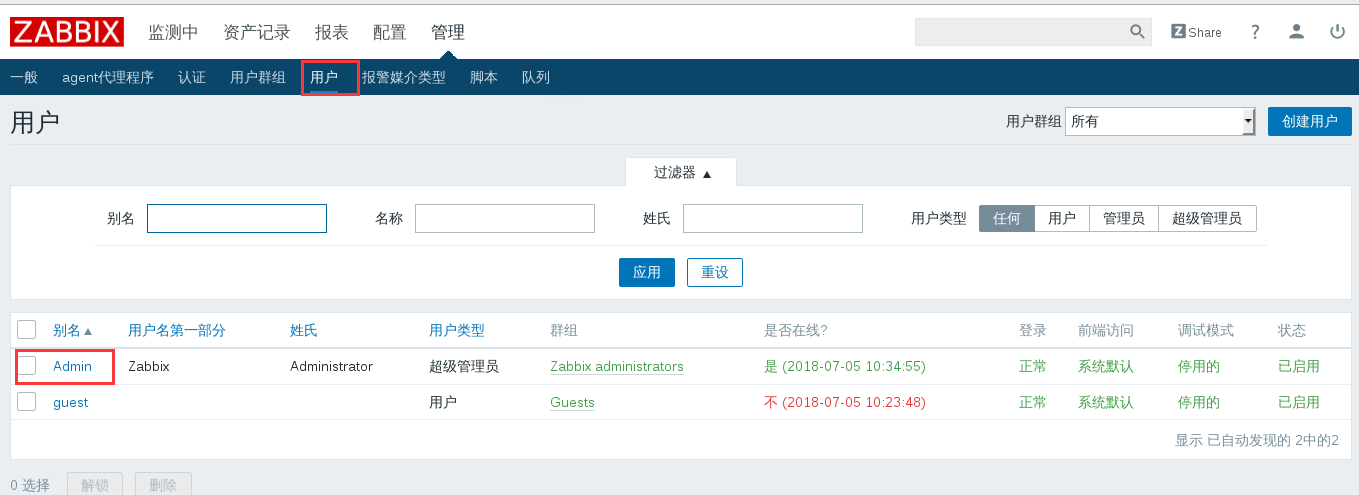
[root@zabbix\_server ~]# useradd martin

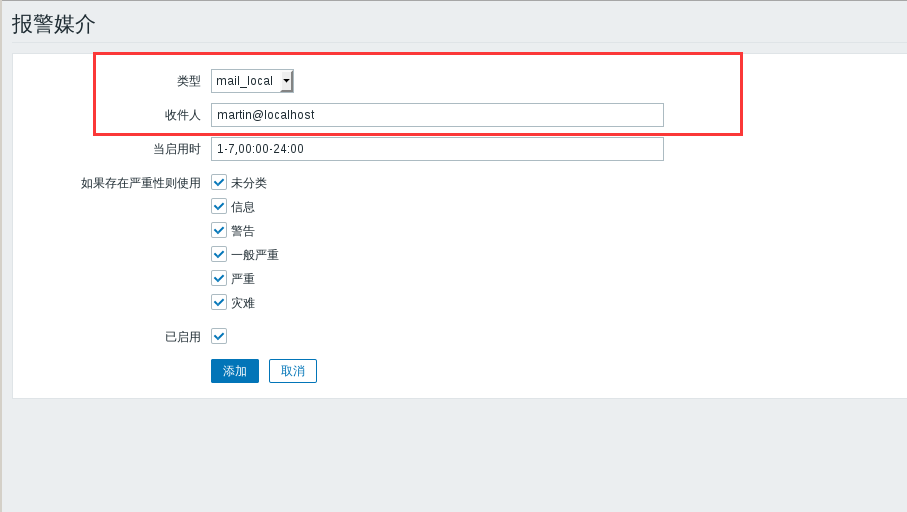
2) 创建媒介media





3) 定义收件人

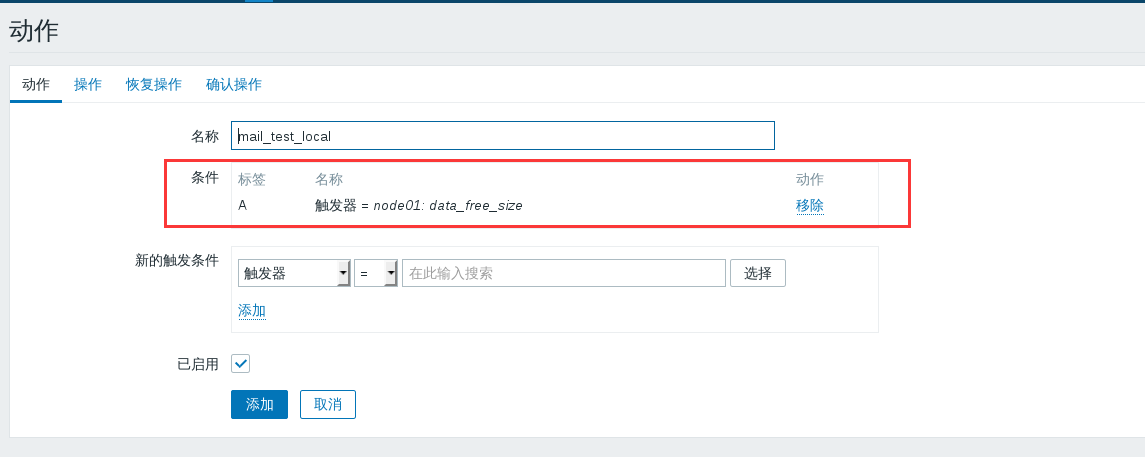


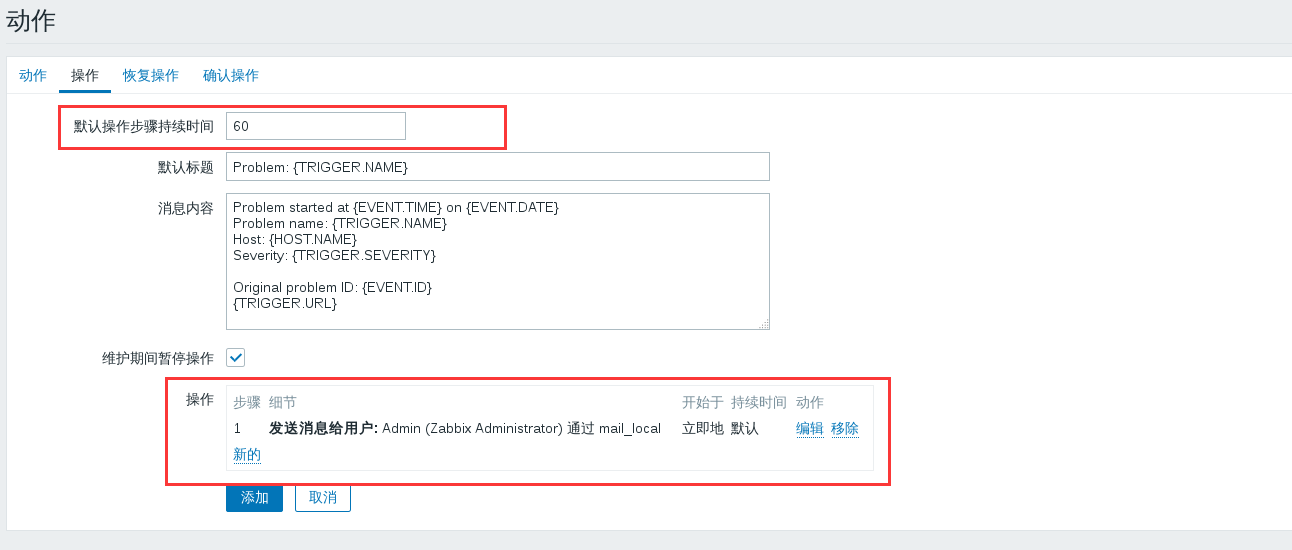


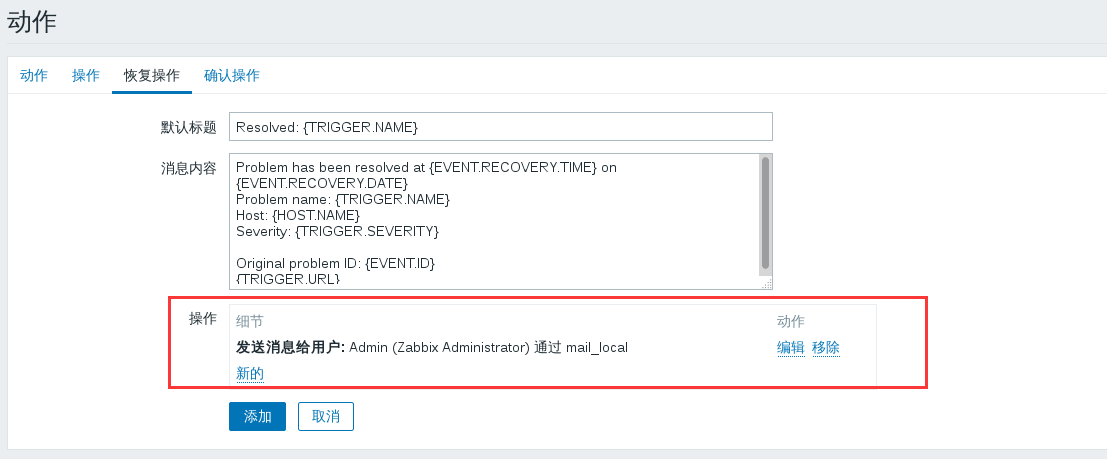


3) 创建动作









测试

示例：实现本地多用户user01, user02报警

1、创建系统用户

[root@zabbix\_server ~]# useradd user01

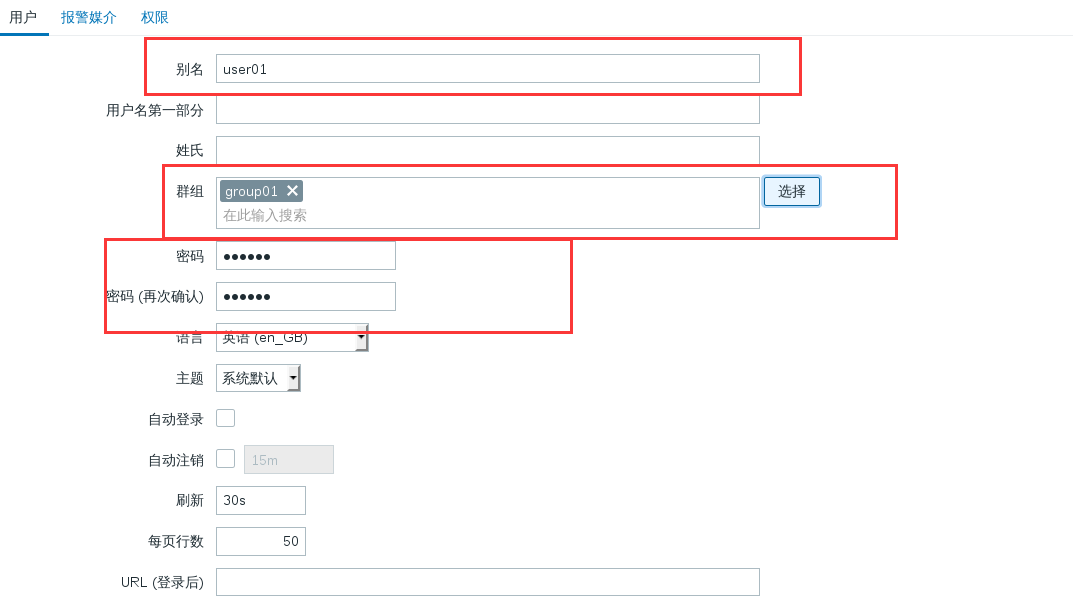
[root@zabbix\_server ~]# useradd user02

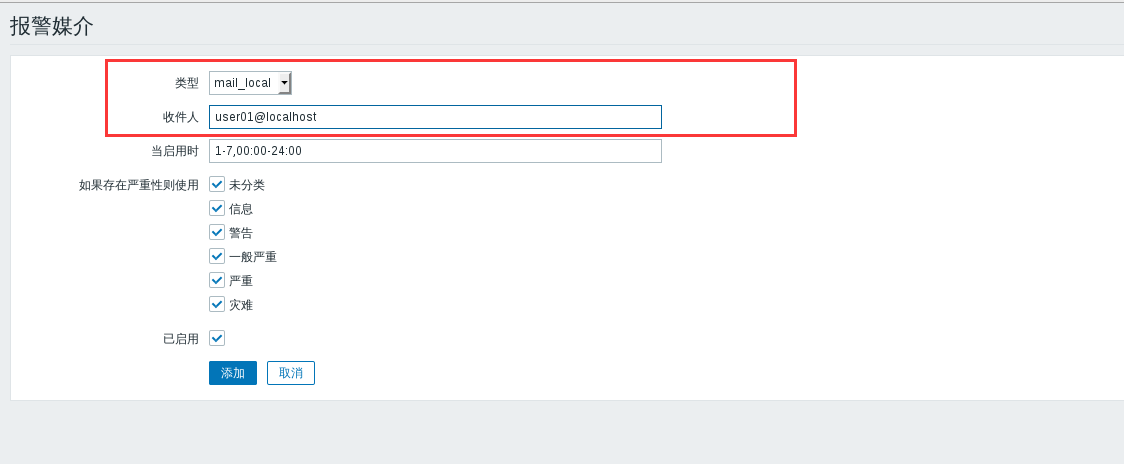
2、创建用户群组



3、创建zabbix用户关联用户邮箱

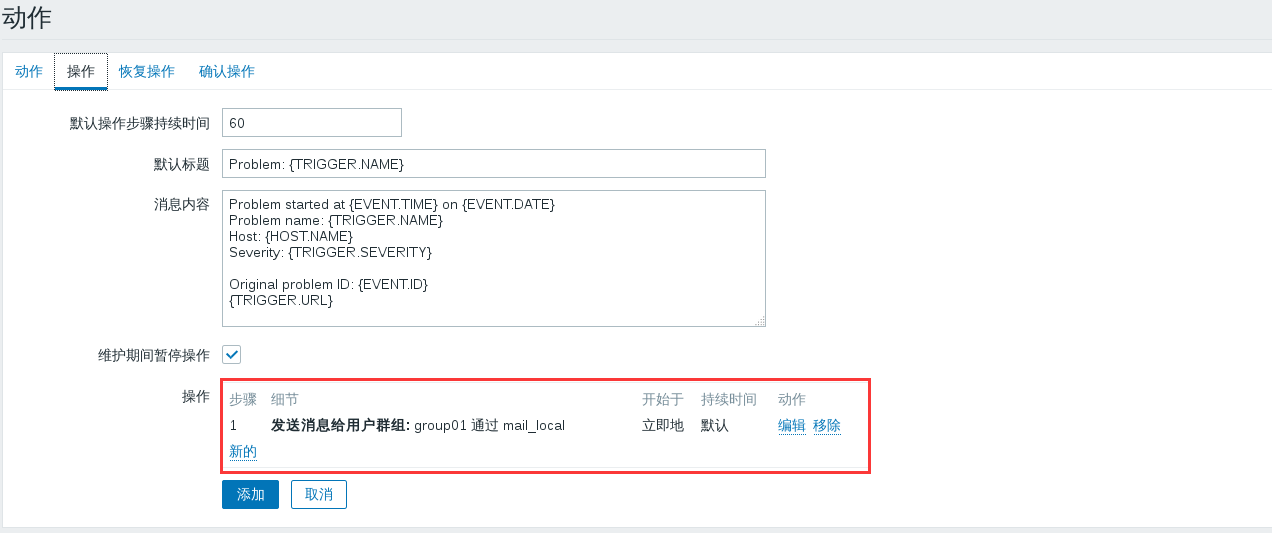








4) 创建动作



测试

配置外部邮件报警

以网易邮箱为例

1、开启客户端授权



2、配置postfix

[root@zabbix\_server ~]# vim /etc/postfix/main.cf

myhostname = zabbix\_server.uplooking.com

mydomain = uplooking.com

inet\_interfaces = all

[root@zabbix\_server ~]# systemctl restart postfix

[root@zabbix\_server ~]# netstat -antp | grep :25

tcp 0 0 0.0.0.0:25 0.0.0.0:\* LISTEN 23610/master

tcp6 0 0 :::25 :::\* LISTEN 23610/master

[root@zabbix\_server ~]#

3、配置外部邮箱

[root@zabbix\_server ~]# vim /etc/mail.rc

70 set from=zabbix\_linux\_wjc@126.com smtp=smtp.126.com

71 set smtp-auth-user=zabbix\_linux\_wjc smtp-auth-password=uplooking123[客户端的授权码] smtp-auth=login

测试向外部邮箱发送邮件

[root@zabbix\_server ~]# mail -s "test mail" sb\_linux@126.com

hello,ni hao

.

EOT

4、配置发送邮件的脚本

1) 编辑zabbix-server的配置文件，定义外部脚本的存放位置

[root@zabbix\_server ~]# vim /etc/zabbix/zabbix\_server.conf

AlertScriptsPath=/usr/lib/zabbix/alertscripts

[root@zabbix\_server ~]# vim /usr/lib/zabbix/alertscripts/isp\_mail.sh

#!/bin/bash

echo $1 >> /tmp/text.txt

echo $2 >> /tmp/text.txt

echo $3 >> /tmp/text.txt

messages=`echo $3 | tr '\r\n' '\n'`

subject=`echo $2 | tr '\r\n' '\n'`

echo "${messages}" | mail -s "${subject}" $1 >>/tmp/mailx.log 2>&1

[root@zabbix\_server ~]# chown -R zabbix.zabbix /usr/lib/zabbix/alertscripts/

[root@zabbix\_server ~]# chmod a+x /usr/lib/zabbix/alertscripts/isp\_mail.sh

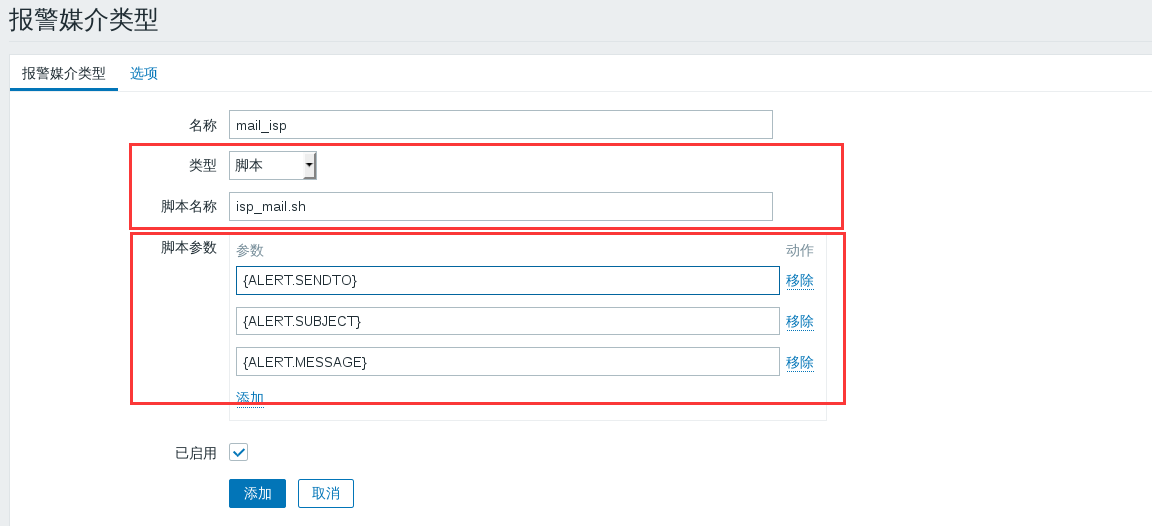
手动测试脚本：

[root@zabbix\_server alertscripts]# ./isp\_mail.sh zabbix\_linux\_wjc@126.com bbbb cccc

[root@zabbix\_server alertscripts]# chmod 777 /tmp/text.txt /tmp/mailx.log

5、创建报警媒介media





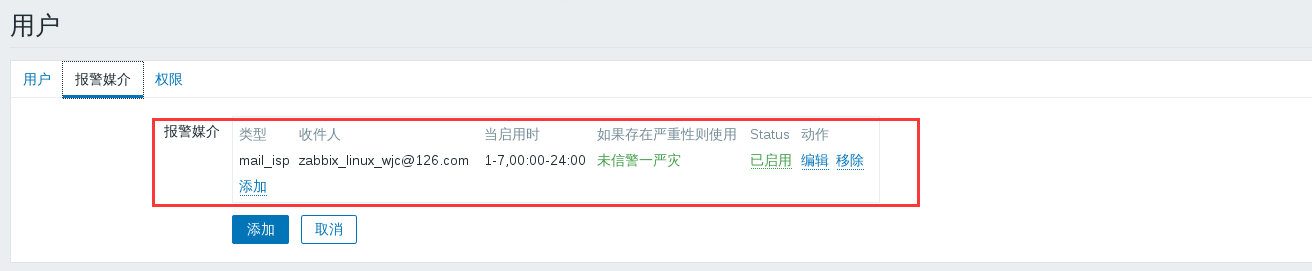
zabbix变量/宏

{ALERT.SENDTO} --------- 关联zabbix用户绑定的收件人

{ALERT.SUBJECT} -------- 内容标题

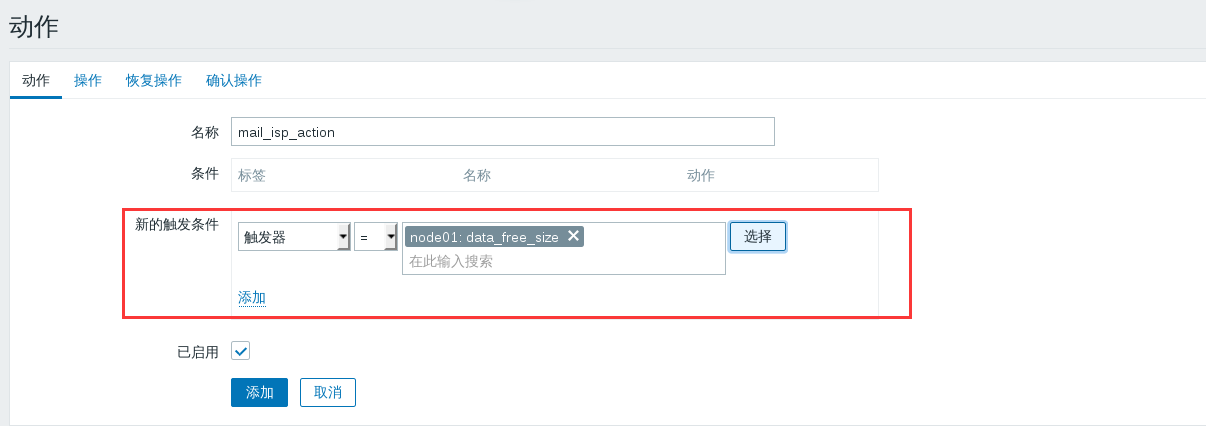
{ALERT.MESSAGE} ------- 消息内容

6、创建zabbix用户，关联收件人

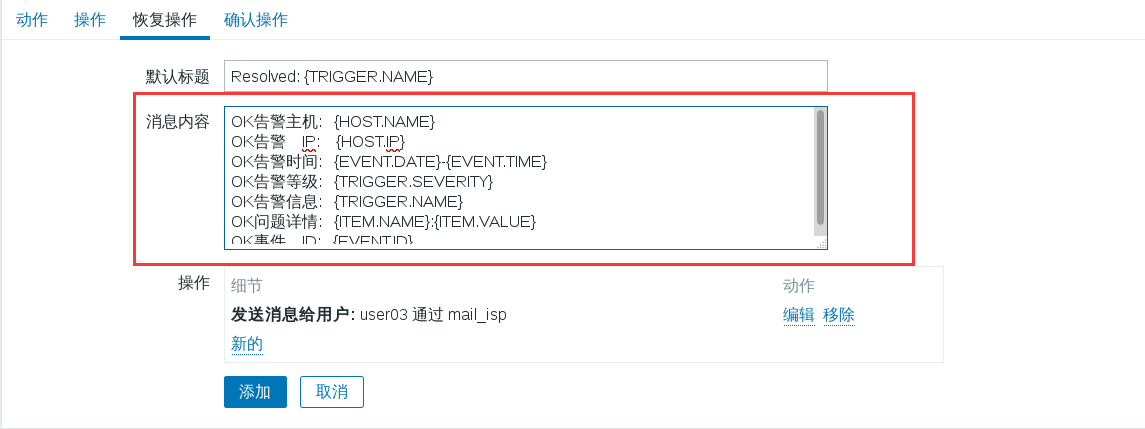


7、创建发送邮件的动作









https://www.zabbix.com/documentation/3.4/manual/appendix/macros/supported\_by\_location

**发送内容：**  
{HOST.NAME}     主机名称

{HOST.IP}      主机

{EVENT.DATE}-{EVENT.TIME} YYYY-MM-DD-HH:MM:SS

{TRIGGER.SEVERITY} 触发器的等级

{TRIGGER.NAME} 触发器名称

{ITEM.NAME}:{ITEM.VALUE} 监控项名称:监控项的值

{EVENT.ID} 事件ID