# Zabbix监控服务器异常IP登录

放入py 脚本

cat /usr/local/zabbix/scripts/illegalIP.py

|  |
| --- |
| #!/usr/bin/python  # -\*- encoding: utf-8 -\*-  #1.收集服务器上登录的IP  #2.删除收集到的白名单IP  #3.如果收集到的IP为空,则将白名单IP写入收集里面  import os  import sys  #获取ip  ip=os.popen("who -u | grep -Eo '([0-9]{1,3}\.){3}[0-9]{1,3}' |sort -t'.' -k1,1nr -k2,2nr -k3,3nr -k4,4nr |uniq").read().split("\n")  #判断是否要删除ip  newip=ip  Whitelist=[]  for num in range(1,len(sys.argv)):  newip=' '.join(newip).replace(sys.argv[num], "").split()  Whitelist.append(sys.argv[num])  #判断newip是否为空,为空代表服务器没有被非其他ip登录,则显示当前正常ip登录的账号  #避免误报，如果newip为空就将传入的参数写入newip里面  nulll=0  if len(newip) == 0:  newip=Whitelist  nulll=1  #获取登录信息  data=[]  if nulll == 0:  for i in newip:  if i != '':  #执行获取信息的命令,分割后添加到数组  datatmp=os.popen("who -u | grep '%s' "%i).read().split('\n')  for ii in os.popen("who -u | grep '%s' "%i).read().split('\n'):  if ii != '':  data.append(ii.replace('\n',""))  else:  data.append(os.popen("who -u ").read())  #监控的信息  print "%s\n"%' '.join(newip)  #显示登录信息  print '\n'.join(data) |

将下面的写入到/usr/local/zabbix/etc/zabbix\_agentd.conf最后一行

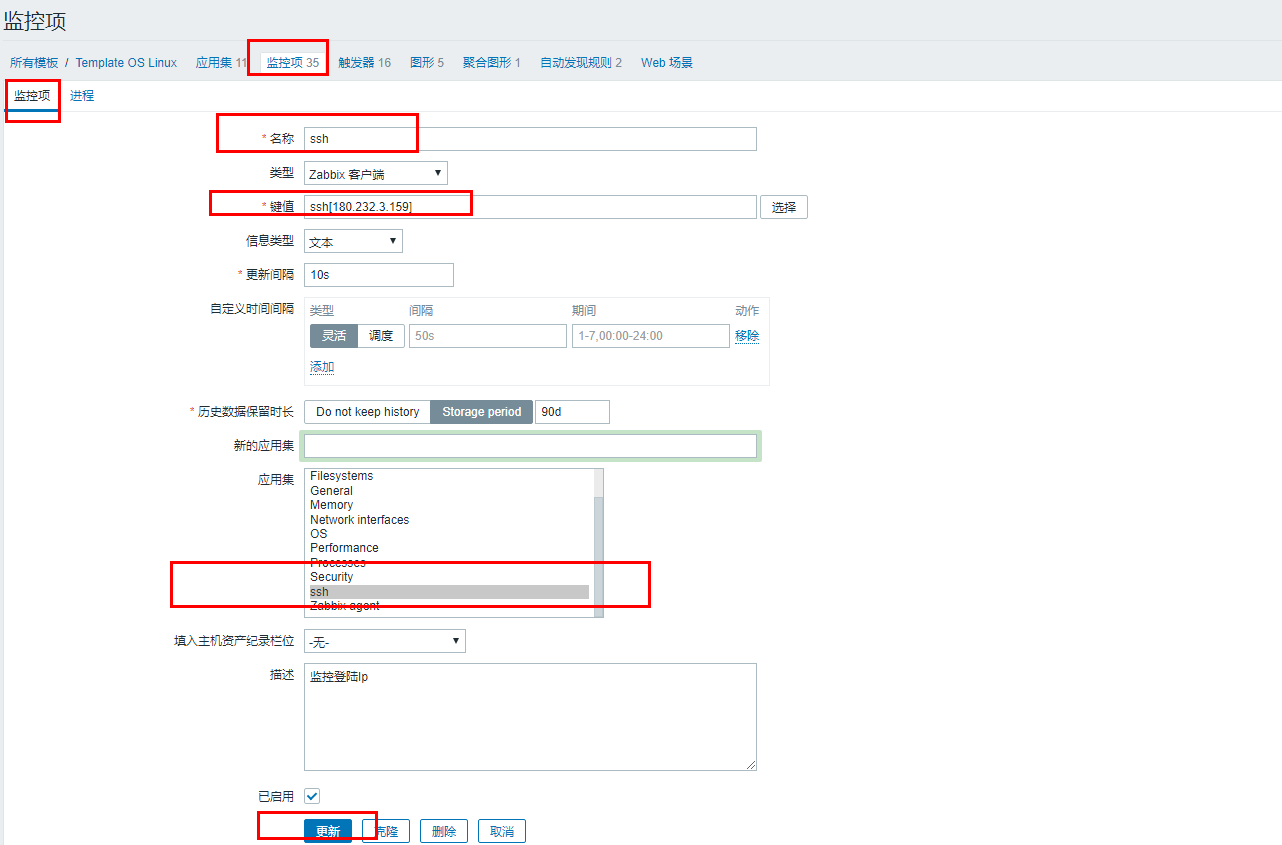
|  |
| --- |
| UserParameter=ssh[\*],python /usr/local/zabbix/scripts/illegalIP.py $1 |

**=======================================**

修改zabbix web

**添加监控项**

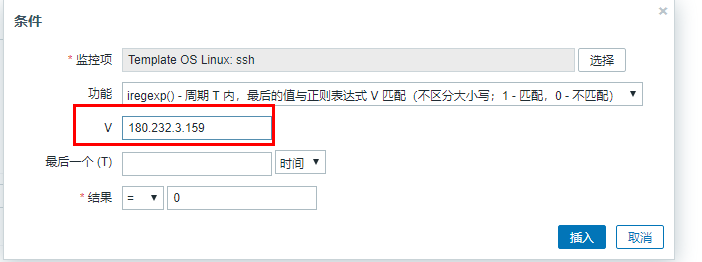
配置>模板>[Template OS Linux](http://zabbix.yunfan.com/templates.php?form=update&templateid=10001)>



ssh["IP"]#多个IP用空格隔开,添加白名单IP,非白名单IP则会警报

**添加触发器**

表达式：多个IP用空格隔开与上面加的IP要一样且顺序相同





参考URL:<https://blog.csdn.net/weixin_33894992/article/details/94506742>