

告警规则

1. 收敛架构图

- ①所有产生告警均由zabbix调用脚本推入缓存redis当中
- ②分析系统将在规定时间（1分钟）内去redis中拉取数据，根据定义好的一系列规则进行，合并、分析或直接丢弃，并存入分析平台数据库，以便供历史查询。
- ③根据预先定义好的规则将报警通过定义好的方式发送给相关人员

2. 配置

动作

操作

恢复操作

Update operations

* 名称

Send..weixin

计算方式

与/或（默认）

A and (B or C or D or E or F or G or H or I)

条件

标签	名称	动作
A	Problem is not suppressed	移除
B	主机群组 equals Hitaes-yongci	移除
C	主机群组 equals Hitaes-PAI-GD	移除
D	主机群组 equals Hitaes-ARCH	移除
E	主机群组 equals Hitaes-Liting	移除
F	主机群组 equals Hitaes-Commons	移除
G	主机群组 equals Hitaes-PAI	移除
H	主机群组 equals Hitaes-CNLU	移除
I	主机群组 equals Hitaes-National_Health	移除

新的触发条件

触发器名称

contains

[添加](#)

已启用

☒

* At least one operation, recovery operation or update operation must exist.

更新

克隆

删除

取消

* 默认操作步骤持续时间 1h

默认标题 {EVENT.ID}_1

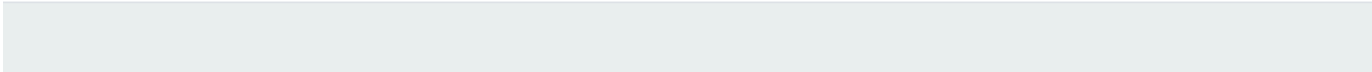
消息内容
triggervalue{TRIGGER.VALUE}#hostname{HOSTNAME1}#ipaddress
{IPADDRESS}#hostgroup{TRIGGER.HOSTGROUP.NAME}#triggerseverity
{TRIGGER.SEVERITY}#triggername{TRIGGER.NAME}#triggerkey
{TRIGGER.KEY1}#triggeritems{ITEM.NAME}#itemvalue
{ITEM.LASTVALUE}#itemid{ITEM.ID}#eventid{EVENT.ID}#eventage
{EVENT.AGE}#eventtime{EVENT.DATE} {EVENT.TIME}

Pause operations for suppressed problems ☒

步骤	细节	开始于	持续时间	动作
1	发送消息给用户: test 通过 Email_v1_py	立即地	默认	编辑 移除
新的				

* At least one operation, recovery operation or update operation must exist.

[更新](#) [克隆](#) [删除](#) [取消](#)



动作 操作 恢复操作 Update operations

默认标题 {EVENT.ID}_0

消息内容
triggervalue{TRIGGER.VALUE}#hostname{HOSTNAME1}#ipaddress
{IPADDRESS}#hostgroup{TRIGGER.HOSTGROUP.NAME}#triggerseverity
{TRIGGER.SEVERITY}#triggername{TRIGGER.NAME}#triggerkey
{TRIGGER.KEY1}#triggeritems{ITEM.NAME}#itemvalue
{ITEM.LASTVALUE}#itemid{ITEM.ID}#eventid{EVENT.ID}#eventage
{EVENT.AGE}#eventtime{EVENT.DATE} {EVENT.TIME}

操作

细节

发送消息给用户: test 通过 Email_v1_py

[编辑](#) [移除](#)

[新的](#)

* At least one operation, recovery operation or update operation must exist.

[更新](#) [克隆](#) [删除](#) [取消](#)

报警媒介类型 选项

* 名称

Email_v1.py

类型

脚本

* 脚本名称

police.py

脚本参数

参数

{ALERT.SUBJECT}

添加

动作

移除

已启用

☒

更新

克隆

删除

取消

报警媒介类型 选项

并发会话

壹

无限

习惯

* 尝试次数

3

* 尝试间隔

10s

更新

克隆

删除

取消

告警：

{EVENT. ID}_1
triggervalue| {TRIGGER. VALUE} #hostname| {HOSTNAME1} #ipaddress| {IPADDRESS} #hostgroup| {TRIGGER. HOSTGROUP. NAME} #triggerseverity| {TRIGGER. SEVERITY} #triggername| {TRIGGER. NAME} #triggerkey| {TRIGGER. KEY1} #triggeritems| {ITEM. NAME} #itemvalue| {ITEM. LASTVALUE} #itemid| {ITEM. ID} #eventid| {EVENT. ID} #eventage| {EVENT. AGE} #eventtime| {EVENT. DATE} {EVENT. TIME}

恢复：

{EVENT. ID}_0
triggervalue| {TRIGGER. VALUE} #hostname| {HOSTNAME1} #ipaddress| {IPADDRESS} #hostgroup| {TRIGGER. HOSTGROUP. NAME} #triggerseverity| {TRIGGER. SEVERITY} #triggername| {TRIGGER. NAME} #triggerkey| {TRIGGER. KEY1} #triggeritems| {ITEM. NAME} #itemvalue| {ITEM. LASTVALUE} #itemid| {ITEM. ID} #eventid| {EVENT. ID} #eventage| {EVENT. AGE} #eventtime| {EVENT. DATE} {EVENT. TIME}

参考链接：<https://www.jianshu.com/p/b29cf0682b58>