

# Zabbixtrigger 文档--VER 1.0

By 小伟

QQ: 141926620

技术交流: 142279493

技术博客: <http://nanwangting.blog.51cto.com/>

2012 年 10 月 27 日

## 目录

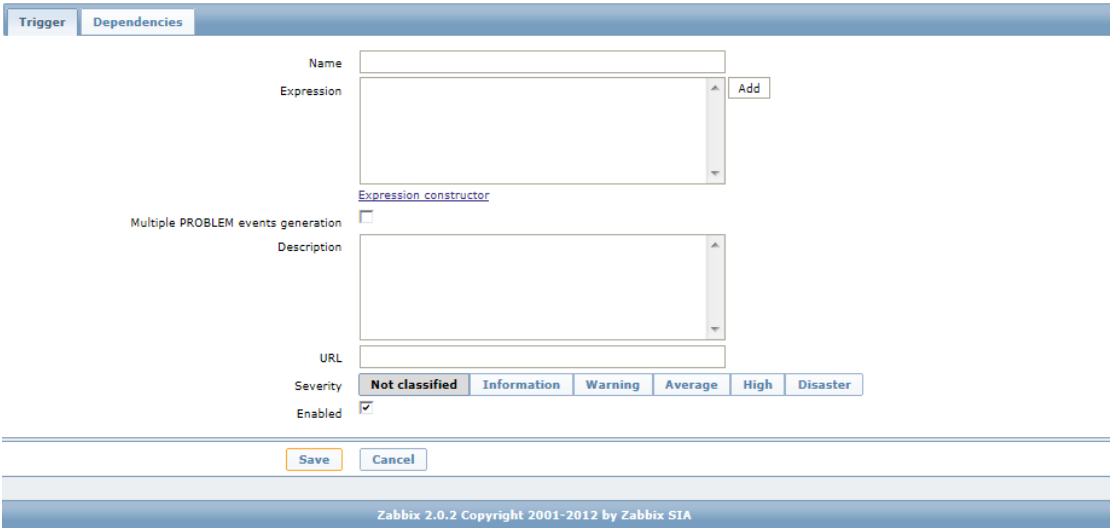
<b>第 1 章</b>	<b>TRIGGER .....</b>	<b>4</b>
1.1	创建一个 TRIGGER .....	4
1.2	TRIGGER 的表达式的使用 .....	4
1.3	操作符 .....	5
1.4	TRIGGER 实例 .....	5
1.5	TRIGGER SEVERITY (警报级别) .....	7
1.6	TRIGGER SEVERITY (警报级别) 的配置 .....	8
1.7	TRIGGER 支持的单位 .....	8



# 第1章 Trigger

## 1.1 创建一个 trigger

选择: Configuration→Host  
双击: Trigger  
双击: Create Trigger(位置在右上角)后图下图所示



Name	Trigger 的名字
Expression	添加 Trigger 表达式，双击 add 后添加
Description	对 trigger 的描述
Serverity	对 trigger 级别的选择
Enabled	Trigger 是否可用

双击 save 能进行保存，这样一个 trigger 就添加好了。

## 1.2 Trigger 的表达式的使用

Trigger 的表达式非常的丰富，我们可用使用 trigger 表达式完成非常复杂的报警时需要的逻辑关系。下面看一下 trigger 的语法。

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

大括号中包括的为主机名字以及对于的 key，我们选择相应的主机和 key 时系统自动生成了就，关键是后边部分。Function 为 trigger 使用的函数，以及函数相对应的参数。大括号后跟着的是 trigger 识别的操作符。

### 函数参数

大部分情况下如果参数只是一个数字的话往往代表着是秒的意思，如果前边加入#意思就不同了。

例:

函数及输入的参数	描述
Sum (600)	600 秒钟的和
Sum (#5)	最后 5 秒钟的和

同时我们可以使用 5m 代表 5 分钟来代替 300 秒, 1d 代表一天来替代 86400 秒, 1k 来代表 1024bytes。

### 1.3 操作符

下面表格为 trigger 可以使用的操作符

1	/	除以
2	*	乘以
3	-	减法
4	+	加法
5	<	大于
6	>	小于
7	=	等于
8	&	逻辑与
9		逻辑或

### 1.4 Trigger 实例

例 1: cpu 负载的监控 last 函数

主机 www.solutionware.com.cn Cpu 负载过高

{www.zabbix.com:system.cpu.load[all,avg1].last(0)}>5

注释: 其中 www.solutionware.com.cn:system.cpu.load[all,avg1]代表的监控项目, 其中主机位 www.solutionware.com.cn, 监控的项的 key 为 cpu.load[all,avg1], last()为函数代表最近时间段, 0 代表最后时间, 如果为 1 的话代表最近 1 秒钟。>为表达式这里不做说明, 5 代表大于的值。

例 2: cpu 过载的监控 last 函数

主机 www.solutionware.com.cn cpu 过载

www.solutionware.com.cn:system.cpu.load[all,avg1].last(0)}>5 | {www.solutionware.com.cn:system.cpu.load[all,avg1].min(10m)}>2

注释：主机 `www.solutionware.com.cn` 的 `cpu` 负载最近超过 5 或者主机 `www.solutionware.com.cn` 的 `cpu` 负载 10 分钟时间之内一直超过 2 则报警

例 3： `/etc/passwd` 发生改变 `diff` 函数

```
{www.solutionware.com.cn:vfs.file.cksum[/etc/passwd].diff(0)}>0
```

注释：这里用到了 `diff` 函数，同样这个例子还可以用到其他的地方，比如 `/etc/inetd.conf` 文件，`/kernel`, `etc` 下的文件等。

例 4： 网卡流量 `min` 函数

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

注释：主机 `www.solutionware.com.cn` 的网卡流量 5 分钟持续超过 100k 则报警。

例 5 测试所有节点的 `smtp` 服务

```
{smtp1.solutionware.com.cn:net.tcp.service[smtp].last(0)}=0&{smtp2.solutionware.com:net.tcp.service[smtp].last(0)}=0
```

注释：注意 `&` 表达式 2 侧的主机不同，例子的意思是：主机 `smtp1.solutionware.com.cn` 和主机 `smtp2.solutionware.com.cn` 的 `smtp` 服务停止则报警。

例 6 代理程序需要更新

```
{www.solutionware.com.cn:agent.version.str("beta8")}=1
```

注释：当主机 `www.solutionware.com.cn` 的代理程序需要更新的时候报警

例 7 主机 `ping`

```
{www.solutionware.com.cn:icmpping.count(30m,0)}>5
```

注释：当主机 `www.solutionware.com.cn`

### 例 8 心跳的测试 nodata()函数

`{www.solutionware.com.cn.tick.nodata(3m)}=1`

注释：这里监控类型必选选择 **zabbix trapper**.如果 3 分钟内心跳没数据则报警。

### 例 9cpu 负载在某时间段

`{www.solutionware.com.cn:system.cpu.load[all,avg1].min(5m)}>2&{www.solutionware.com.cn:system.cpu.load[all,avg1].time(0)}>000000&{www.solutionware.com.cn:system.cpu.load[all,avg1].time(0)}<060000`

注释：在 **at night (00:00-06:00)**这一时间段如果主机 [www.solutionware.com.cn](http://www.solutionware.com.cn) 在 5 分钟之内的负载一直大于 2 则报警

### 例:10 数据库时间检测

`{MySQL_DB:system.localtime.fuzzytime(10)}=0`

注释：如果数据库 **mysql\_db** 的时间和系统时间 10s 钟一直不一致则报警。

## 1.5Trigger severity(警报级别)

Trigger severity 用来显示 Trigger 的级别，zabbix 支持一下几个警报级别。

级别		颜色
Not classified	未知	Grey
Information	系统信息	Light green
Warning	警告	yellow
Average	一般性问题	orange
High	严重警告	red
Disaster	数据丢失	Bright red

分级别的目的：1 不同的警报代表不同的颜色

2 声音警报，不同的级别的可以用不同的声音做警报提示。

3 不同的级别使用不同的报警通知方式，比如 **sms email.....**

# 1.6Trigger severity(警报级别)的配置

级别 的名称和颜色是可以随心配置的，Administration-->General → Trigger severities, 如下图所示，修改名称和颜色后保存即可。

Custom severity

Colour

Not classified

Not classified

DBD8DB

Information

Information

D6F6FF

Warning

Warning

FFF6A5

Average

Average

FFB689

High

High

FF9999

Disaster

Disaster

FF3838

Info

Custom severity names affect all locales and require manual translation!

Save

Reset defaults

# 1.7Trigger 支持的单位

s	秒	h	小时
m	分	d	天
w	星期	K	Kilo
M	mega	G	giga
T	tera	P	peta
E	exa	Z	zetta
Y	yotta		

例:

```
host:zabbix[proxy,zabbix_proxy,lastaccess]}>120
{host:system.uptime[.last(0)}<86400
{host:system.cpu.load.avg(600)}<10
等价于
{host:zabbix[proxy,zabbix_proxy,lastaccess]}>2m
{host:system.uptime.last(0)}<1d
{host:system.cpu.load.avg(10m)}<10
```

只所以弄单位主要还是为了方便书写



