Security-06

服务安全与监控

# Zabbix报警机制

## 概念介绍

自定义的监控项默认不会自动报警

首页也不会提示错误

需要配置触发器与报警动作才可以自定报警

### 触发器（tigger)

### 表达式，如内存不足300M，用户超过30个等

### 当触发条件发生后，会导致一个触发时间

### 触发事件会执行某个动作

### 动作(action)

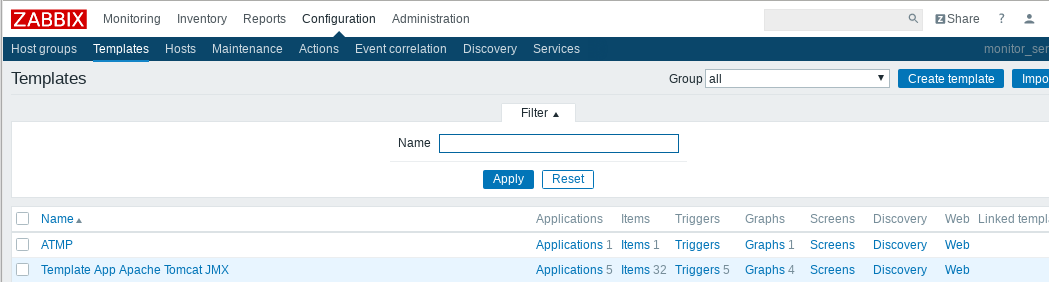
### 触发器的条件被触发后的行为可以是发送邮件，也可以是重启某个服务等

## 创建触发器

通过Configuration—>Templates

选择模版点击后面的Triggers—>Create trigger-找到我们之前创建的ATMP模板，点击模板后面的triggers

- 强烈建议使用英文创建（中文翻译不敢恭维）



### 触发器表达式

### Expression表达式：触发异常的条件

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

{主机：key.函数(参数)}<表达式>常数

### Expression表达式案例

大多数函数使用秒作为参数，使用#代表不同含义

avg,count,last,min and max函数支持额外的第二个参数time\_shift(时间偏移量)

这个参数允许从过去一短时间内引用数据

|  |  |
| --- | --- |
| 函数内容 | 描述 |
| sum(600) | 600秒内所有值的总和 |
| sum(#5) | 最后5个值的总和 |
| last(20) | 最后20秒的值 |
| last(#5) | 倒数第5个值 |
| avg(1h,1d) | 一天前的1小时的平均值 |

**如果web1主机最新的CPU平均负载值大于5，则触发器状态Problem**

{web1:system.cpu.load[all,avg1].last(0)}>5 //0为最新数据

**根分区，最近5分钟的最大容量小于10G，则状态进入Problem**

{vfs.fs.size[/,free].max(5m)}<10G //5m为最近5分钟

**最新一次校验/etc/passwd如果与上一次有变化，则状态进入Problem**

{vfs.file.cksum[/etc/passwd].diff(0)}>0 //0为最新数据

## 配置触发器

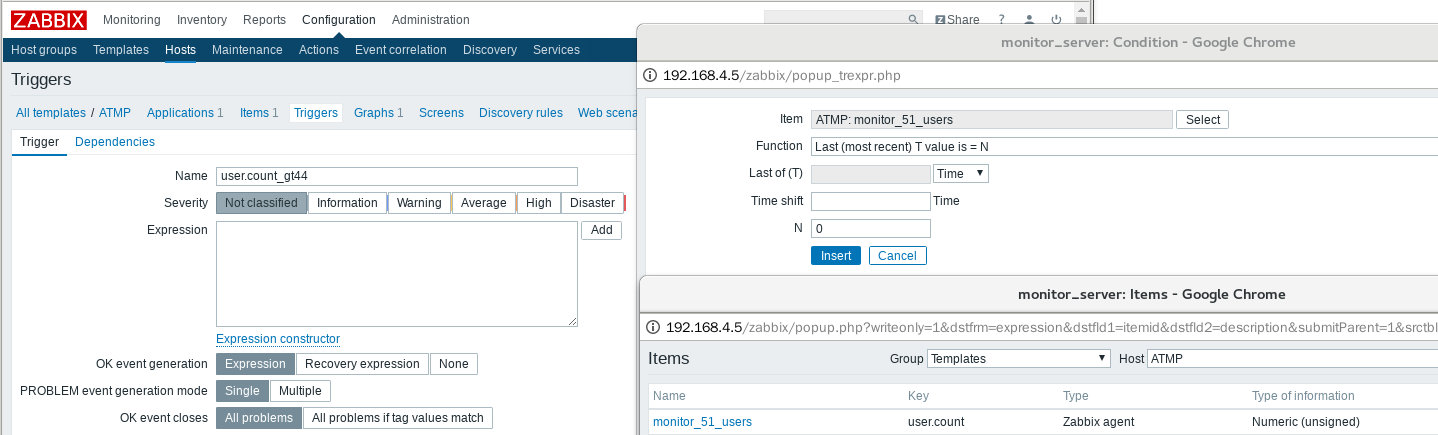
设置触发器名称，点击add添加表达式

填写表达式

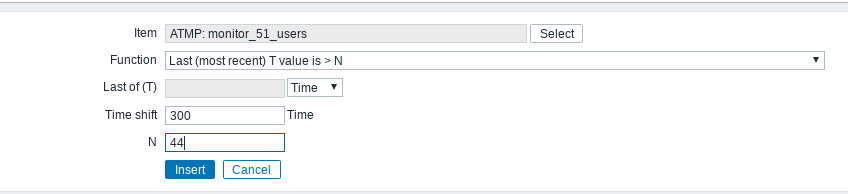
监控项为账户数量，最近300秒账户数量大于44

**配置-Templates-Triggers-Create Triggers**

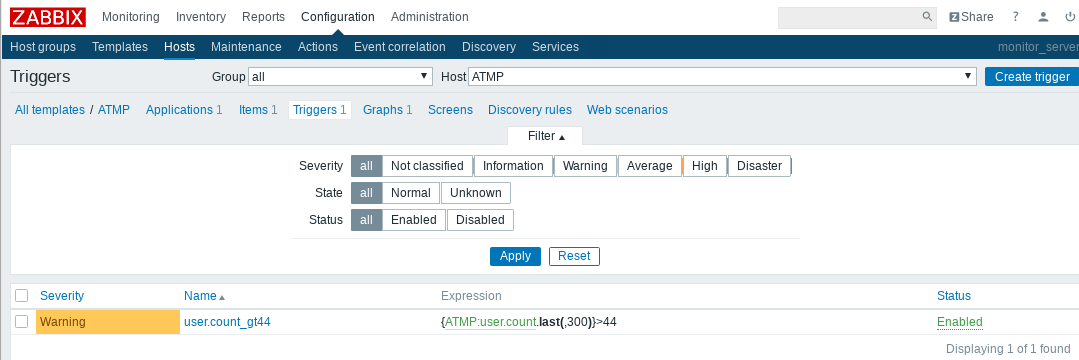
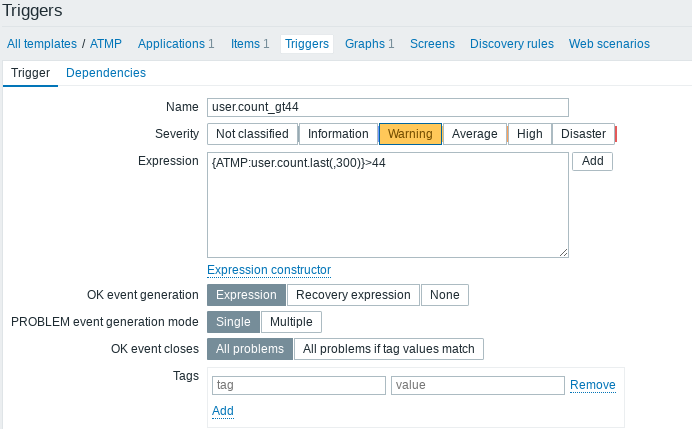
**Name自定义（知名晓义）-add-select-选择即可**



选择时间(Time shift)，条件(Function)-Insert



选择级别（Severity）-点击add



## 设置邮件

创建Media

通过Administration（管理）-->Media Type（报警媒体类型）-->选择Email（邮件）字样进入配置-完成之后更新即可



设置邮件服务器信息，设置邮件服务器及邮件账户信息



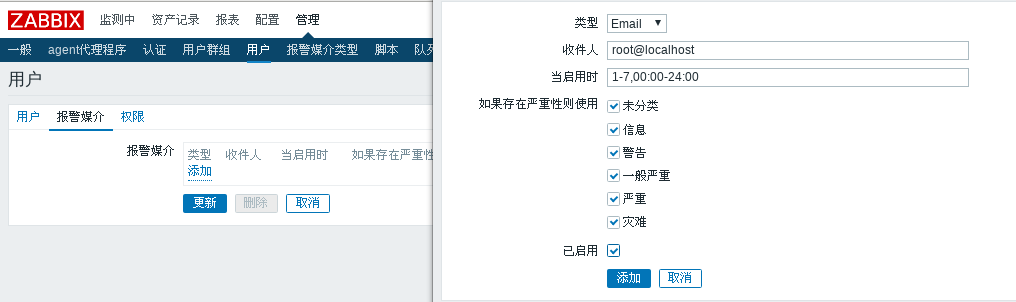
**为用户添加Media**

1.在Administration（管理）-->Users（用户）中找到选择admin账户

2.点击Admin账户后，在弹出的界面中选择Media（报警媒介）菜单-->点击Add(添加)报警媒介

3.点击Add（添加）后，在Meida Type中填写报警类型，收件人，时间等信息





**创建ACTION动作：**

**Action动作**

Action（动作）是定义当触发器被触发时的时候，执行什么行为。

通过Configuration（配置）-->Actions（动作）-->Create action（创建动作）

**配置Action动作的触发条件(触发器根据实际需要选择的即可)**

填写Action动作的名称，配置什么触发器被触发时会执行本Action动作（账户数量大于44）



**点击操作配置Action动作的具体行为**

配置动作的具体操作行为（发送信息或执行远程命令），无限次数发送邮件，60秒1次，发送给Admin用户

**点击新的-步骤-步骤持续时间-操作类型-添加用户/群组-仅送到-添加-添加**

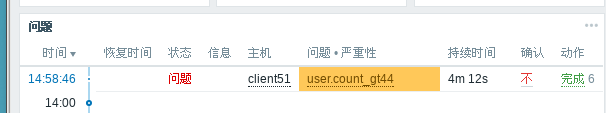




**测试效果**

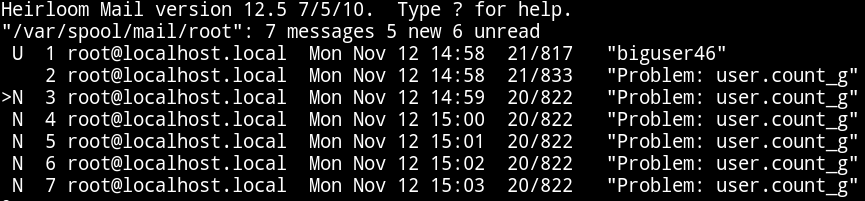
在被监控主机创建账户（让账户数量大于44），然后登录监控端Web页面，在仪表盘中查看问题报警（需要等待一段时间）

[root@client51 ~]# for i in {1..10}; do useradd user$i; done



查看报警邮件，在监控服务器上使用mail命令查收报警邮件

[root@node2 ~]# mail



# Zabbix进阶操作

## 自动发现

当Zabbix需要监控的设备越来越多，手动添加监控设备越来越有挑战，此时，可以考虑使用自动发现功能

需要批量一次性添加一组监控主机，也可以使用自动发现功能

### 自动发现功能的实现

自动发现、添加主机，自动添加主机到组

自动连接模版到主机，自动添加监控项目与图形等

### 自动发现(Discovery)流程

创建自动发现规则

常见Action动作，说明发现主机后自动执行什么动作

通过动作，执行添加主机，链接模版到主机等操作

### 自动发现规则

创建自动发现规则

- Configuration(配置)—>Discovery(自动发现)—>Create discovery rule

填写规则

自动发现的IP范围（逗号隔开可以写多个）

多久做一次自动发现（默认1小时，仅实验修改为1m）

检查的方式：HTTP、FTP、Agent的自定以key等检查





创建动作

Configuration—>Actions

Event source (Discovery)—>Create action

注意：选择事件源为：自动发现

添加动作名称，添加触发动作的条件

操作(触发动作后要执行的操作指令)，操作细节如下：

添加主机到组，与模版链接(HTTP模版)



添加新的触发条件-添加



点击操作-新的（添加主机到群组、链接到模版）-添加-添加



### 创建新的主机

创建一台新的主机，验证zabbix是否可以自动发现该主机

可以重新部署一台新的虚拟机，也可以将旧虚拟机的IP地址，临时修改为其他IP

登录Zabbix服务器的Web页面，查看主机列表



## 主被动监控

### 概述

主动和被动都是对被监控端主机而言的

默认zabbix采用的是被动监控

- 被动监控：Server向Agent发起连接，发送监控key，Agent接受请求，响应监控数据

- 主动监控：Agent向Server发起连接，Agent请求需要监测的监控项目列表，Server响应Agent发送一个items列表，Agent确认受到监控列表，TCP连接完成，会话关闭，Agent开始周期性的收集数据

### 区别

- Server不用每次需要数据都连接Agent，Agent会自己收集数据并处理数据，Server仅需要保存数据即可

当监控主机达到一定量级后，Zabbix服务器会越来越慢，此时，可以考虑时用主动监控，释放服务器的压力；另外，Zabbix也支持分布式监控，也是可以考虑的方案

### 创建新的主机

创建新的被监控主机（主动监控）；安装zabbix\_agent软件

[root@client50 ~]# vim /usr/local/etc/zabbix\_agentd.conf

#Server=127.0.0.1,192.168.4.5 //注释该行，允许谁监控本机

StartAgents=0 //被动监控时启动多个进程

//设置为0，则禁止被动监控，不启动zabbix\_agentd服务

ServerActive=192.168.4.5

//允许哪些主机监控本机（主动模式），一定要取消127.0.0.1

Hostname=client50

//告诉监控服务器，是谁发的数据信息

//一定要和zabbix服务器配置的监控主机名称一致（后面设置）

RefreshActiveChecks=120 //默认120秒检测一次

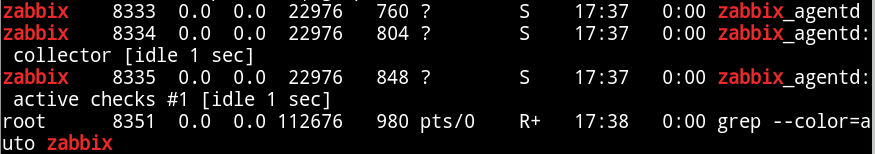
Include=/usr/local/etc/zabbix\_agentd.conf.d/

UnsafeUserParameters=1

[root@client50 ~]# killall zabbix\_agentd

[root@client50 ~]# zabbix\_agentd

[root@client50 ~]# ps aux | grep zabbix //可以查到进程



[root@client50 ~]# ss -natpul | grep zabbix //无监听端口号

### 克隆模版

为了方便，克隆系统自带模版（在此基础上就该更方便）

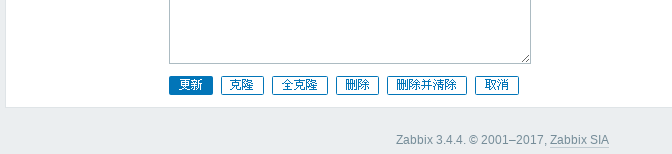
Configuration—>Templates

选择Template OS Linux

全克隆该模版，新建一个新的模版

新模版名称为：Template OS Linux ServerActive,点击添加即可







### 修改监控项模式

**将模版中的所有监控项目全部修改为主动监控模式**

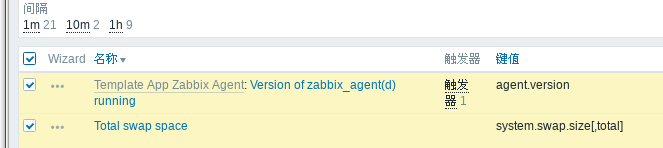
Configuration—>Templates

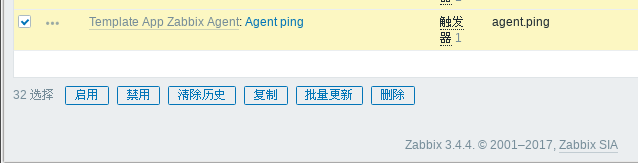
选择新克隆的模版，点击后面的Items（监控项）

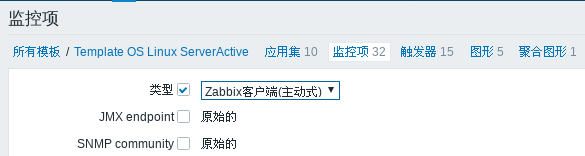
点击全选，选择所有监控项目，点击批量更新

将类型修改为：Zabbix Agent（Active主动模式）









批量修改监控项的监控模式后，并非所有监控项目都支持主动模式

批量修改后，会发现有几个没有修改主动模式成功

说明，这些监控项目不支持主动模式，关闭即可

可以点击类型排序，方便操作，点击状态即可关闭

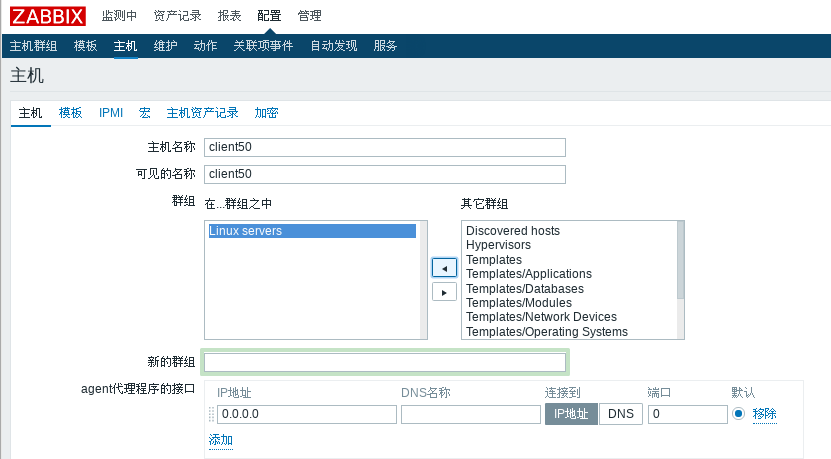


### 添加监控主机

1）手动添加监控主机（主动模式监控）

在Zabbix监控服务器，添加被监控的主机（主动模式）

设置主机名称：zabbixclient\_web2 （必须与被监控端的配置文件Hostname一致），将主机添加到Linux servers组，IP地址修改为0.0.0.0，端口设置为0

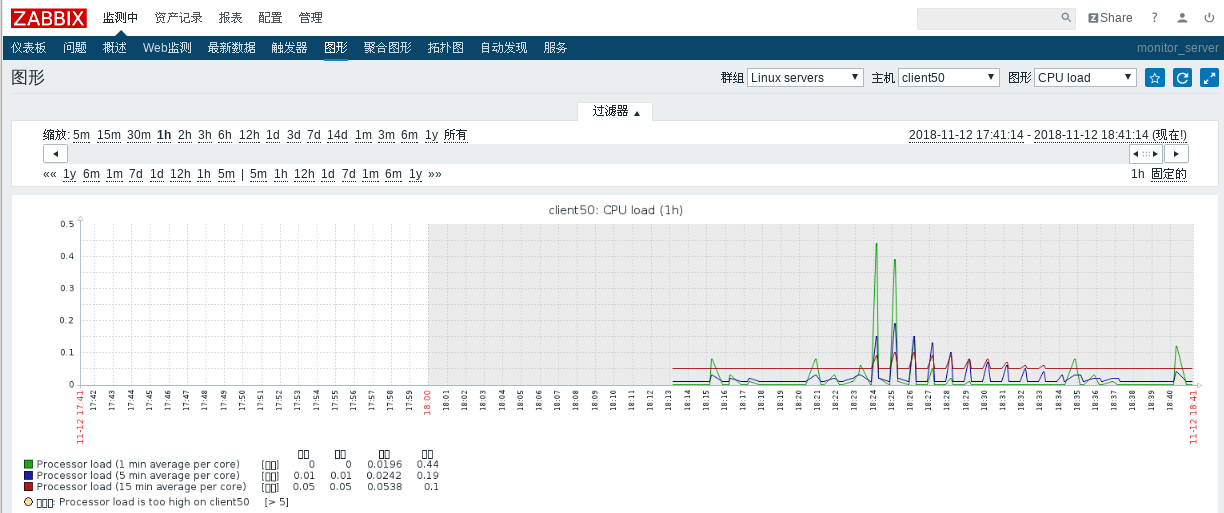


为主机添加监控模板，选择刚刚创建的模板（主动模式），添加链接模板到主机



2）验证监控效果

查看数据图表，通过Monitoring-->Graphs菜单，选择需要查看的主机组、主机以及图形，查看效果



CPU、内存等其他数据可用正常获取，但是，查看分区图表时并无数据，因为分区数据采用的是自动发现监控，与普通监控项一样，修改为主动模式即可，选择Template OS Linux ServerActive模板，修改Discovery自动发现为主动模式。





## 拓扑与聚合图形

### 拓扑图

绘制拓扑图可以快速了解服务器架构

Monitoring—>Maps（拓扑图）

选择默认的Local network拓扑图，编辑即可

Icon（图标），添加新的设备后可以点击图标修改属性

Shape（形状）

Link（连线），先选择两个图标，在选择连线

完成后，点击Update（更新）

### 聚合图形

**在一个轧棉显示多个数据图表，方便了解多组数据**

**Monitoring—>Screens（聚合图形）—>Create screen**

- Owner:使用默认的Admin用户

- Name:名称设置

- Columns:列数设置为2列

- Rows:行数设置为4行