--

监控

流程如下：

1,收集信息，对监控主机，服务等进行检测,记录相关信息

2,图形表现 展现给用户

3,邮件(短信，微信等)报警。 通知用户

4,开发接口(写程序自定义监控） 开源产品仅仅提供基本功能，需要定制开发

开源的监控软件

mrtg \*\* 老产品

ntop \*\* 老产品

cacti \*\* 前几年很多，仙人掌 www.cacti.net。 图形表现好。Nagios报警好。通过与Nagio结合，利用Nagio的报警+cacti的图形。

nagios \*\* 多年流行软件

zabbix \*\* 目前最流行的软件

Ganglia \*\* 老师也没有用过

centreon \*\* Nagios整合版本

监控宝 \*\* www.jiankongbao.com

360监控 \*\* 云市场监控软件

阿里云监控 \*\* 云市场监控软件

|2G

| -

| - -

|1G

|

---------------------------------------->

1 2 3 4 5 6 7

zabbix

============================================================================

zabbix服务器 －－》　zabbix agent(被监控端)

192.168.224.10 192.168.224.11

基本准备（系统平台为centos7.3)

1，主机名

# hostnamectl set-hostname --static server.com

# vim /etc/hosts

192.168.224.10 server.com

2，时间同步

3，iptables,selinux关闭

4，配置yum(本地镜像yum源和163源.可以不用epel源)

# wget http://mirrors.163.com/.help/CentOS7-Base-163.repo --163源

5, 配置zabbix官方yum源(版本为目前最新的版本zabbix3.2) 现在最新为4.3

# wget http://repo.zabbix.com/zabbix/3.2/rhel/7/x86\_64/zabbix-release-3.2-1.el7.noarch.rpm

# rpm -ivh zabbix-release-3.2-1.el7.noarch.rpm #安装官方 zabbix源

wget <http://repo.zabbix.com/zabbix/4.3/rhel/7/x86_64/zabbix-release-4.3-1.el7.noarch.rpm>

rpm -ivh zabbix-release-4.3-1.el7.noarch.rpm

也可以使用笔记站点提供的yum源仓库！

# vim /etc/yum.repos.d/zabbix.repo

[zabbix]

name=zabbix

baseurl=http://3.3.3.3/zabbixyum

gpgcheck=0

enable=1

总结:一共三个yum仓库(本地iso,163,zabbix官方)

更新 yum makecache fast

第一步:

安装zabbix和mariadb数据库

# yum install zabbix-server-mysql zabbix-web-mysql mariadb-server -y

第二步:

在mysql里建立存放数据的库并授权，然后导入zabbix所需要用的表和数据

# systemctl restart mariadb.service

# systemctl status mariadb.service

# systemctl enable mariadb.service

# mysql

MariaDB [(none)]> create database zabbix default charset utf8;

MariaDB [(none)]> grant all on zabbix.\* to zabbix@'localhost' identified by '123';

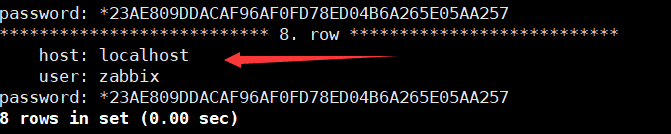
MariaDB [(none)]> flush privileges;

MariaDB [(none)]> use zabbix;

MariaDB [(none)]> show tables;

MariaDB [(none)]> use mysql;

MariaDB [mysql]> select host,user,password from user\G



MariaDB [(none)]> quit

第三步:

导入表数据

导入数据前记得打开防火墙

# zcat /usr/share/doc/zabbix-server-mysql-3.2.11/create.sql.gz |mysql -u zabbix -p123 zabbix

zcat /usr/share/doc/zabbix-server-mysql-4.4.0/create.sql.gz | mysql -u zabbix -p123 zabbix

第四步:

配置zabbix主配置文件，并启动服务

# vim /etc/zabbix/zabbix\_server.conf --找到并确认如下参数（默认值正确的可以打开注释也可以不打开 ，.默认值不对的，要修改正确并打开注释）

12 ListenPort=10051

91 DBHost=localhost

100 DBName=zabbix

116 DBUser=zabbix

124 DBPassword=123 --这里要对应上面的授权进行修改

131 DBSocket=/var/lib/mysql/mysql.sock --这里默认的socket路径不对，改成我这个路径

373 ListenIP=0.0.0.0

# systemctl restart zabbix-server.service

# systemctl status zabbix-server.service

# systemctl enable zabbix-server.service

# lsof -i:10051

第五步:

配置zabbix的httpd子配置文件,并启动httpd

# vim /etc/httpd/conf.d/zabbix.conf --打开时区注释，并修改成你的时区

php\_value date.timezone Asia/Shanghai

# systemctl restart httpd.service

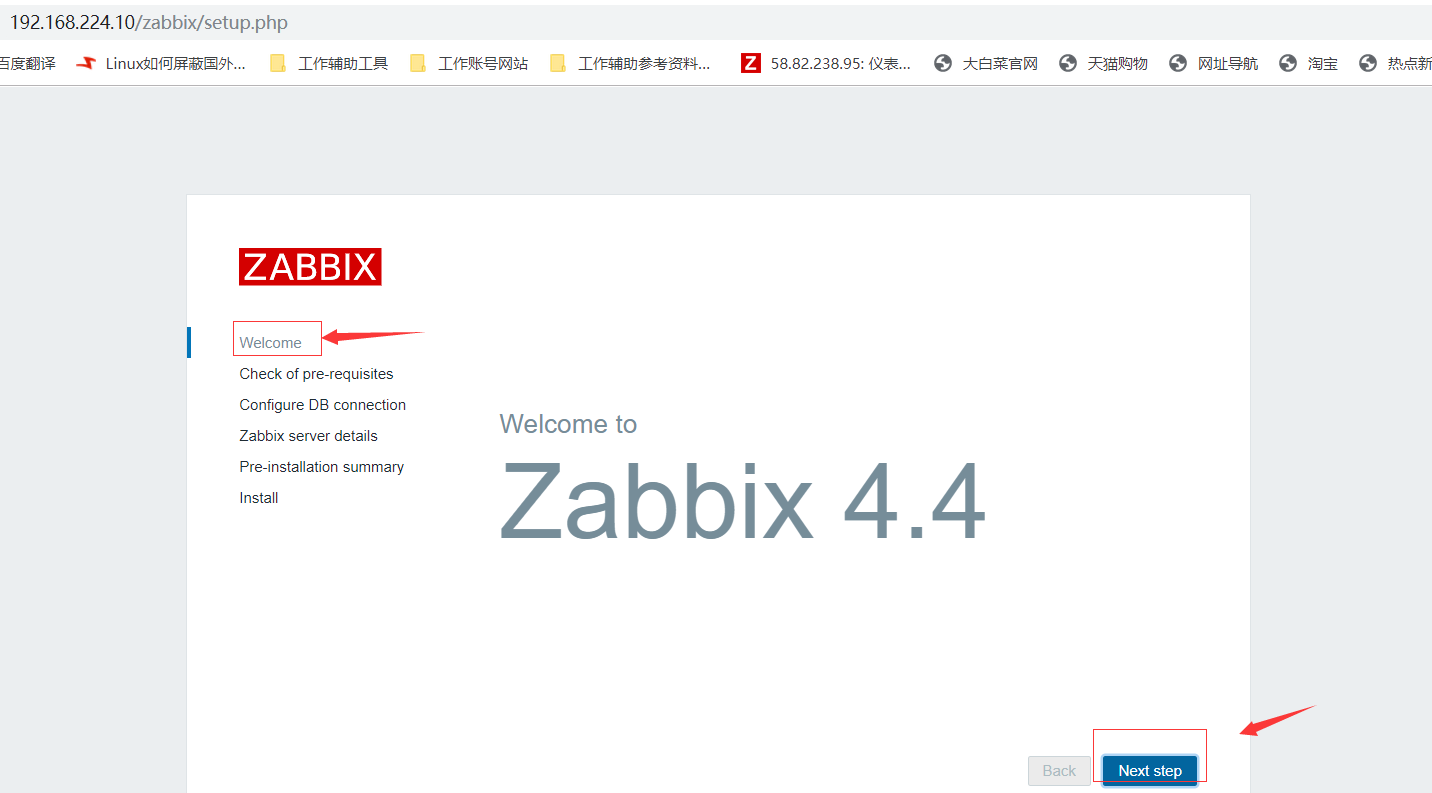
# systemctl status httpd.service

# systemctl enable httpd.service

第六步:

然后使用firefox访问，并进行安装

http://IP/zabbix http://192.168.224.10/zabbix



按照图示过程安装

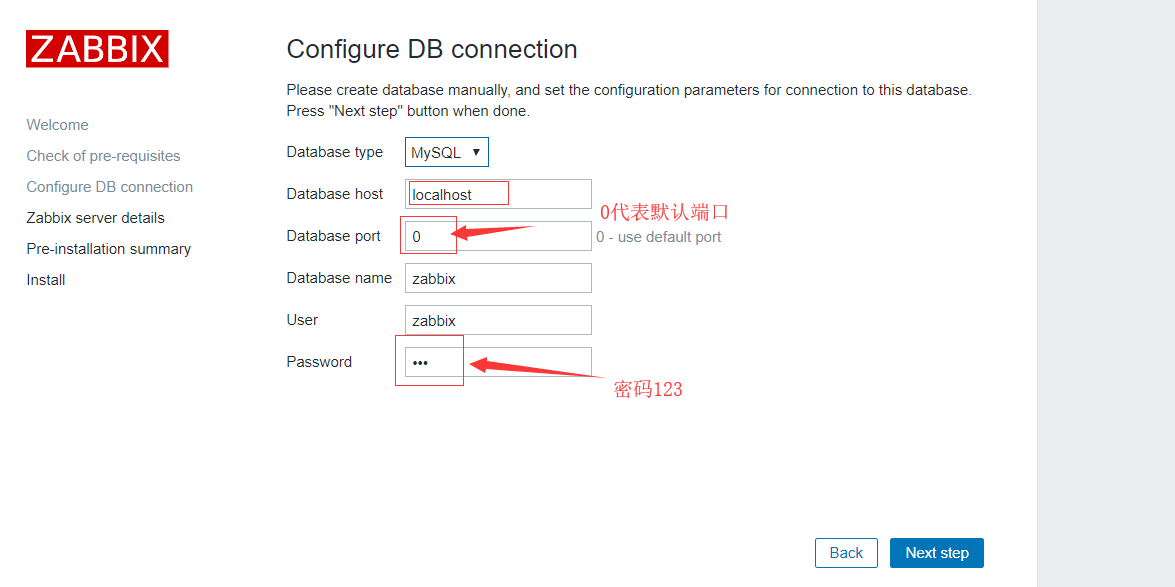
1,welcome

2,Check of pre-requisites

3,Configure DB connection

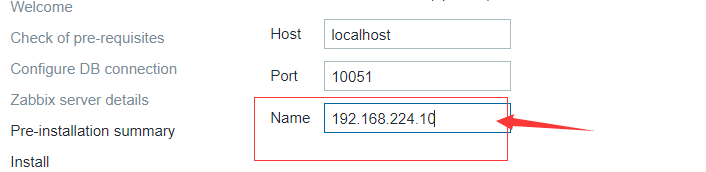
数据库用户名填zabbix,

密码填123（前面授权过的）



4,Zabbix server details

在name选项填上你zabbix服务器的IP或者主机名(server.com)



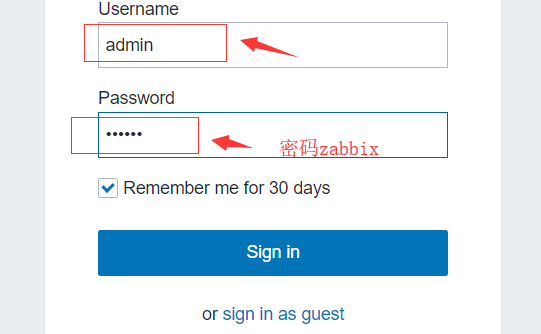
5,Pre-Installation summary

6,install

完成后

登陆用户名为:admin

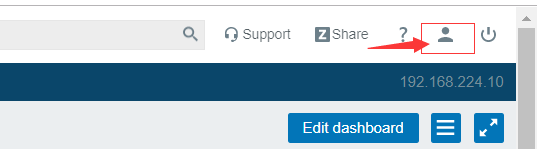
登陆密码为:zabbix

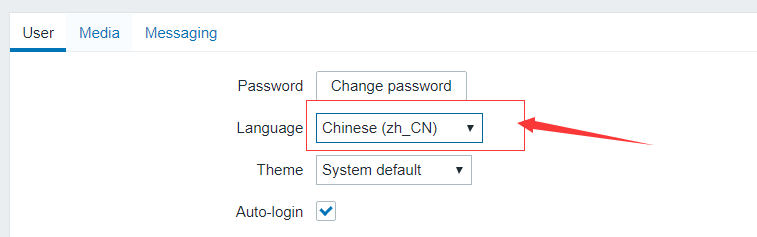


============================================================================

例一,转换成中文界面

右上角点一个类似小人的图标－－》 语言选 中文zh-cn －－》 点 update





例二,使用zabbix-agent方式来监控本机(在Zabbix Server执行)

# yum install zabbix-agent -y --本机安装agent包

# vim /etc/zabbix/zabbix\_agentd.conf --下面几个常见选项都为默认值，不用配置

95 Server=127.0.0.1 --zabbix服务器的IP，这里是本机(被动监控方式；这里的被动是相对于客户端而言，客户端被动接收服务器的监控）

103 ListenPort=10050 --监控服务器连接被监控客户端的端口

123 StartAgents=3 --如果设置为0，则禁用被动检查，

150 Hostname=server.com ----- 192.168.224.10 主机名字，加IP是为了好区分

180 HostMetadataItem=system.uname 定义用于获取主机元数据的项的可选参数

255 Timeout=10 定义超时时间，改为10秒

309 UnsafeUserParameters=1 允许使用，0是不允许

318 UserParameter= 自定义监控参数 可以定义多个

使用sed 来修改

sed -i 's/Server=127.0.0.1/Server=192.168.224.10/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/ServerActive=127.0.0.1/ServerActive=192.168.224.10/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/Hostname=Zabbix server/Hostname='$name' ----- '$ip'/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/# ListenPort=10050/ListenPort=10050/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/# HostMetadataItem=/HostMetadataItem=system.uname/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/# StartAgents=3/StartAgents=3/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/# Timeout=3/Timeout=10/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/# UnsafeUserParameters=0/UnsafeUserParameters=1/g' /etc/zabbix/zabbix\_agentd.conf

下面的这行自定义监控，查询当前访问日志异常ip访问登陆,指登录失败次数

sed -i 's/# UserParameter=/UserParameter=check\_failed,sh \/script\/check\_failed.sh/g' /etc/zabbix/zabbix\_agentd.conf

相关脚本

mkdir /script

vim /script/check\_failed.sh

#!/bin/bash

LOG\_PATH="/var/log/secure"

mon=$(date +%B)

h=$(date +%d)

ms=$(date +%H:%M)

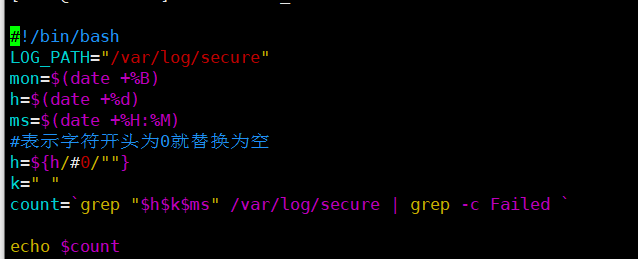
#表示字符开头为0就替换为空

h=${h/#0/""}

k=" "

count=`grep "$h$k$ms" /var/log/secure | grep -c Failed `

echo $count



# systemctl restart zabbix-agent

# systemctl status zabbix-agent

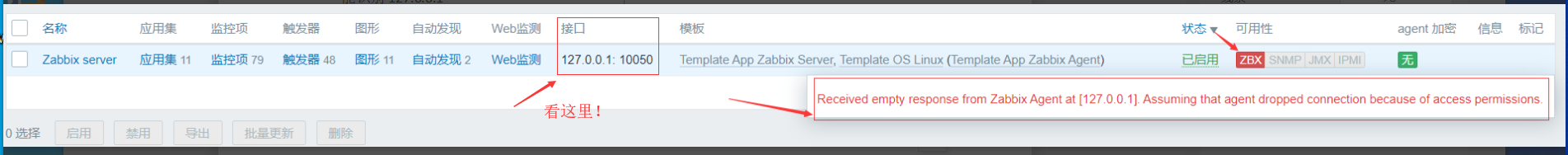
# systemctl enable zabbix-agent

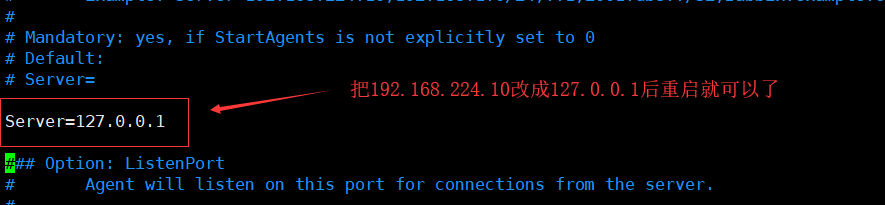
# lsof -i:10050

回到web管理界面－－》点配置－－》点主机－－》默认看到叫Zabbix server的本机，但状态是停用的－－》点击并启用. 在可用性中ZBX开始为灰色，等待变成绿色状态，大约几分钟。



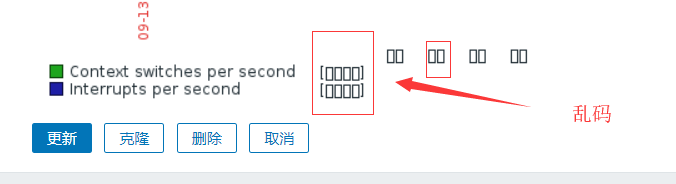
如果报这种错误，说明是防火墙导致连接失败，或者server识别不了ip 192.168.224.10,只能识别127.0.0.1





然后可以通过点图形－－》选图后点预览－－》看到图上有乱码

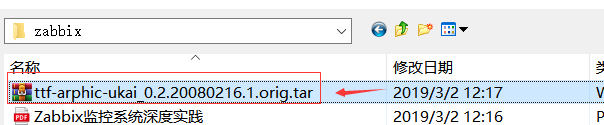




解决方法：

把原来的图形字符换成ukai字体

**上传这个包**



# tar xf ttf-arphic-ukai\_0.2.20080216.1.orig.tar.gz -C /usr/share/zabbix/fonts/

# mv /usr/share/zabbix/fonts/ukai.ttc /usr/share/zabbix/fonts/ukai.ttf

# vim /usr/share/zabbix/include/defines.inc.php

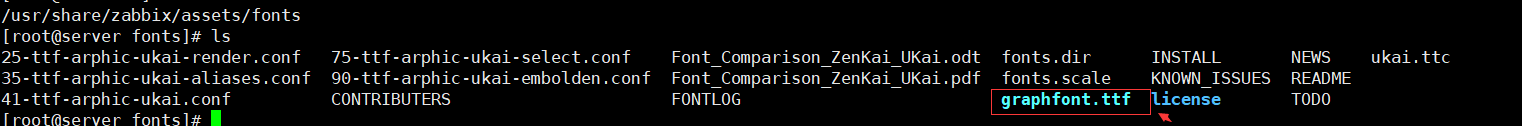
45行，修改为： define('ZBX\_GRAPH\_FONT\_NAME','ukai');

**Zabbix4.4版本fonts目录是在这个路径下**

/usr/share/zabbix/assets/fonts 所以需要解压

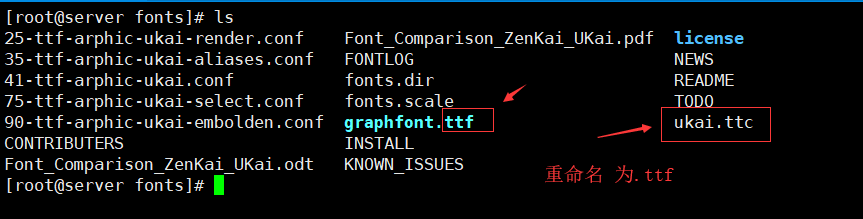
tar xf ttf-arphic-ukai\_0.2.20080216.1.orig.tar.gz -C /usr/share/zabbix/assets/fonts/

cd /usr/share/zabbix/assets/fonts 会多一些文件 ，除了红色的，其他全是解压出来的文件，



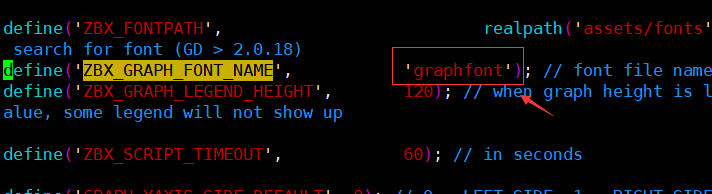
重命名为.ttf结尾，因为zabbix默认识别的是.ttf结尾的文件

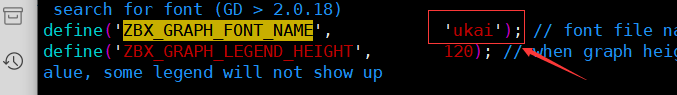
mv /usr/share/zabbix/assets/fonts/ukai.ttc /usr/share/zabbix/assets/fonts/ukai.ttf



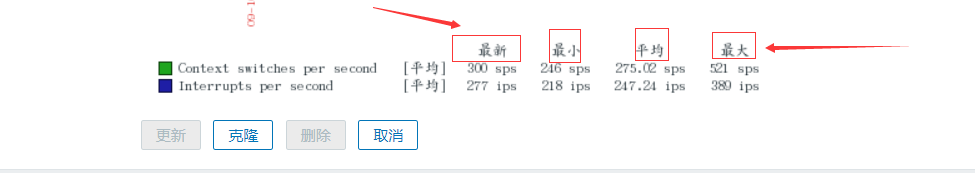
# vim /usr/share/zabbix/include/defines.inc.php

67行，修改为： define('ZBX\_GRAPH\_FONT\_NAME','ukai');





做完后，不用重启服务，回到zabbix的web界面刷新查看图形就会发现没有乱码了。Zabbix基于 rrd-tool开发，所以字体有兼容性。 从cacti开始国外软件对中文的兼容性就有问题。



例三，监控远程linux

zabbix服务器 －－》　zabbix agent(被监控端)

192.168.224.10 192.168.224.11

第一大步：

在被监控客户端上192.168.224.11安装zabbix-agent并配置

1,配置主机名

2,关闭iptables,selinux

3,时间同步

4,配置yum(需要zabbix官方yum源) **上面安装的是zabbix4.4的，这里也需要安装，版本不一样会监控不了**

# wget http://repo.zabbix.com/zabbix/3.2/rhel/7/x86\_64/zabbix-release-3.2-1.el7.noarch.rpm

# rpm -ivh zabbix-release-3.2-1.el7.noarch.rpm #安装官方 zabbix源

wget <http://repo.zabbix.com/zabbix/4.3/rhel/7/x86_64/zabbix-release-4.3-1.el7.noarch.rpm>

rpm -ivh zabbix-release-4.3-1.el7.noarch.rpm

5,安装zabbix-agent 写的是4.3版本，实际是4.4版本

# yum install zabbix-agent -y

# vim /etc/zabbix/zabbix\_agentd.conf

95 Server=192.168.224.10 --写上zabbix监控服务器的IP

103 ListenPort=10050 --监控的端口

147 Hostname=server1.com.com --写上你的被监控客户端的主机名

使用sed 来修改

sed -i 's/Server=127.0.0.1/Server=192.168.224.10/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/ServerActive=127.0.0.1/ServerActive=192.168.224.10/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/Hostname=Zabbix server/Hostname='$name' ----- '$ip'/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/# ListenPort=10050/ListenPort=10050/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/# HostMetadataItem=/HostMetadataItem=system.uname/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/# StartAgents=3/StartAgents=3/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/# Timeout=3/Timeout=10/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/# UnsafeUserParameters=0/UnsafeUserParameters=1/g' /etc/zabbix/zabbix\_agentd.conf

下面的这行自定义监控，查询当前访问日志异常ip访问登陆,指登录失败次数

sed -i 's/# UserParameter=/UserParameter=check\_failed,sh \/script\/check\_failed.sh/g' /etc/zabbix/zabbix\_agentd.conf

相关脚本 ：

mkdir /script

vim /script/check\_failed.sh

#!/bin/bash

LOG\_PATH="/var/log/secure"

mon=$(date +%B)

h=$(date +%d)

ms=$(date +%H:%M)

#表示字符开头为0就替换为空

h=${h/#0/""}

k=" "

count=`grep "$h$k$ms" /var/log/secure | grep -c Failed `

echo $count

加读权限， chmod +r /var/log/secure 要不然zabbix-server 访问不了，

# systemctl restart zabbix-agent

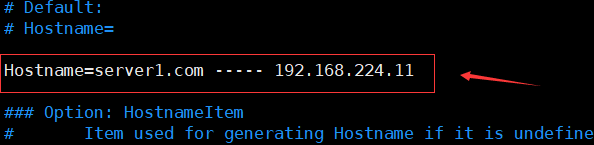
# systemctl status zabbix-agent

# systemctl enable zabbix-agent

# lsof -i:10050

第二大步：

回到zabbix服务器的web管理界面－－》点配置－－》点主机 －－》 点创建主机



主机名写里面配置的，

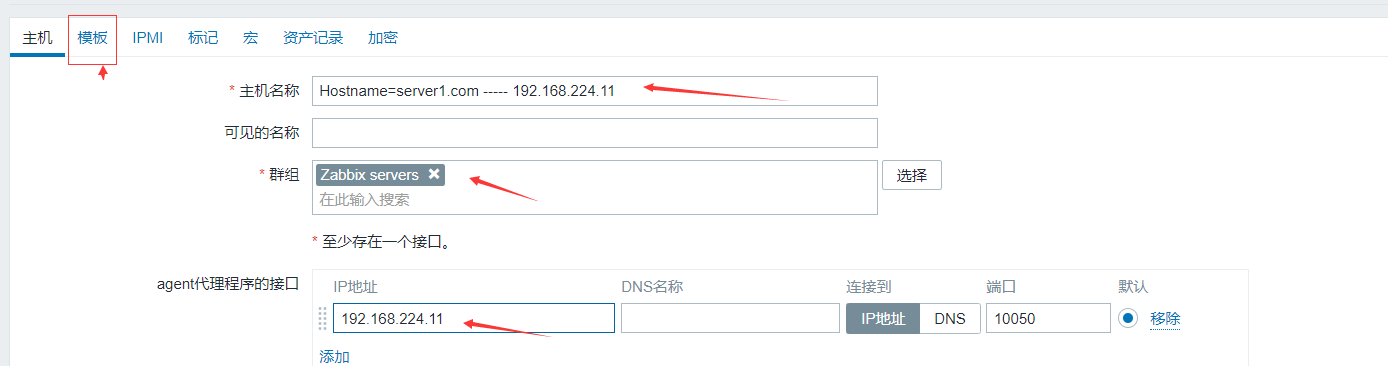
主机名称: server1.com.com

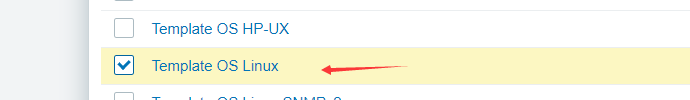
可见的名称:server1.com --这个名是优先显示在监控web页面的host页面

* 群组: Linux servers -- Zabbix servers

或者自己新建一个群组名都可以

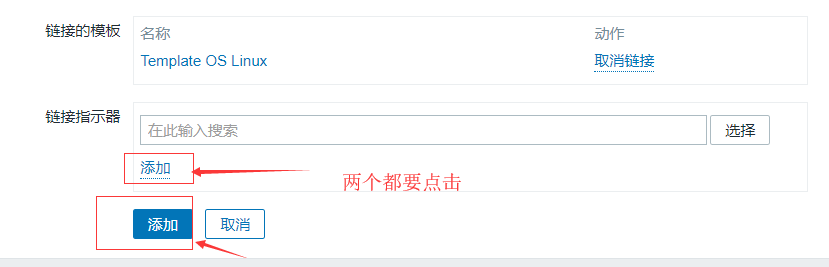
IP地址: 192.168.224.11





**可以导入本地的，模板，**

点模版，点选择,把 Template OS Linux　前面打勾(其它模版随意加)：(也可以先把模板增加一些监控项，后面的客户端就直接用这个修改过的模板就可以了)　－－》点选择 －－》点添加 --最后点右下角的添加

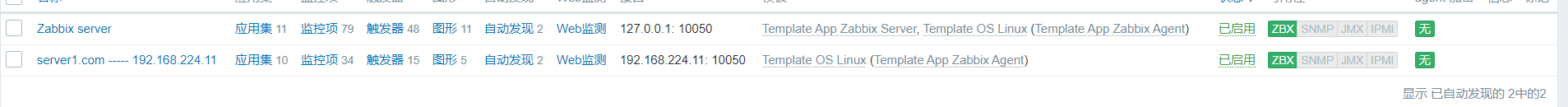




把名字改下，改成把前面的 Hostname= 去掉



OK之后，就能看到一共监控了两台机器了



注意：如果server1.com 的 ZBX一直是红色的报错，可能和防火墙和selinux，还有zabbix-server服务端IP有多个

导致连不上server1.com有关。ip a del ip/24 dev ens33 删除多的ip

===========================================================================

基本概念解析:

概念一: 用户与群组

用户(user)

　 用户群组(group)

管理->用户

管理->用户群组

题目:添加一个用户群组叫usergroup1,再添加一个用户叫张三，加入usergroup1组和Zabbix administrators组

概念二:主机和主机组

　　主机(hosts)代表被监控的一台机器

　　主机组(hostgroups)代表被监控的一组机器（主要在特别多的机器情况，方便分组区分)

操作路径:

配置->主机群组

配置->主机

题目:把前面做的server1.com这个被监控端换一个新的组，组名为hostgroup1,再把linux servers组删除

概念三:

监控项(items)和应用集（applications)

监控项(items)代表搜集数据或监控的一个最小单位

应用集（applications)代表多个监控项目合成的组

配置->主机->监控项（这里我选的是远程叫server1.com的主机的监控项)->右上角点创建监控项

然后先随意创建一个监控项 例如：vm.memory.size[<mode>] 键值内容为内存大小

创建完成后，在这个主机的监控项列表里就可以找到你创建的监控项

配置－>主机->图形(还是选的agent1的主机的图形)->右上解点创建图形

选择图形名称，并在下面添加刚才定义好的监控项

例:自定义自己的监控项

zabbix服务器 －－》　zabbix agent(被监控端)

192.168.224.10 192.168.224.11

zabbix server server1.com

自定义监控server1.com(192.168.224.11)上的用户登录数(默认有一个键值叫system.users.num可以实现监控登录用户数，但我这里实验使用的是自己定义的键值)

1,在被监控端server1.com上，随意多打开几个终端

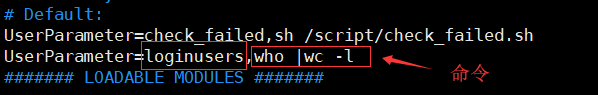
# who |wc -l

14

2,在被监控端server1.com上，定义用户参数

# vim /etc/zabbix/zabbix\_agentd.conf --加上下面这名定义的参数

293行 UserParameter=loginusers,who | wc -l --loginusers是我自定义的一个键值名称（会在创建监控项时用到),后面的who |wc -l就要被监控的命令

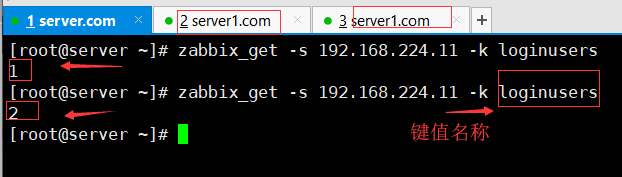


# systemctl restart zabbix-agent --重启服务让其生效

3,命令行测试自定义的测试项目是否可以工作。在服务器端执行

# yum install zabbix-get -y --需要zabbix-get 软件包官方yum源

# zabbix\_get -s 192.168.224.11 -k loginusers --使用此命令就可以得到被监控端的结果，则测试ok

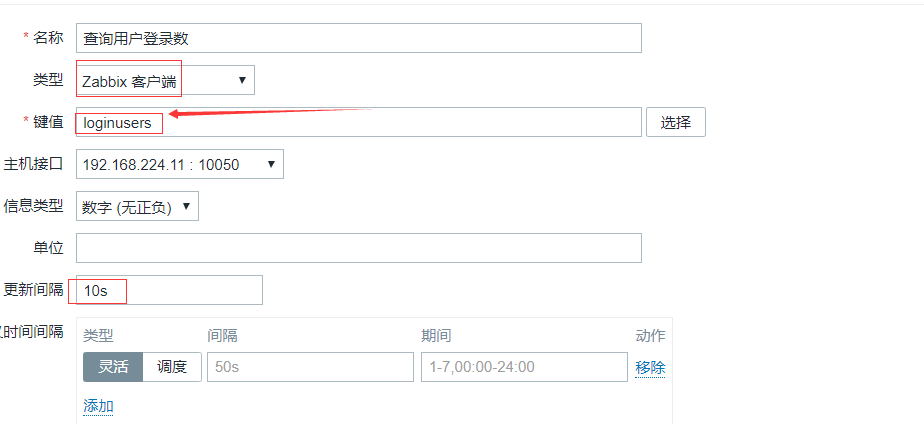


4，web界面创建这个监控项

配置->主机->监控项（选远程server1.com的监控项)->右上角点创建监控项

创建时主要要注意的是键值要写上面定义的loginusers

创建完后，在server1.com的监控项列表里就能看到创建好的监控项



然后为这个监控项创建图形

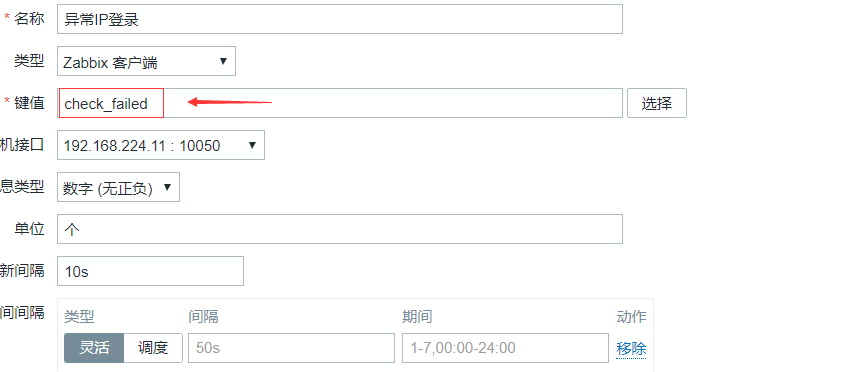
配置－>主机->图形(还是选的server1.com的主机的图形)->右上角点创建图形－>选择图形名称，并在下面添加刚才定义好的监控项－－添加后，预览图形



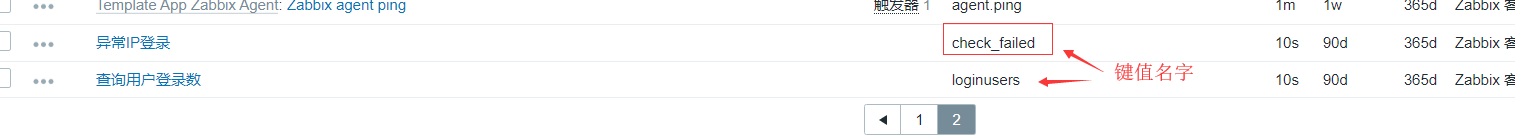
创建异常IP 登录这个监控项

配置->主机->监控项（选远程server1.com的监控项)->右上角点创建监控项

创建时主要要注意的是键值要写上面定义的check\_failed



创建完后，在server1.com的监控项列表里就能看到创建好的监控项



然后为这个监控项创建图形

配置－>主机->图形(还是选的server1.com的主机的图形)->右上角点创建图形－>选择图形名称，并在下面添加刚才定义好的监控项－－添加后，预览图形

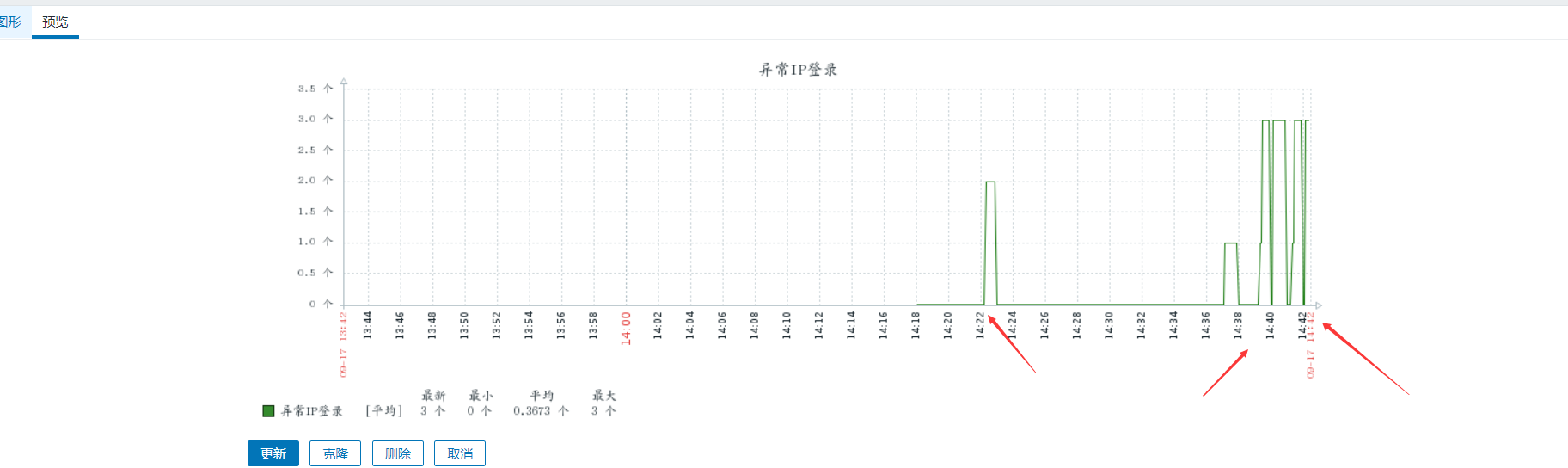


进行本地测试，server.com SSH 访问测试，ssh 之前先开通防火墙源端口进来，

iptables -A INPUT -p tcp -m multiport --sports 22 -j ACCEPT

iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT 这条也可以，表示状态是已连接的，就可以进来

然后连接ssh [root@192.168.224.11](mailto:root@192.168.224.11) 密码故意输错 再看下web端的监控变化，会发现上面有监控异常ip登录次数



练习:

自定义监控系统(server1.com)所有进程数量

UserParameter=totalprocs,ps -ef | awk 'NR>1 {print $0}' |wc -l

Note:

NR>1 -- 行号大于一

awk 'NR>1 {print $0}' -- 行号大于一的内容输出

自定义监控系统(server1.com)mariadb的当前登录用户数

# yum install mariadb\\*

# systemctl restart mariadb

# systemctl enable mariadb

UserParameter=mariadb\_loginusers,echo $[`mysqladmin -u root processlist |wc -l`-4]

Notes:

mysqladmin -u root processlist 列出当前登陆mysql的用户列表。

概念四:

可视化图形 Visualisation

指图形和图形里的定义(高，宽，坐标，X,Y的单位，颜色)的综合

我们使用监控项已经创建过相关的图形

概念五:

触发器trigger

定义监控项到达一个临界值或者满足一个条件，就会发现状态变化

例:把上面做的远程server1.com的监控登录用户数做一个触发器（大于5个登录用户就警告)

配置->主机->触发器（选远程server1.com的触发器)->右上角点创建触发器－>填触发器名称－>在表达式的右边点添加

选择上面做的监控server1.com的登录用户数的监控项，并设置最新的Ｔ值> N (N设为5)。



添加完表达式后，就可以添加这个触发器了

最后可以把server1.com的用户数调整大于5后，去web界面->监测中->触发器　界面可以查看到触发了

练习:

1监控系统(server1.com)所有进程数量，当大于250就警告，当大于400就一般严重

2监控系统(server1.com)mariadb的登录用户数，当大于50个就警告，当大于100就一般严重

概念六:

web监测(类似一个监控项)

　可以对一个url页面进行监测

例:监测server1.com的主页

1.配置->主机->web监测（选远程server1.com的web监测)->右上角点创建web场景->填写名称和加入一个应用集

2.点步骤，然后填写名称，URL(监控的页面的路径server1.com的ip),要求的状态码(我这里写的200，表示http协议的200状态码)

3.点添加后，就能看到server1.com这台机器的这个web监测场景

4.监测中->web监测，会看到此监测有问题（原因是server1.com没有安装httpd)

5.在server1.com上安装并启动httpd服务，做好主页，再回到监测中->web监测查看，监测就ok了，说明此监测有效

yum install -y httpd

systemctl restart httpd

echo hallo > /var/www/html/index.html

练习:为此web监测配置触发器

提示：检测项目 web.test.rspcode[web检测,portal page] 不为200，就表示错误。

表达式： {server1.com.com:web.test.rspcode[web检测,portal page].last()}<>200

概念七:

事件events

　　　各种需要管理员知悉或处理的事情(触发器事件，discovery事件，网络事件)

概念八:

自动发现(discovery)

动作(action)

例:再加一台client2远程被监控端，通过discovery+action发现它并加上相应的监控模版

zabbix server

192.168.224.10

server1.com client2

192.168.224.11 192.168.224.12

在client2机器上做如下相关的准备工作

1,配置主机名,并互相都要绑定主机名

# hostnamectl set-hostname --static server2.com

# vim /etc/hosts

192.168.224.12 server2.com

2,关闭iptables,selinux

3,时间同步 #rdate -s IPaddress.

4,配置yum(需要zabbix官方yum源)

# wget http://repo.zabbix.com/zabbix/3.2/rhel/7/x86\_64/zabbix-release-3.2-1.el7.noarch.rpm

# rpm -ivh zabbix-release-3.2-1.el7.noarch.rpm #安装官方 zabbix源

wget <http://repo.zabbix.com/zabbix/4.3/rhel/7/x86_64/zabbix-release-4.3-1.el7.noarch.rpm>

rpm -ivh zabbix-release-4.3-1.el7.noarch.rpm

5,安装zabbix-agent 写的是4.3版本，实际是4.4版本

# yum install zabbix-agent -y

# vim /etc/zabbix/zabbix\_agentd.conf

95 Server=192.168.224.10 --写上zabbix监控服务器的IP

103 ListenPort=10050 --被动监控的端口

136 ServerActive=192.168.224.10 --写上zabbix监控服务器的IP

147 Hostname=server2.com --写上你的被监控客户端的主机名

使用sed 来修改

sed -i 's/Server=127.0.0.1/Server=192.168.224.10/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/ServerActive=127.0.0.1/ServerActive=192.168.224.10/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/Hostname=Zabbix server/Hostname='$name' ----- '$ip'/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/# ListenPort=10050/ListenPort=10050/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/# HostMetadataItem=/HostMetadataItem=system.uname/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/# StartAgents=3/StartAgents=3/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/# Timeout=3/Timeout=10/g' /etc/zabbix/zabbix\_agentd.conf

sed -i 's/# UnsafeUserParameters=0/UnsafeUserParameters=1/g' /etc/zabbix/zabbix\_agentd.conf

下面的这行自定义监控，查询当前访问日志异常ip访问登陆,指登录失败次数

sed -i 's/# UserParameter=/UserParameter=check\_failed,sh \/script\/check\_failed.sh/g' /etc/zabbix/zabbix\_agentd.conf

相关脚本 ：

mkdir /script

vim /script/check\_failed.sh

#!/bin/bash

LOG\_PATH="/var/log/secure"

mon=$(date +%B)

h=$(date +%d)

ms=$(date +%H:%M)

#表示字符开头为0就替换为空

h=${h/#0/""}

k=" "

count=`grep "$h$k$ms" /var/log/secure | grep -c Failed `

echo $count

加读权限， chmod +r /var/log/secure 要不然zabbix-server 访问不了，

# systemctl restart zabbix-agent

# systemctl status zabbix-agent

# systemctl enable zabbix-agent

# lsof -i:10050

准备好client2后，回到zabbix server的web界面进行操作

1. 自动发现

1. 配置->自动发现

默认有一个叫Local network的发现规则，这次就不创建新的规则了，直接修改这个Local network规则就好

主要修改了我们的试验网段为192.168.224.0/24

把"已启用打勾

修改完后点更新

2. 然后在监测中－>自动发现　里查找已经发现的设备（如果使用类似172.16.0.0/16的网段，范围大，测试的速度很慢). 设置延迟为5秒，以便快速发现。

3. 继续配置动作action

配置->动作->右上角事件源选 自动发现

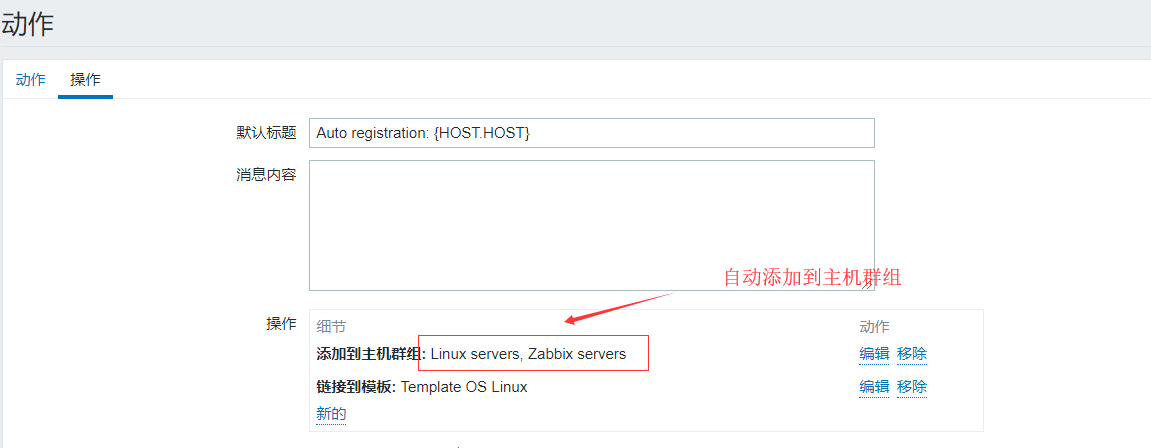


然后会发现一个默认的叫Auto discovery. Linux servers的动作，然后需要修改IP网段。

192.168.224.1-254,192.168.224.1 #192.168.224.2 为gateway



然后点操作，增加相应的模块添加和主机群组添加



4.最后过段时间去配置->主机里查看，会发现把discovery的主机自动加到了配置里了

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

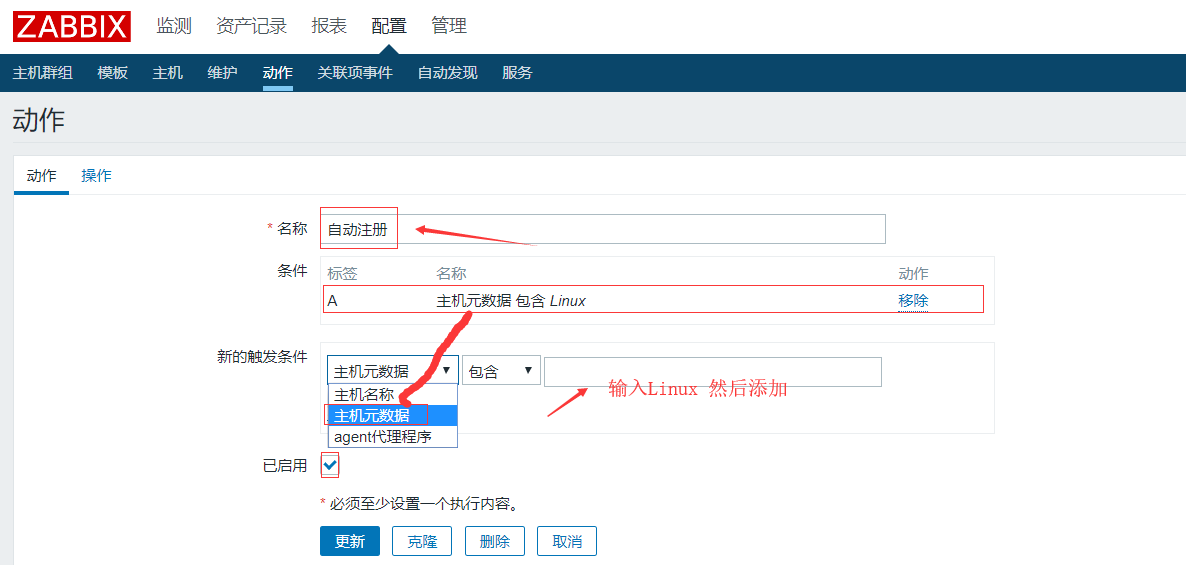
提示：如果配置完成后还是无法实现自动注册，请将“自动发现” “Auto discovery. Linux servers.” 停用，并停止zabbix-server几分钟后重启启动即可！

1. 自动注册

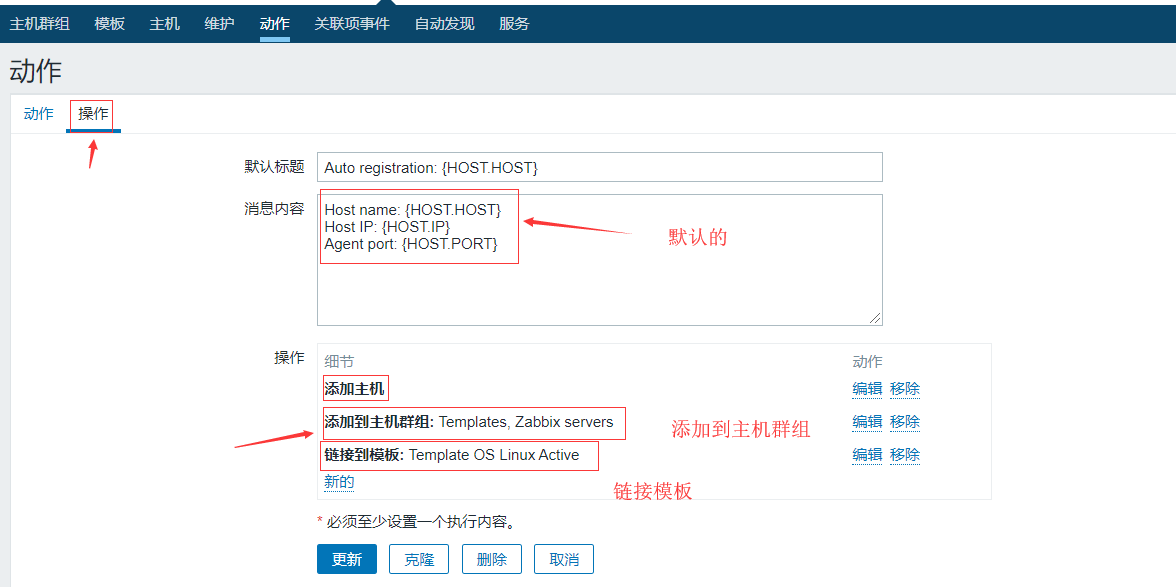
配置->动作->右上角事件源选 自动注册 然后点击创建动作



然后输入动作的名称，我命名为 自动注册 添加新的触发条件



第二步 选择 ---> 操作 增加一些添加主机后需要做的动作



然后所有客户端增加agent，只要指定了server是192.168.224.10 这台, server端都可以自动发现自动注册，自动添加群组，

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

概念

聚合检测，汇总检测(Aggregate checks)

zabbix server

192.168.224.10

server1.com client2

192.168.224.11 192.168.224.12

item1 item2

注意：如果要创建聚合监测，所有机器都必须在同一个主机组里面

监测server1.com和client2两台服务器登陆用户数之和

1,两台都要配置登陆用户数的监控项,

vim /etc/zabbix/zabbix\_agentd.conf

设置 UserParameter=loginusers,who | wc -l

systemctl restart zabbix-agent

1.5 在client2，创建loginusers的监控项。步骤参考前面。

2.Console->配置->主机->server1.com->监控项

Console右上角 创建监控->

类型选择“Zabbix”整合

键值填写：grpsum["hostgroup1","loginusers",last] note:确保机器都在group'hostgroup1'

概念九：

通知(notification)

出现报警事件或者触发器触发，进行通知。通知类型默认有:email,jabber,短信(sms).其它方式比如微信，需要接口(比如企业公众号)；还可以定义shell脚本报警

Step 1.管理->报警媒介类型->Email

Step 2 分配这个报警类型给用户admin

管理 -> 用户 -> admin -> 报警媒介 -> 添加

====================================================================================

概念十:

模版(templates)

代表监控项,应用集,触发器，图形，自动发现规则,web监测等的组合. 例如：Template App HTTPS Service

用于在监控时直接应用到一台被监控的主机

配置->模版

概念十一:

批量更新

配置－>主机->选取要批量更新的主机（前面打勾）->选择下面的批量更新选项－>执行相应的更新动作

导入导出

配置->主机->选取要导出的主机（前面打勾）->下面选择导出->默认会导出到你使用浏览器的机器的/root/Downloads/

配置->模版->选取要导出的模版（前面打勾）->下面选择导出->默认会导出到你使用浏览器的机器的/root/Downloads/

练习:把本机的一个模版删除，然后从同桌的zabbix服务器那导出成xml文件，并拷贝过来导入(记得要修改相应的IP等参数)

概念十二:

通过代理实现分布式监控

机房一 机房二

zabbix核心服务器

机房三 机房四

zabbix server ------ zabbix proxy ---- 被代理和被监控的机器(agent)

zabbix\_server －－－－－－ zabbix\_proxy －－－－－－－－－ zabbix\_agent1

192.168.224.10 192.168.224.12 192.168.224.11

准备:

我这里把原来的client2用来模拟zabbix\_proxy

1，先在zabbix\_server的web界面把agent2的配置删除（并把先前做的自动发现规则禁用）

2，主机名改成zabbix\_proxy.com

3, systemctl stop zabbix-agent

第一大步：zabbix\_proxy上的配置(需要本地yum源和zabbix源)(192.168.224.12)

# yum install mariadb\\* zabbix-proxy zabbix-proxy-mysql zabbix-agent -y

# systemctl restart mariadb

# systemctl enable mariadb

# mysql

MariaDB [(none)]> create database zabbix\_proxy default charset utf8;

MariaDB [(none)]> grant all privileges on zabbix\_proxy.\* to 'zabbix'@'localhost' identified by '123';

MariaDB [(none)]> flush privileges;

# zcat /usr/share/doc/zabbix-proxy-mysql-3.2.11/schema.sql.gz |mysql zabbix\_proxy -u zabbix -p123

把数据导入mysql zabbix\_proxy库

# vim /etc/zabbix/zabbix\_proxy.conf

13 ProxyMode=0 --zabbix\_proxy的代理方式为主动（zabbix\_proxy主动发数据给zabbix\_server)

24 Server=192.168.224.10 --zabbix\_server的ip

43 Hostname=zabbix\_proxy.com --这个名字一定要和你的主机名还有后面在web界面配置代理的名字保持一致

128 DBHost=localhost

139 DBName=zabbix\_proxy

154 DBUser=zabbix

162 DBPassword=123

216 ConfigFrequency=60 --主动模式下zabbix\_proxy多久从zabbix\_server接收一次配置数据

225 DataSenderFrequency=5 --主动模式下zabbix\_proxy多久发送一次收集的数据给zabbix\_server

# vim /etc/zabbix/zabbix\_agentd.conf

64 SourceIP=192.168.224.12 --代理服务器IP地址

95 Server=192.168.224.12 --代理服务器IP地址

136 ServerActive=192.168.224.12 --代理服务器IP地址

147 Hostname=zabbix\_proxy.com

# systemctl restart zabbix-proxy

# systemctl restart zabbix-agent

# systemctl enable zabbix-agent

# systemctl enable zabbix-proxy

第二大步：zabbix\_agent的配置(192.168.224.11)

# vim /etc/zabbix/zabbix\_agentd.conf --把服务器的ip改成zabbix\_proxy的ip，而不是zabbix\_server的ip

95 Server=192.168.224.12

136 ServerActive=192.168.224.12

147 Hostname=server1.com.com --- 代表本机器的hostname

# systemctl restart zabbix-agent

第三大步:

回到zabbix\_server的图形管理界面

1,代理机器zabbix proxy 加入到监控的主机中

配置－》主机－》创建主机

主机名称：zabbix\_proxy.com

群组： 随意加一个组

IP地址：192.168.224.12 端口:10050

2,加一个代理程序

管理－》agent代理程序－》创建代理

agent代理程序名称:zabbix\_proxy.com --名字要和配置里的主机名一致

系统代理程序模式: 主动式

agent代理程序的主机: server1.com

zabbix\_proxy.com

加完后，agent1和zabbix\_proxy.com就自动被代理了

第四大步：

测试

在server1.com(192.168.224.11)上找一个监控项做改变（比如登录用户数），然后在192.168.224.10上的zabbix\_server的图形界面能看到这个改变，说明proxy成功

概念十三：

主动监控和被动监控

zabbix\_server －－－－－－ zabbix\_proxy －－－－－－－－－ zabbix\_agent1

agent被动模式(相对于agent的被动，也就是表示是server或proxy去找agent拿数据）

# vim /etc/zabbix/zabbix\_agentd.conf

Server=192.168.224.12 --IP为zabbix\_proxy的ip(如果没有proxy，则直接为zabbix\_server的ip);这个参数是被动模式相关（监控项里的类型配置为zabbix客户端就表示为被动模式）

agent主动模式(相对于agent的主动，也就是表示agent主动把数据传给server或proxy）

# vim /etc/zabbix/zabbix\_agentd.conf

Serveractive=192.168.224.12 --IP为zabbix\_proxy的ip(如果没有proxy，则直接为zabbix\_server的ip);这个参数是主动模式相关（监控项里的类型配置为zabbix客户端（主动式）就表示为主动模式）

proxy主动模式（zabbix\_proxy主动发数据给zabbix\_server) 可以用于被监控主机没有公网IP,而Zabbix Server无法直接访问的情况，由被监控机器直接发送数据给Zabbix Server。

# vim /etc/zabbix/zabbix\_proxy.conf

ProxyMode=0

proxy被动模式（zabbix\_server找zabbix\_proxy收集数据)

# vim /etc/zabbix/zabbix\_proxy.conf

ProxyMode=1

--------------------------------------------------------------------------

end

=========================