**Author:** 郭恒志

**Version:** 1.0

**Date:** 2017.10.31

**知了服务**

**zabbix监控**

0

Table of ContenTs

[1 linux监控 3](#_Toc497750676)

[2 iostat监控 4](#_Toc497750677)

[3 mysql监控 12](#_Toc497750678)

[4 redis监控 14](#_Toc497750679)

[5 tomcat监控 18](#_Toc497750680)

[6 Web监控 21](#_Toc497750681)

[7 keepalived监控 27](#_Toc497750682)

[8 gearman进程监控 28](#_Toc497750683)

**注意zabbix用户对/etc/zabbix目录下文件的权限**

zabbix-get用于zabbix-server到zabbix-agent的数据获取，通常可以用来验证zabbix-agent的配置是否正确

zabbix-get -s zabbix-agent的IP -p zabbix-agent的端口 -I zabbix-server的IP -k key

如果环境没有zabbix-get命令，需要安装，执行yum –y install zabbix-get.x86\_64即可

linux监控

zabbix自带监控模板，可以直接应用于需要监控的主机

| **模板** | **说明** |
| --- | --- |
| Template SVC OS Linux.xml | 模板包含自动发现规则（Mounted filesystem discovery、Network interface discovery），自动发现文件系统和网口 |

按照下面的图1~图3的操作步骤，即可实现对Linux系统的监控：

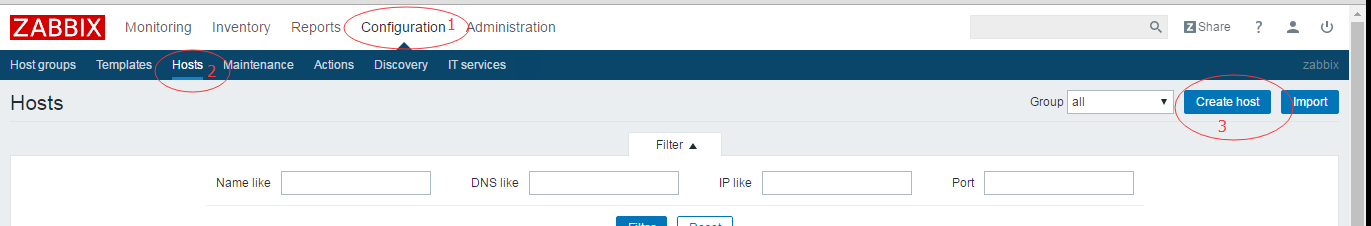


图-1

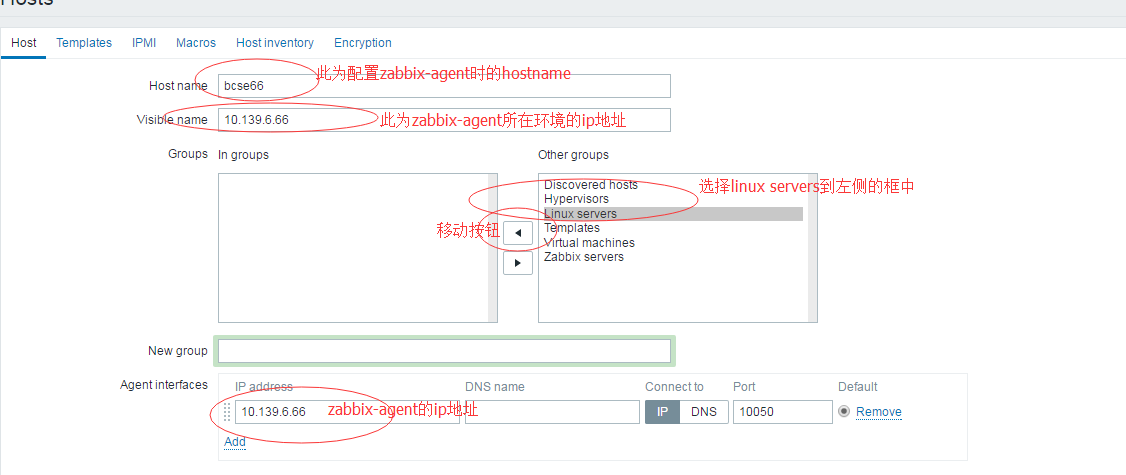


图-2

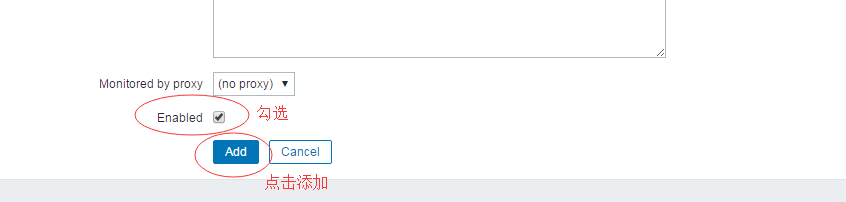


图-3

iostat监控

1、首先确认被监控的环境可以执行iostat命令 ：iostat -kx 10 2，如无法执行，安装sysstat（yum install sysstat）

2、添加userparameter\_io.conf配置文件在各个被监控的环境上,

在/etc/zabbix/zabbix\_agentd.d下添加userparameter\_io.conf, 文件内容如下:

UserParameter=custom.vfs.dev.read.ops[\*],cat /proc/diskstats | grep $1 | head -1 | awk '{print $$4}'

UserParameter=custom.vfs.dev.read.ms[\*],cat /proc/diskstats | grep $1 | head -1 | awk '{print $$7}'

UserParameter=custom.vfs.dev.write.ops[\*],cat /proc/diskstats | grep $1 | head -1 | awk '{print $$8}'

UserParameter=custom.vfs.dev.write.ms[\*],cat /proc/diskstats | grep $1 | head -1 | awk '{print $$11}'

UserParameter=custom.vfs.dev.io.active[\*],cat /proc/diskstats | grep $1 | head -1 | awk '{print $$12}'

UserParameter=custom.vfs.dev.io.ms[\*],cat /proc/diskstats | grep $1 | head -1 | awk '{print $$13}'

UserParameter=custom.vfs.dev.read.sectors[\*],cat /proc/diskstats | grep $1 | head -1 | awk '{print $$6}'

UserParameter=custom.vfs.dev.write.sectors[\*],cat /proc/diskstats | grep $1 | head -1 | awk '{print $$10}'

**建议：实际添加时，把配置文件中的注释以及注释后面的内容删除掉**

3、重启zabbix-agent服务

service zabbix-agent restart

4、在zabbix-server服务所在环境进行验证，能否获取到磁盘IO信息

zabbix\_get -s 目标服务器IP -p 10050 -k custom.vfs.dev.write.ops[sda]

说明：目标服务器IP即被监控环境地址；

sda是被监控环境的磁盘名称，此名称可以通过df –h命令在被监控环境上执行查看，如下图红圈中所示

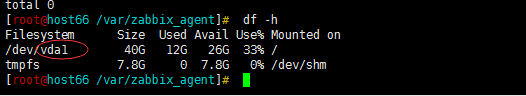


图-4

5、配置zabbix-server模板

* 登录zabbix web页面
* 依次选择Configuration>>Templates>>Create templates,如图-5

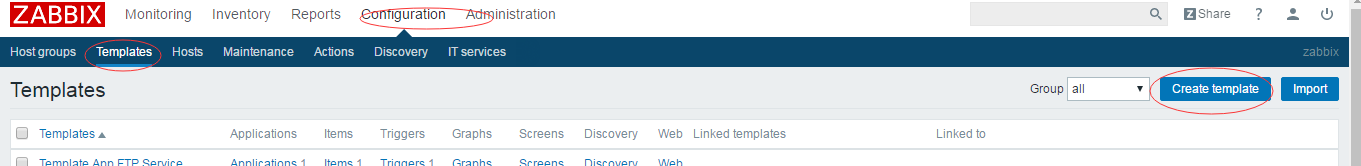


图-5

* 依次填写Template name>>Groups in groups>>add,如图-6~图-7

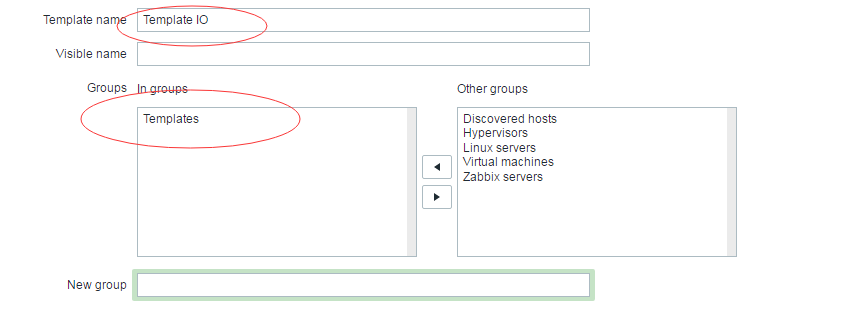


图-6

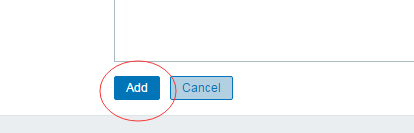


图-7

6、配置监控项

* 在web页面依次执行Conflguration>>Templates,在模板列表中选择刚刚添加的模板Templates IO,
* 选择如图-8所示的Items

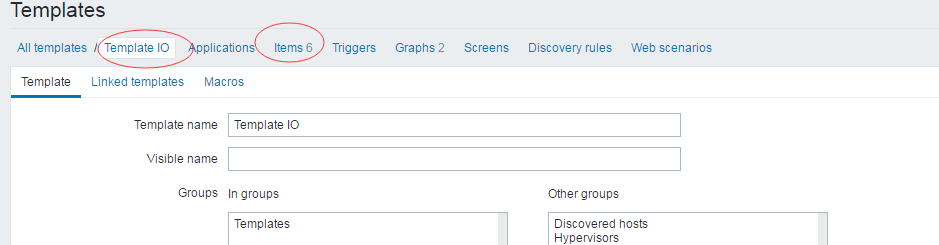


图-8

* 选择Create item

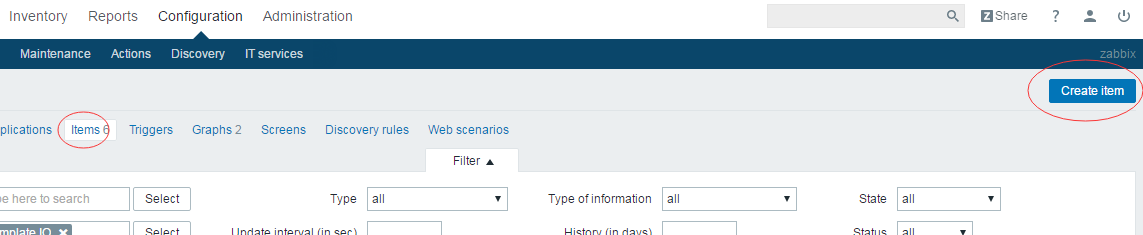


图-9

* 依次配置Name,Key,Units,Store value,Use custom multiplier，具体信息如下

Name: Disk:$1:Read:Bytes/sec

Key: custom.vfs.dev.read.sectors[sda] //sda修改为实际被监控环境的磁盘名称，如上面图-4所示的方法，下面监控二到监控六都需要修改实际磁盘名称

Units: B/sec

Store value: speed per second //会进行差值计算

Update interval (in sec) 10 //间隔时间

Use custom multiplier 512 //会对值乘以512，因为这里是一个扇区，转换为字节为512B

History storage period (in days) 30 //历史数据保留时长

Trend storage period (in days) 365 //趋势数据存储周期

勾选 Enabled

* 监控一配置完，如图-10

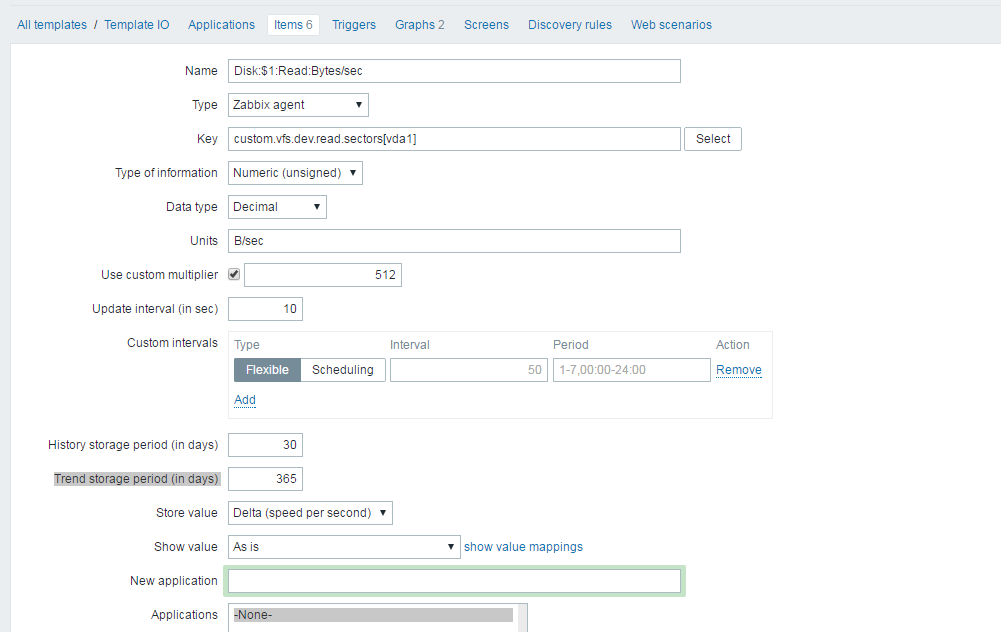


图-10

* 再配置监控二，配置信息如下

Name:Disk:$1:Write:Bytes/sec

Key: custom.vfs.dev.write.sectors[sda]

Units: B/sec

Store value: speed per second

Use custom multiplier 512

History storage period (in days) 30

Trend storage period (in days) 365

勾选 Enabled

* 配置监控三，配置信息如下

Name:Disk:$1:Read:ops per second

Key: custom.vfs.dev.read.ops[sda]

Units: ops/second

Store value: speed per second

History storage period (in days) 30

Trend storage period (in days) 365

勾选 Enabled

* 配置监控四，配置信息如下

Name: Disk:$1:Write:ops per second

Key: custom.vfs.dev.write.ops[sda]

Units: ops/second

Store value: speed per second

History storage period (in days) 30

Trend storage period (in days) 365

勾选 Enabled

* 配置监控五，配置信息如下

Name: Disk:$1:Read:ms

Key: custom.vfs.dev.read.ms[sda]

Units: ms

Store value: speed per second

History storage period (in days) 30

Trend storage period (in days) 365

勾选 Enabled

* 配置监控六，配置信息如下

Name:Disk:$1:Write:ms

Key: custom.vfs.dev.write.ms[sda]

Units: ms

Store value: speed per second

History storage period (in days) 30

Trend storage period (in days) 365

勾选 Enabled

7、添加图形，依次点击Configuration>>Templates>>Templates IO>>Graphs>>Create graph，如图-11

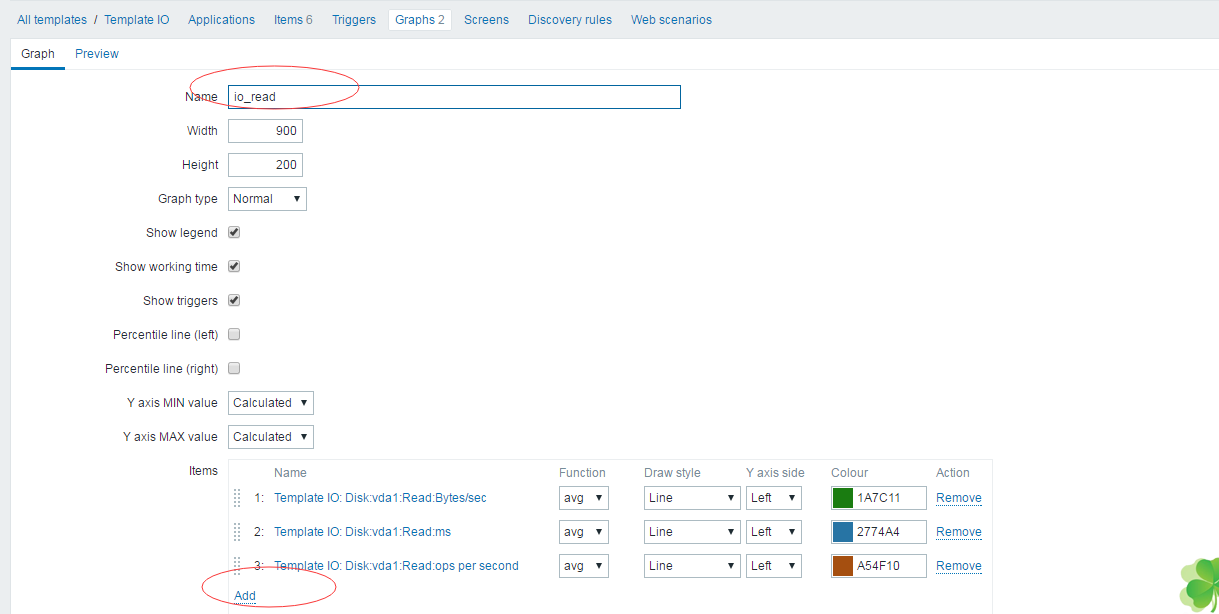


图-11

8、实现对被监视系统的IO监控

* 依次点击configuration>>Hosts
* 如果对章节1中的linux监控环境同时监控IO资源，则在Host列表中选择一家创建好的Host节点信息，在Groups in groups列表中增加Templates，如图-12和图-13所示

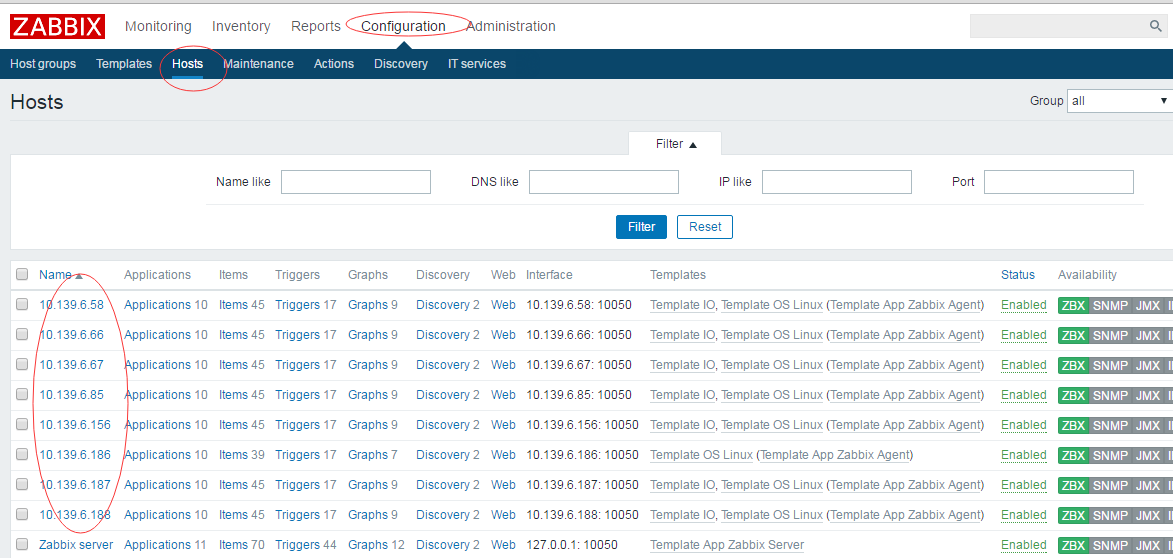


图-12

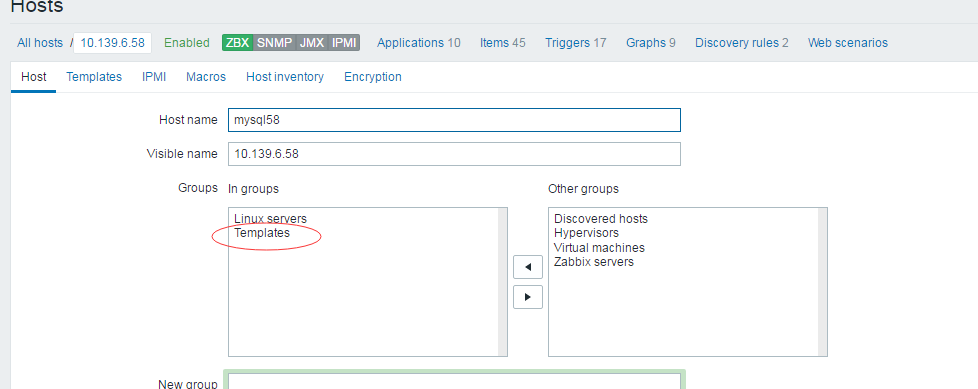


图-13

* 如果没有可选的Host信息，需要新增Host信息，则点击Create host，方法与章节1linux监控中创建host的方法相同，只是Groups in group选Templates即可
* 配置完host信息后，选择配置好的host信息，点击Host右侧的Templates进行模板关联操作，如图-14~图-17

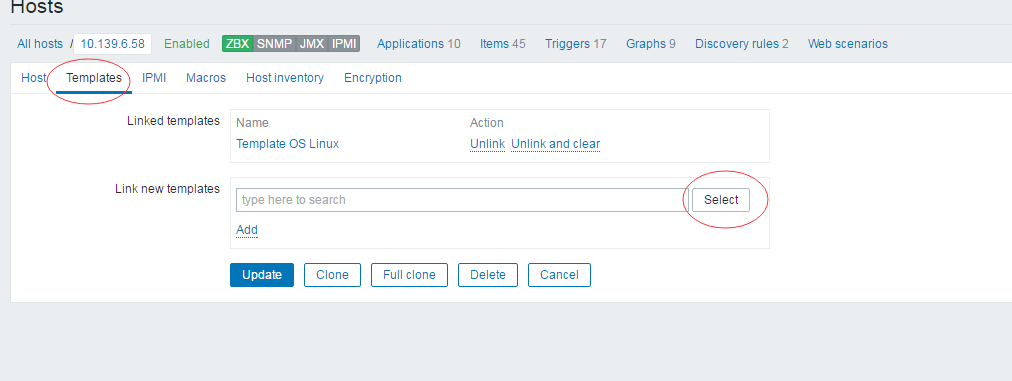


图-14

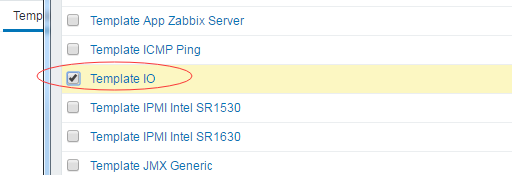


图-15

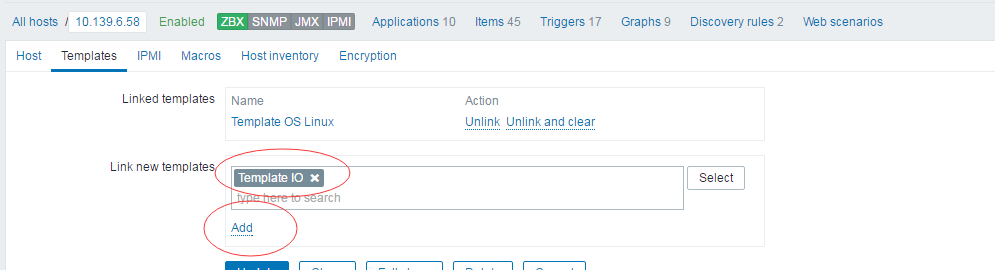


图-16

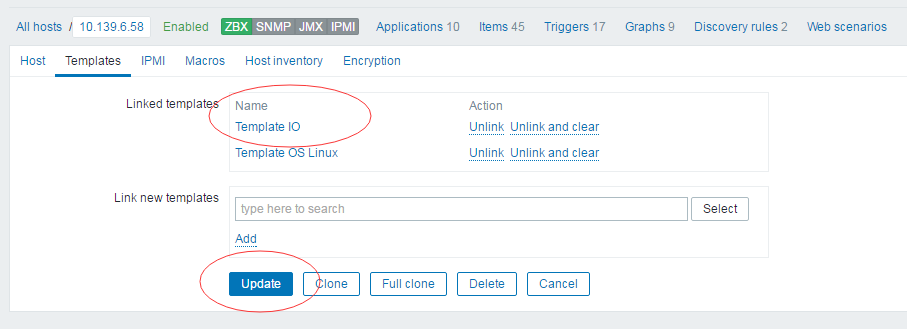


图-17

9、到监控页面查看监控效果，如图-18所示

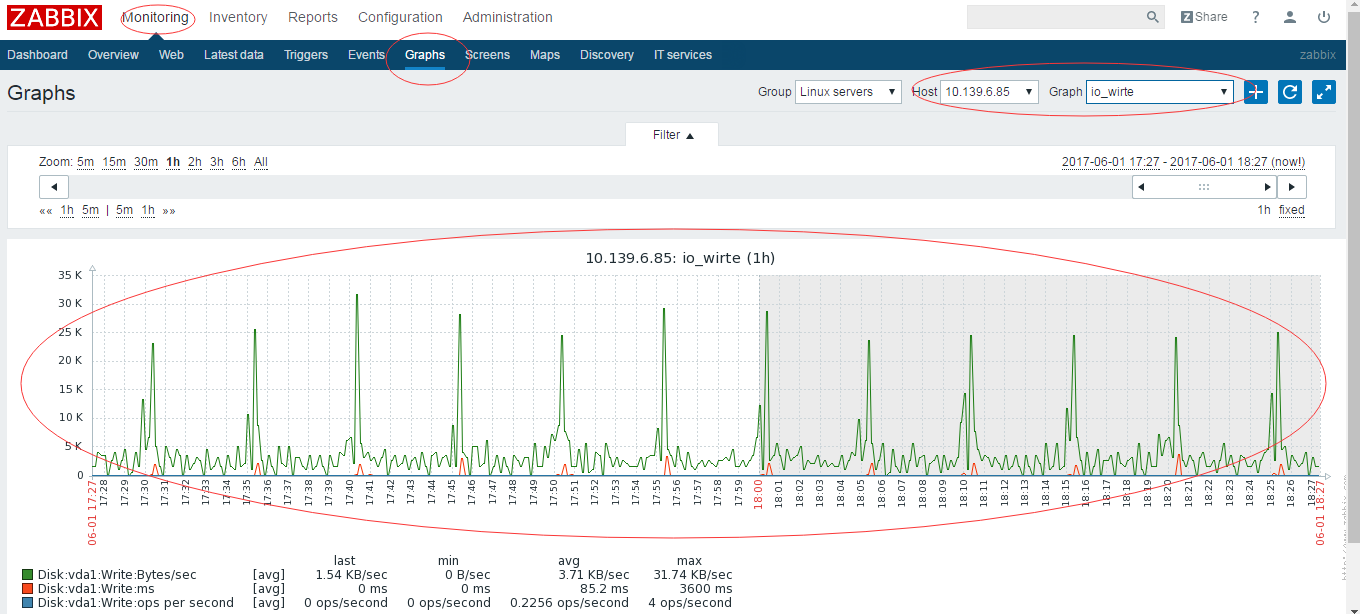


图-18

mysql监控

1、在需要监控的mysql主机上创建监控账号：

**shell>** GRANT USAGE,PROCESS,REPLICATION CLIENT,REPLICATION SLAVE ON \*.\* TO 'zabbix'@'%' IDENTIFIED BY 'Zabbix@123';

**shell>** GRANT USAGE,PROCESS,REPLICATION CLIENT,REPLICATION SLAVE ON \*.\* TO 'zabbix'@'localhost' IDENTIFIED BY 'Zabbix@123'

**shell>** flush privileges;

2、在/etc/zabbix/目录下创建一个 .my.cnf 文件,内容如下

[mysql]

user=zabbixagent

password=zabbixagent

[mysqladmin]

user=zabbixagent

password=zabbixagent

3、创建存放监控脚本的目录在/etc/zabbix路径下

**Shell>** mkdir zabbix\_scripts

4、在新建目录zabbix\_scripts下创建监控脚本chk\_mysql.sh，内容如下



5、在/etc/zabbix/zabbix\_agentd.d路径下，将原有的配置文件userparameter\_mysql.conf备份，然后新建一个userparameter\_mysql.conf，内容如下：



6、重启zabbix-agent服务

**shell>** service zabbix-agent restart

7、打开zabbix server界面（http://<server\_ip>/zabbix），Configuration-Templates-Import，添加mysql的模板



8、然后按照章节5步骤8的方法配置mysql的监控

redis监控

1、创建监控脚本目录

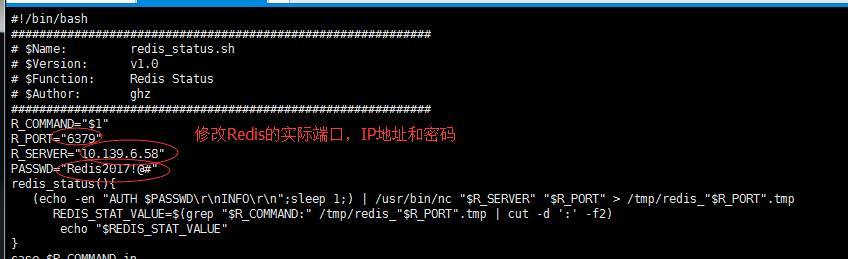
$ cd /etc/zabbix

$ mkdir zabbix\_scripts

2、上传附件redis\_status.sh脚本到zabbi\_scripts目录下



3、修改redis\_status.sh中相关配置，如下图所示：



4、修改完后保存退出，并赋予权限，chmod 755 redis\_status.sh 并执行yum –y install nc，安装nc命令，如果环境已经有nc命令，则忽略安装动作。

5、添加zabbix agent配置文件

$ cd /etc/zabbix/zabbix\_agentd.d

$ vi redis\_status.conf

在新建文件redis\_status.conf中添加下面的内容：

UserParameter=redis\_status[\*],/bin/bash /etc/zabbix/zabbix\_scripts/redis\_status.sh "$1"

$ :wq 保存退出

6、重启zabbix-agent

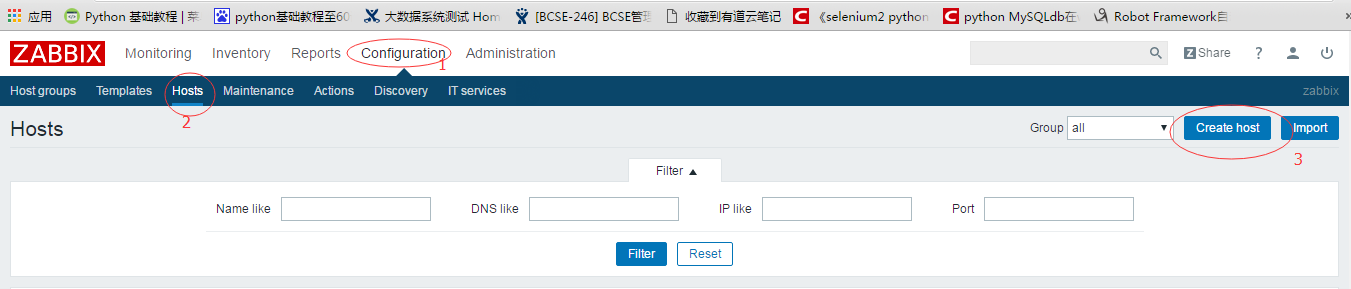
**shell>** service zabbix-agent restart

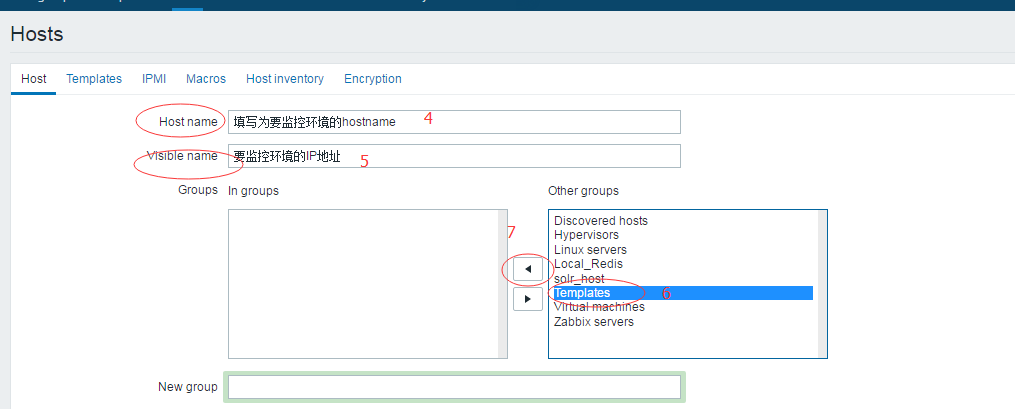
7、打开zabbix server界面（http://<server\_ip>/zabbix），依次点击Configuration-Templates-Import，添加redis的模板，如下面的附件



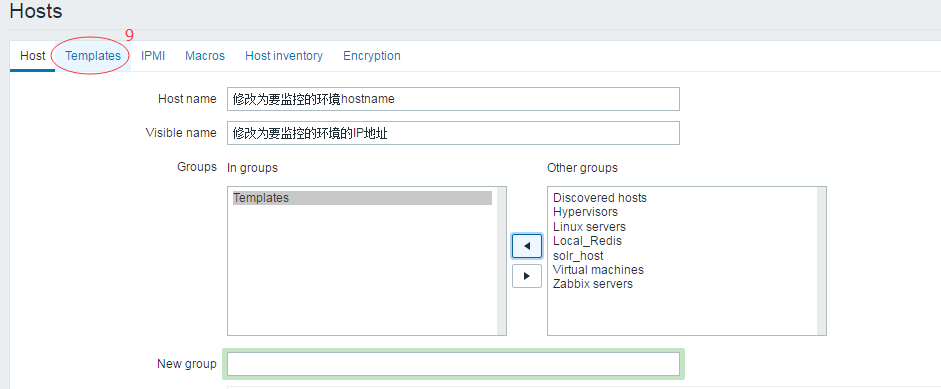
8、配置监控

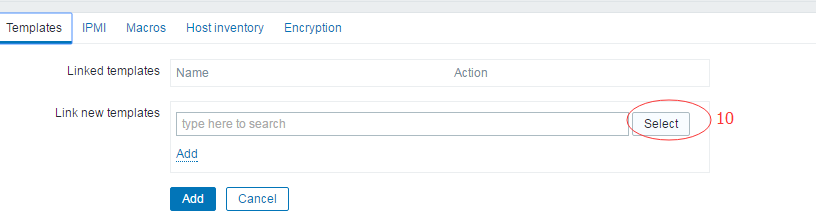
登录监控界面（http://<server\_ip>/zabbix），依次点击Configuration-Host，添加或选择已经存在的要监控的Host信息，然后点击Templates-select，选择之前导入的redis模板即可，具体步骤可参考下图：

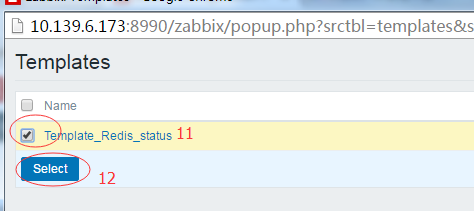


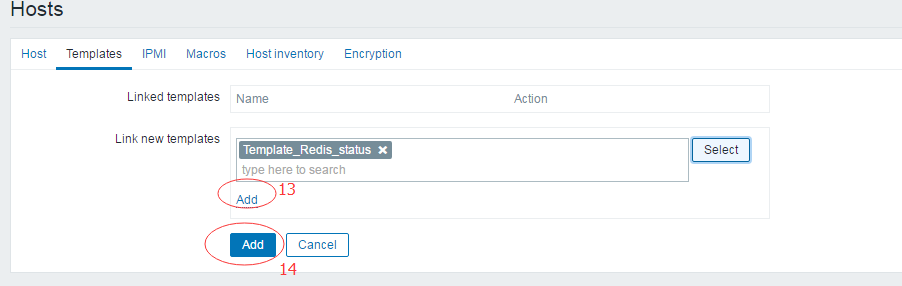




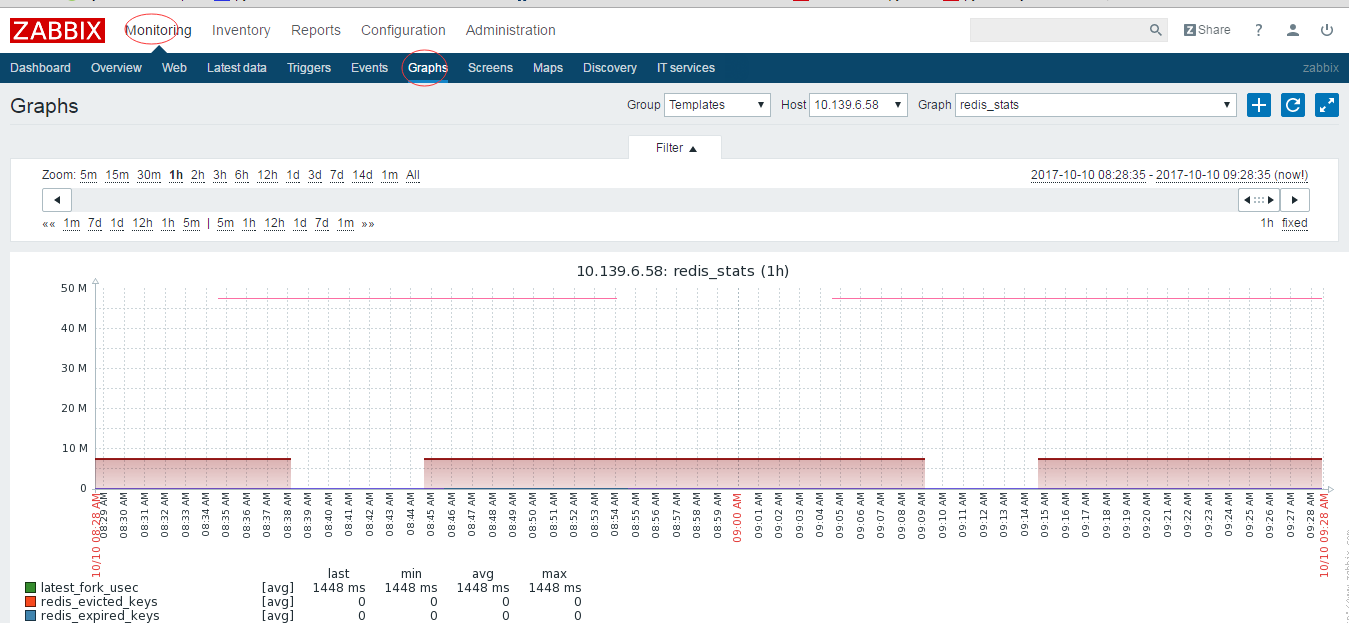








9、在监控界面依次点击Monitoring-Graphs，选择redis环境即可查看redis的监控信息，如下图所示：



tomcat监控

前提：已经完成Java GateWay的安装部署，如果没有请参照zabbix安装部署手册中章节3.6进行安装部署。（所需的一些jar包等可联系实施人员获取）

1. 添加catalina-jmx-remote.jar到zabbix java gateway的lib目录下/usr/sbin/zabbix\_java/lib
2. 添加catalina-jmx-remote.jar文件到tomcat的lib目录
3. 修改tomcat的catalina.sh

$ vi catalina.sh

添加如下内容：

CATALINA\_OPTS="${CATALINA\_OPTS} -Djava.rmi.server.hostname=**192.168.7.186**"

CATALINA\_OPTS="${CATALINA\_OPTS} -Djavax.management.builder.initial="

CATALINA\_OPTS="${CATALINA\_OPTS} -Dcom.sun.management.jmxremote=true"

CATALINA\_OPTS="${CATALINA\_OPTS} -Dcom.sun.management.jmxremote.ssl=false"

CATALINA\_OPTS="${CATALINA\_OPTS} -Dcom.sun.management.jmxremote.authenticate=false"

注意：hostname位机器ip地址，即被监控机器对外服务地址

1. 修改tomcat的server.xml

$ vi tomcat/conf/server.xml

添加如下，注意添加位置在

<Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener" />

之后添加如下代码：

<Listener className="org.apache.catalina.mbeans.JmxRemoteLifecycleListener" rmiRegistryPortPlatform="12345" rmiServerPortPlatform="12346" />

1. 添加tomcat应用自动发现脚本

由于默认的jmx不能自动发现部署的新应用，因此需要添加一个脚本自动发现，并且利用zabbix的LLD（Low-level discovery）来发现

mkdir /opt/tomcat/

mkdir /tmp/tomcat/

chmod -R 777 /tmp/tomcat/

cd /opt/tomcat/

wget http://dl.cactifans.org/tools/context.sh

wget http://dl.cactifans.org/tools/cmdline-jmxclient-0.10.3.jar

chmod a+x /opt/tomcat/context.sh

echo "\*/1 \* \* \* \* root /opt/tomcat/context.sh" >>/etc/crontab

注意：如果上述红色部分无法获取到响应脚本和jar，可以联系实施工程师获取。

1. 修改context.sh脚本内容

#!/bin/bash

java -jar /opt/tomcat/cmdline-jmxclient-0.10.3.jar - 192.168.7.186:12345 Catalina:type=Manager,\*| awk -F "," '{ print $1 }'|awk -F: '{ print $2 }'>/tmp/tomcat/context.csv

注意：此脚本在被监控端添加，注意要把ip改成本机的服务IP地址，port修改为步骤4中的rmiRegistryPortPlatform的port值

1. 添加一个应用自动发现的程序，我放到zabbix agent的zabbix\_scripts目录下

$ cd /etc/zabbix/ zabbix\_scripts

$ wget <http://dl.cactifans.org/tools/context> //如果获取不下来，可以联系实施工程师获取

$ chmod a+x context

1. 修改zabbix agentd设置，添加应用自动发现的key

$vi /etc/zabbix/zabbix\_agentd.d/ userparameter\_tomcat.conf

添加如下内容：

UserParameter=tomcat.context.discovery,/etc/zabbix/zabbix\_scripts/context

保存退出。

1. 重启tomcat
2. 重启zabbix-agent

注：防火墙需要开放12345，12346端口或关闭防火墙

1. 测试

在zabbix server上执行：

java -jar cmdline-jmxclient-0.10.3.jar - 192.168.7.186:12345 java.lang:type=Memory NonHeapMemoryUsage

如果有如下回显表示jmx配置正确，如不正确，请检查配置

09/23/2017 13:25:29 +0800 org.archive.jmx.Client NonHeapMemoryUsage:

committed: 271646720

init: 270991360

max: 587202560

used: 38207984

在zabbix server上用zabbix\_get执行：

zabbix\_get -s 192.168.7.153 -k tomcat.context.discovery //ip修改为tomcat的对外服务ip

如果能回显如下数据表示获取成功



1. 在监控web界面，导入tomcat监控模板

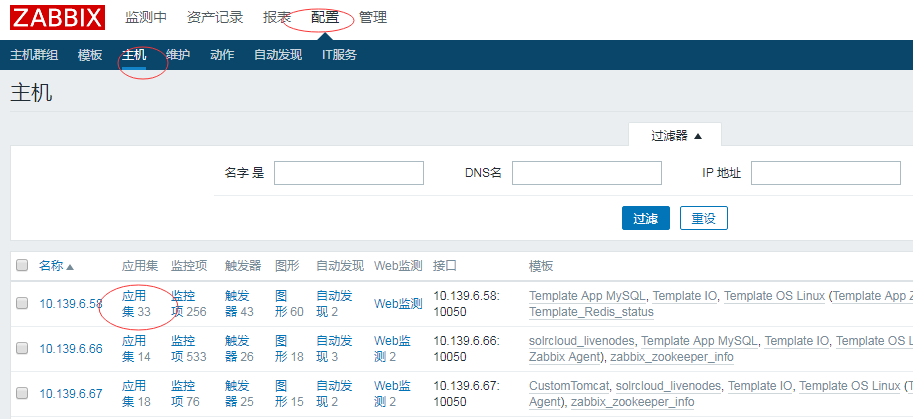


1. 配置监控项按照5章节的步骤8配置tomcat的监控。

Web监控

1、登录zabbix监控页面

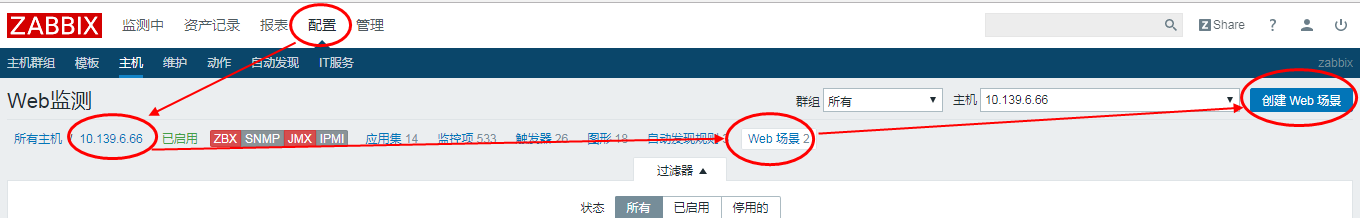
2、应用集配置  
 在配置—>主机中打开主机列表，选择需要添加监控主机的web，创建应用集

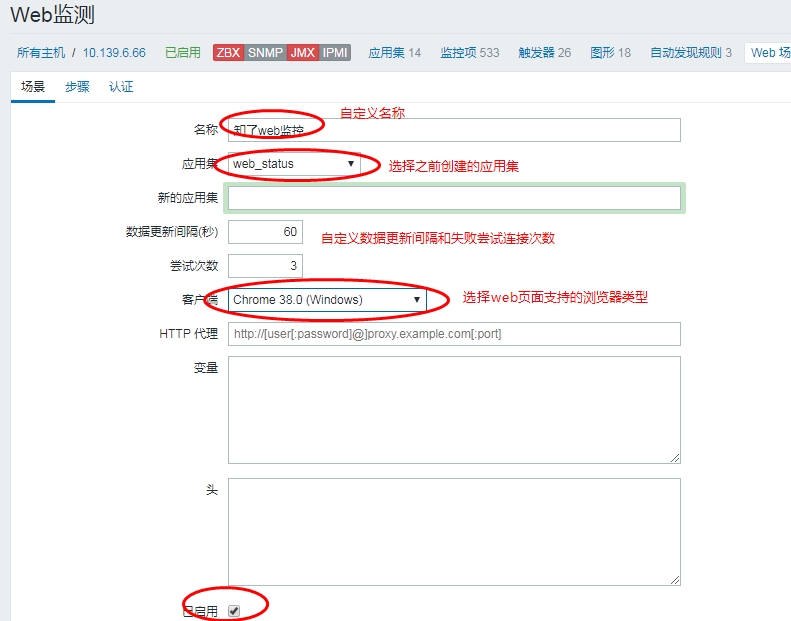




3、web监测配置

选择web场景，再单击右上角的创建web场景





在步骤选项卡添加测试步骤

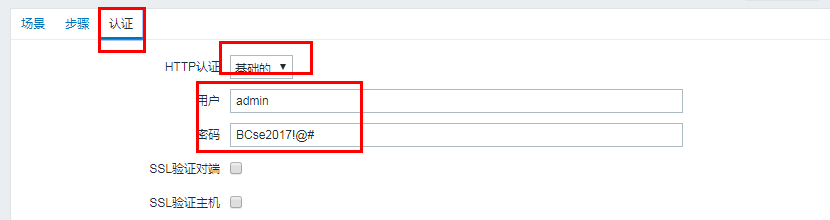
Name是测试步骤的名称，URL监控站点的真实url，Required status colder是监控时要求页面返回的状态码，通常设置200

添加完成后可以在monitor—web 看到刚才添加的监控



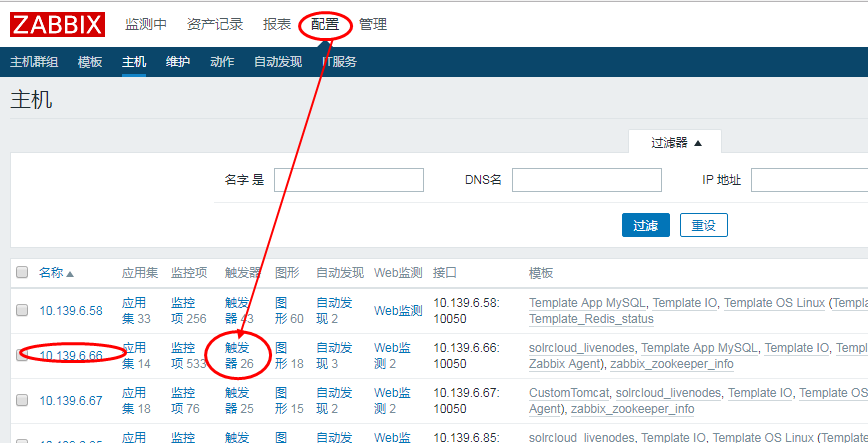


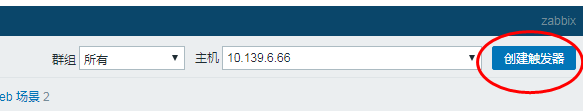
说明：如果涉及用户密码登录，还需要点击认证按钮，配置http认证，如下图



4、触发器配置

添加完web监控后再次打开主机列表，选择触发器，点击右上角的创建触发器





在Name中输入Triggers的名称

点击表达式右侧添加按钮



在添加完web 监控后回自动创建相应的Keys，但是要选择已经定义web的相应主机

在Function中选择相应的表达式，这里是设置返回的状态码不等于变量 N 时触发报警，N的值在下面设置成200

表达式：如果最近连续4次取到的response\_code值不是200，则触发报警

{IP地址:web.test.rspcode[http\_status\_gm, http\_status\_gm].last(0)}<>200

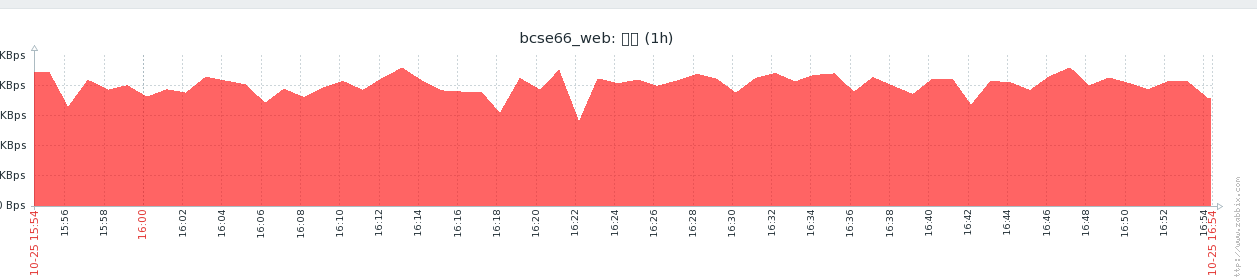
{IP地址:web.test.rspcode[http\_status\_gm, http\_status\_gm].last(1)}<>200

{IP地址:web.test.rspcode[http\_status\_gm, http\_status\_gm].last(2)}<>200

{IP地址:web.test.rspcode[http\_status\_gm, http\_status\_gm].last(2)}<>200

测试





keepalived监控

1、添加zabbix agent配置文件：

**shell>** 将下面的脚本放到/etc/zabbix/zabbix\_agentd.d/下



**shell>** 将下面的脚本放到/etc/zabbix/scripts下面

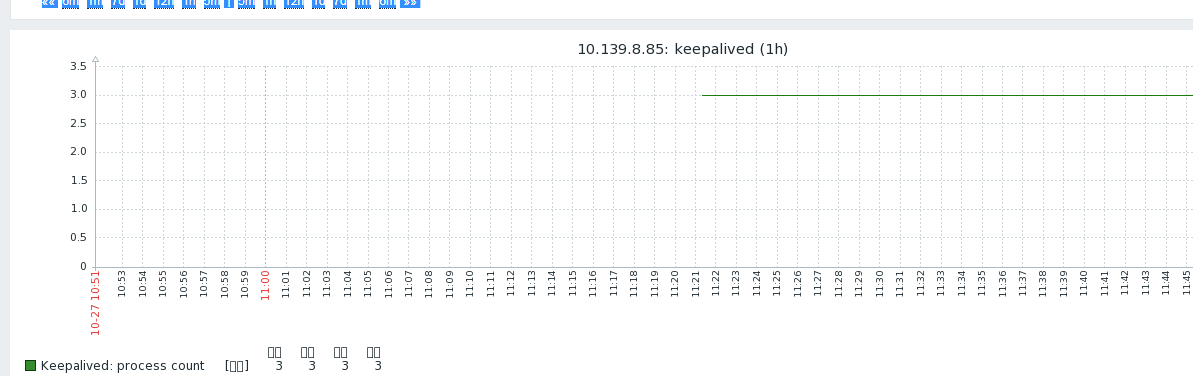


**shell>** service zabbix-agent restart

2、打开zabbix server界面（http://<server\_ip>/zabbix），Configuration-Templates-Import，添加keepalived的模板

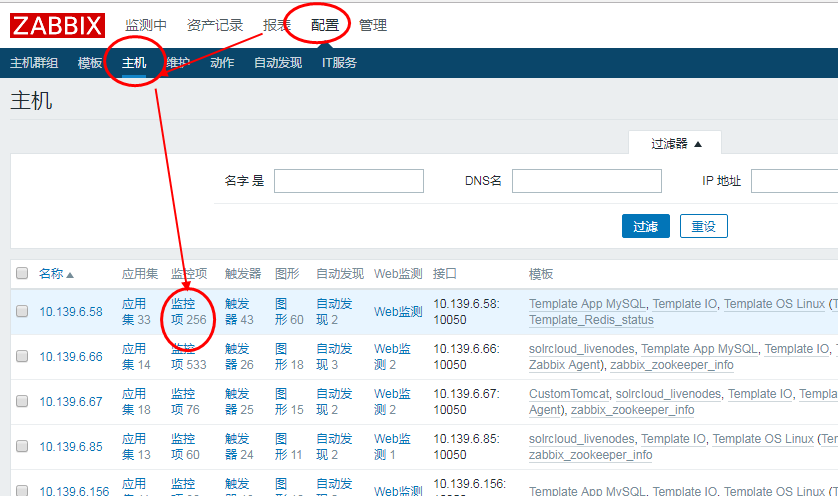


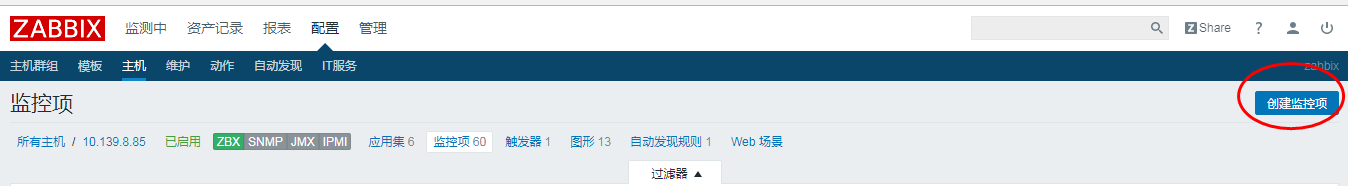
3、然后按照章节5步骤8的方法配置keepalive的监控，最终监控结果如下图

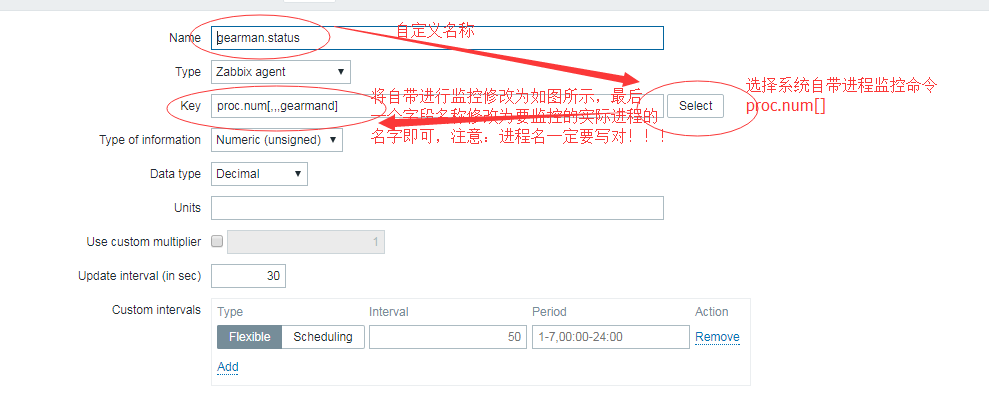


gearman进程监控

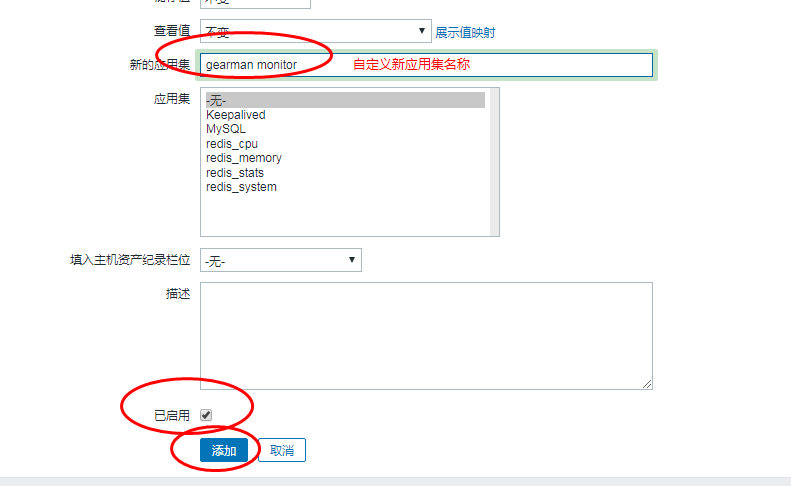
1. 登陆zabbix web页面配置监控项，步骤如下





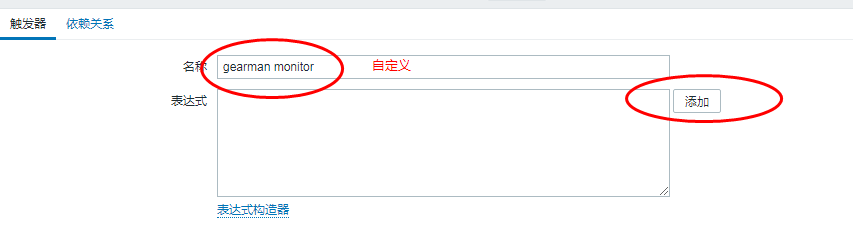


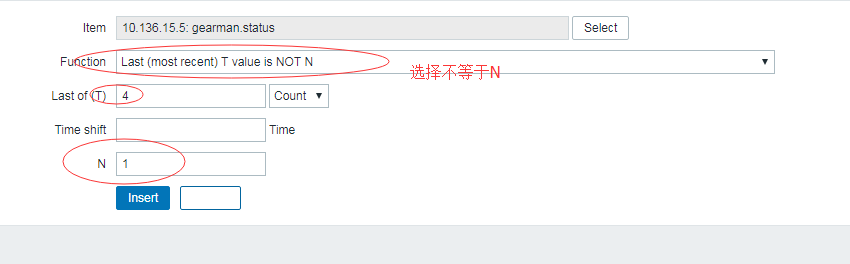


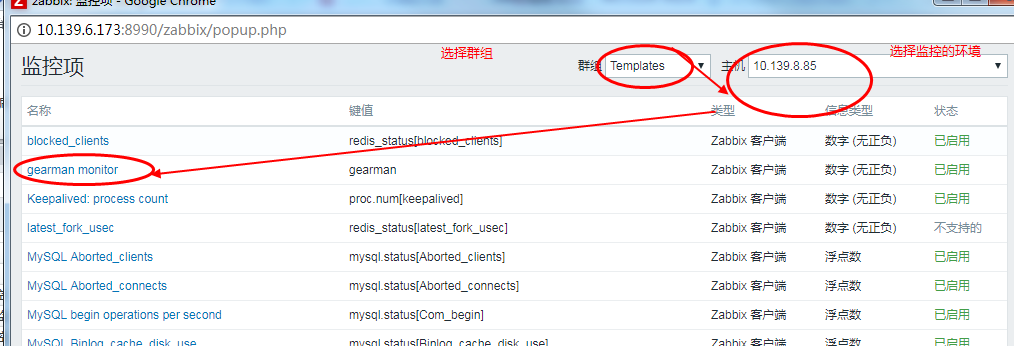


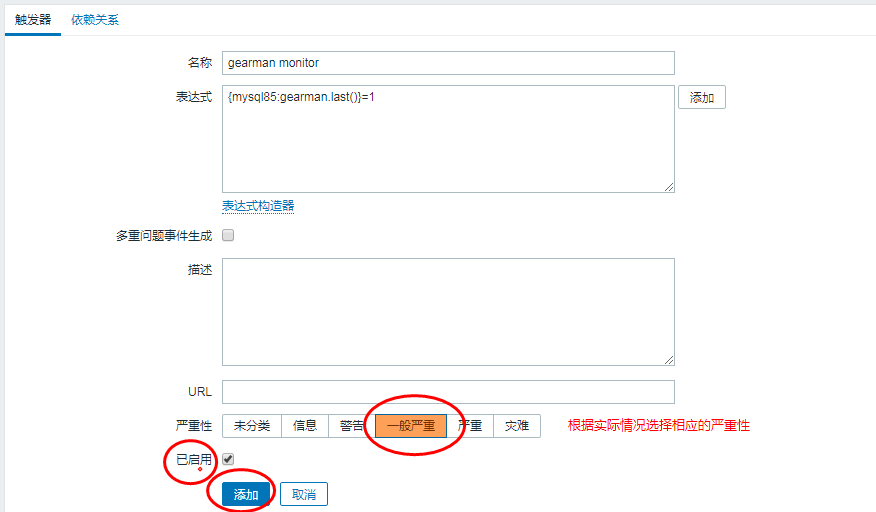


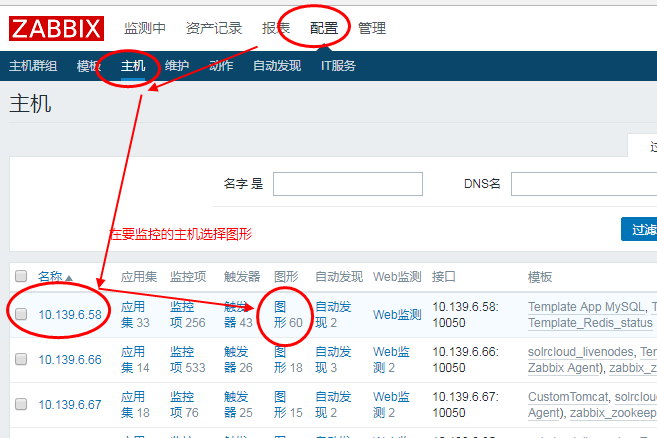




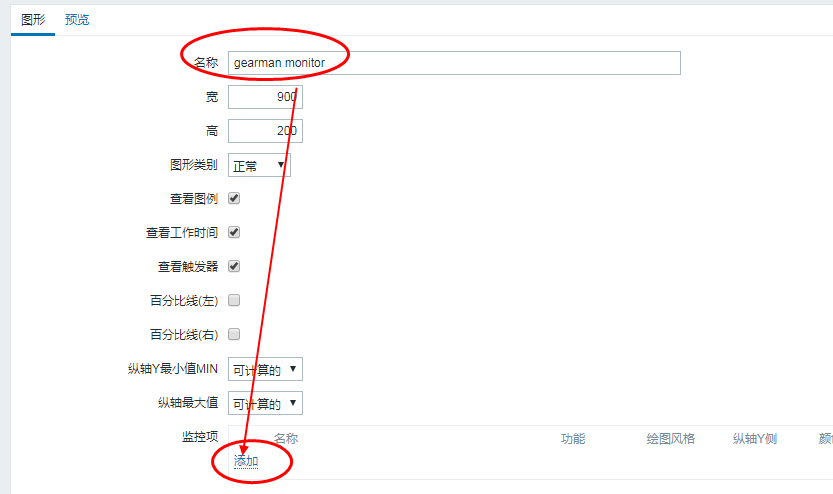




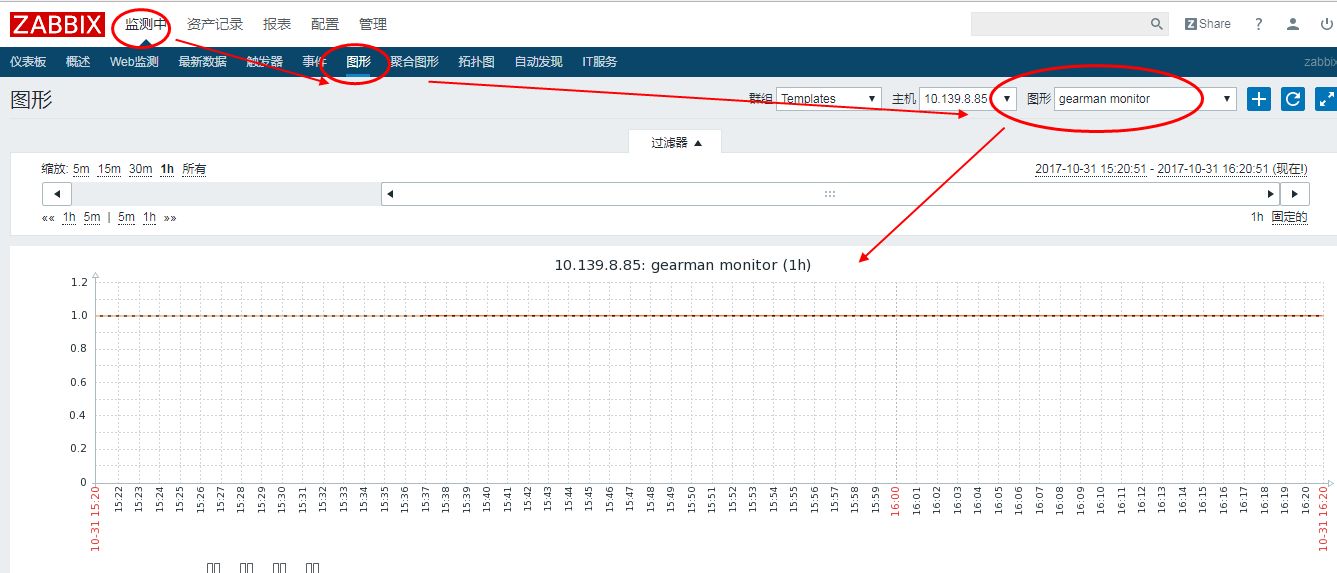








1. 最终在监控中可以查看最终效果



**说明：按照章节12可以配置任意进程的监控**

解决中文乱码问题

这个问题是由于zabbix的web端没有中文字库，我们最需要把中文字库加上即可

* 找到本地C:\Windows\Fonts\simkai.ttf（楷体），上传到服务器zabbix网站目录：\var\www\html\zabbix\fonts下
* 修改zabbix的web端/var/www/html/zabbix/include/defines.inc.php

将graphfont替换为simkai，一共两处需要修改，如下图





* 保存退出
* 无须重启服务，刷新zabbix监控页面即