Security-05

服务安全与监控

# 监控

## 监控的目的：

### 报告系统运行状态

每一部分必须同时监控

内容包括吞吐量、反应时间、使用率

### 提前发现问题

进行服务器性能调整前，直到调整什么

找出系统的瓶颈在什么地方

## 监控的资源类别

### 公开数据

Web、FTP、SSH、数据库等应用服务

TCP或UDP端口

### 私有数据

CPU、内存、磁盘、网卡流量等使用信息

用户、进程等运行信息

## 监控软件

### 系统监控命令

ps 、 ifconfig、uptime(查看cpu负载1，5，15分钟)、netstat或ss、free(查看内存信息)、ping、swapon -s(查看交换分区) 、traceroute（路由追踪）、df -h(查看所有磁盘的使用率) 、iostat（查看磁盘的读写速度）

[root@client51 ~]# ifconfig eth0 | awk '/RX p/{print $5}' //网卡接受数据流量

[root@client51 ~]# ifconfig eth0 | awk '/TX p/{print $5}'//网卡发送数据流量

[root@client51 ~]# ss -ntupl //查看本机监听的所有端口

[root@client51 ~]# ss -antup //查看所有的网路连接信息

### 自动化监控系统

cati

基于SNMP（简单网络管理）协议的监控软件，强大的绘图能力

Nagios（无画图功能）

基于Agent监控，强大的状态检查与报警机制

插件及多，自己写监控脚本潜入到Nagios非常方便

Zabbix

基于多种监控机制，支持分布式监控

# Zabbix基础

## Zabbix简介

**Zabbix**是一个高度集成的监控监控解决方案

可以实现企业级的开源分布式监控

**Zabbix**通过C/S模式采集监控数据

**Zabbix**通过B/S模式实现Web管理

## Zabbix监控拓扑

### 监控服务器

监控服务器可以通过SNMP或Agent采集数据

数据可以写入MySQL、Oracle等数据库中

服务器使用LNMP实现web前端的管理

### 被监控主机

被监控主机需要Agent

常见的网络设备一般支持SNMP

# 部署LNMP

## 安装前准备

### 监控服务器

设置主机名（node2）

设置IP地址（192.168.4.5）

关闭防火墙、SELinux

### 监控客户端

主机client50（192.168.4.50）

主机client51（192.168.4.51）

安装nginx及其依赖包

[root@node2 ~]# yum -y install gcc pcre-devel zlib-devel

[root@node2 ~]# tar -xf zabbix.tar.gz

[root@node2 ~]# cd zabbix/

[root@node2 zabbix]# tar -xf nginx-1.12.2.tar.gz

[root@node2 zabbix]# cd nginx-1.12.2/

[root@node2 nginx-1.12.2]# ./configure --prefix=/usr/local/nginx

[root@node2 nginx-1.12.2]# make && make install

[root@node2 ~]# echo 123 > /usr/local/nginx/html/test.html

[root@node2 ~]# /usr/local/nginx/sbin/nginx

[root@node2 ~]# curl http://192.168.4.5/test.html

**安装并运行MySQL服务**

[root@node2 ~]# yum -y install mariadb-server mariadb-devel

[root@node2 ~]# systemctl start mariadb

[root@node2 ~]# systemctl enable mariadb

[root@node2 ~]# mysqladmin -uroot password

New password:

Confirm new password:

[root@node2 ~]# mysql -uroot -p

**安装php软件并运行php-fpm服务**

[root@node2 ~]# yum -y install php-mysql php

[root@node2 ~]# cd zabbix/

[root@node2 zabbix]# yum -y install php-fpm-5.4.16-42.el7.x86\_64.rpm

[root@node2 zabbix]# systemctl start php-fpm

[root@node2 zabbix]# systemctl enable php-fpm

**修改nginx配置**

[root@node2 ~]# vim /usr/local/nginx/conf/nginx.conf

17 http {

18 include mime.types;

19 default\_type application/octet-stream;

20

21 fastcgi\_buffers 8 16k; //缓存php生成的页面内容，8个16k

22 fastcgi\_buffer\_size 32k; //缓存php生成的头部信息

23 fastcgi\_connect\_timeout 300; //连接php的超时时间

24 fastcgi\_send\_timeout 300; //发送请求的超时时间

25 fastcgi\_read\_timeout 300; //读取请求的超时时间

......

65 location ~ \.php$ {

66 root html;

67 fastcgi\_pass 127.0.0.1:9000;

68 fastcgi\_index index.php;

69 include fastcgi.conf;

70 }

[root@node2 ~]# /usr/local/nginx/sbin/nginx -s reload

[root@node2 ~]# cat /usr/local/nginx/html/test.php

<?php

$i=”hello world”;

echo $i

?>

[root@node2 ~]# curl http://192.168.4.5/test.php

hello world

# 部署Zabbix

## 编译安装Zabbix服务

## 源码安装软件

[root@node2 zabbix]# useradd zabbix

[root@node2 zabbix]# rpm -q gcc

gcc-4.8.5-16.el7.x86\_64 //zabbix依赖包

[root@node2 zabbix]# yum -y install libevent-devel-2.0.21-4.el7.x86\_64.rpm libcurl-devel net-snmp-devel //安装依赖包

**注：自行下载软件包**libevent-devel-2.0.21-4.el7.x86\_64.rpm

[root@node2 zabbix]# tar -xf zabbix-3.4.4.tar.gz

[root@node2 zabbix-3.4.4]# cd zabbix-3.4.4/

[root@node2 zabbix-3.4.4]# ./configure --prefix=/usr/local/zabbix --enable-server --enable-agent --with-mysql --with-net-snmp --with-libcurl



**--enable-server //提供监控服务模块**

**--enable-proxy //代理模块**

**--enable-agent //根据是否需要监控自己选择安装此模块（私有数据）**

**--with-mysql //配置mysql\_config路径**

**--with-net-snmp //允许zabbix通过snmp协议监控其他设备（硬件信息）**

**--with-libcurl //安装相关curl库文件，使zabbix就可以通过curl连接http等服务，测试被监控主机服务的状态（公共数据）**

## 初始化Zabbix

### 创建数据库与数据库账户

[root@node2 ~]# mysql -uroot -p123456

MariaDB [(none)]> create database zabbix character set utf8;

//创建数据库，支持中文字符集

MariaDB [(none)]> grant all on zabbix.\* to zabbix@'localhost' identified by 'zabbix'; //创建可以访问数据库的账户与密码

[root@node2 ~]# mysql -hlocalhost -pzabbix -uzabbix

//保证授权用户能够连接到数据库

[root@node2 zabbix-3.4.4]# cd database/mysql/

[root@node2 mysql]# mysql -uzabbix -pzabbix zabbix < schema.sql

[root@node2 mysql]# mysql -uzabbix -pzabbix zabbix < images.sql

[root@node2 mysql]# mysql -uzabbix -pzabbix zabbix < data.sql

//刚刚创建是空数据库，zabbix源码包目录下，有提前准备好的数据

//使用mysql导入这些数库即可（注意导入数据）

[root@node2 mysql]# mysql -uzabbix -pzabbix zabbix

MariaDB [zabbix]> show tables;

### 上线Zabbix页面

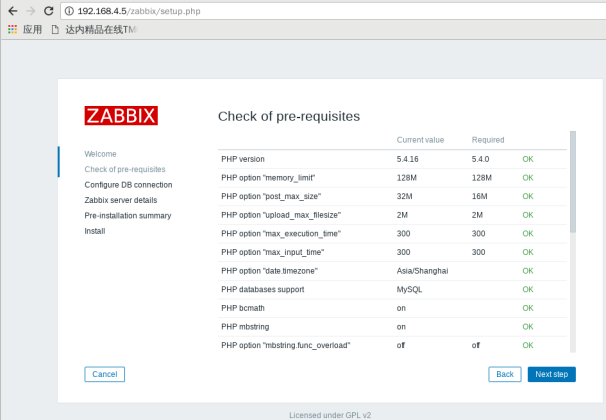
[root@node2 ~]# cd /root/zabbix/zabbix-3.4.4

[root@node2 php]# cp -r frontends/php/ /usr/local/nginx/html/zabbix

[root@node2 zabbix]# chmod o+w /usr/local/nginx/html/zabbix/conf

### 初始化web管理页面（浏览器访问web）

1. 网页浏览http://192.168.4.5/zabbix/index.php（左图）
2. 点击下一步,确认都是OK状态（右图）

### 根据检查的报警提示，修改系统环境

修改php程序的运行参数，并安装依赖软件包

[root@node2 mysql]# yum -y install php-gd php-xml php-ldap

[root@node2 zabbix]# yum -y install php-bcmath-5.4.16-42.el7.x86\_64.rpm php-mbstring-5.4.16-42.el7.x86\_64.rpm

[root@node2 zabbix]# vim /etc/php.ini

date.timezone = Asia/Shanghai //设置时区

max\_execution\_time = 300 //最大执行时间（秒）

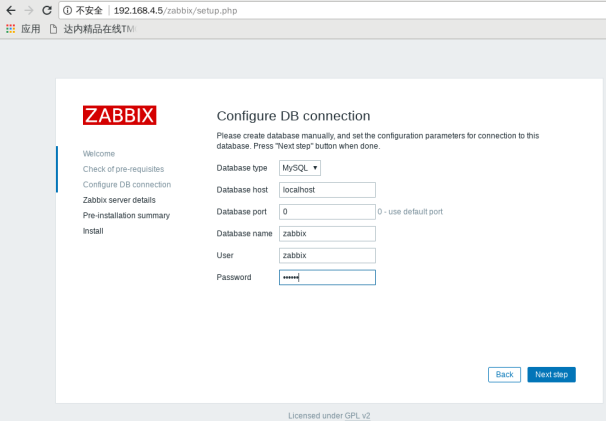
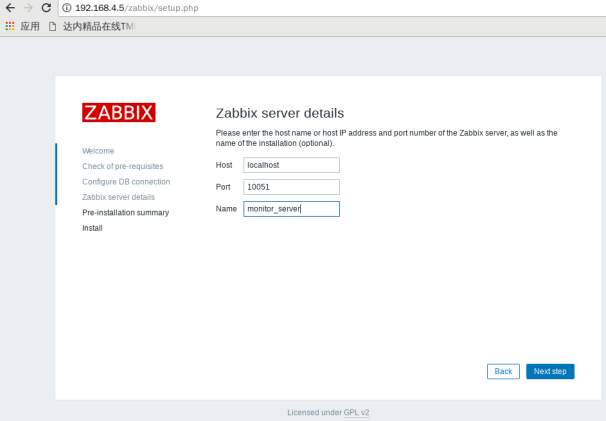
post\_max\_size = 32M //POST数据最大容量

max\_input\_time = 300 //服务器接收数据的时间限制

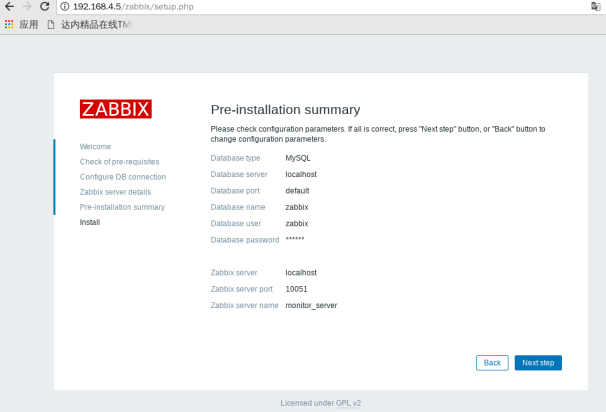
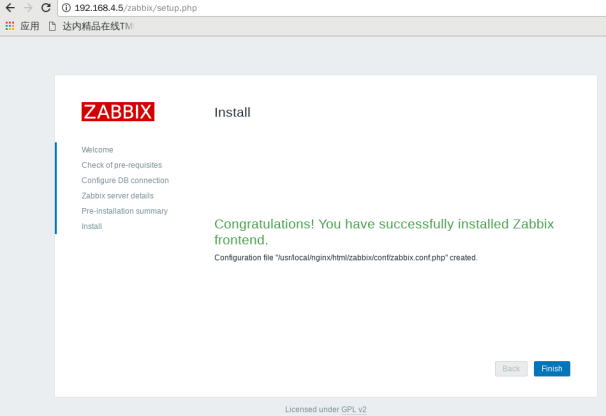
memory\_limit = 128M

[root@node2 zabbix]# systemctl restart php-fpm

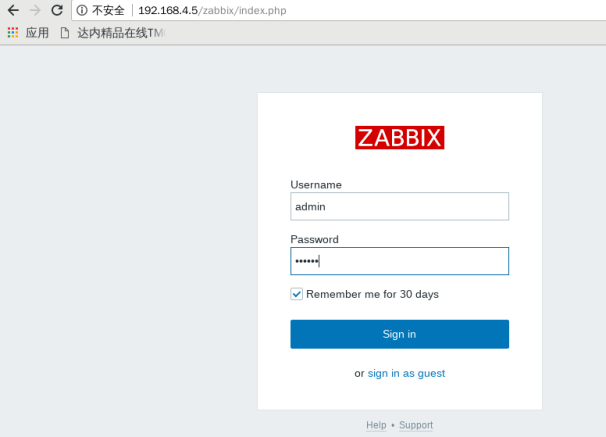
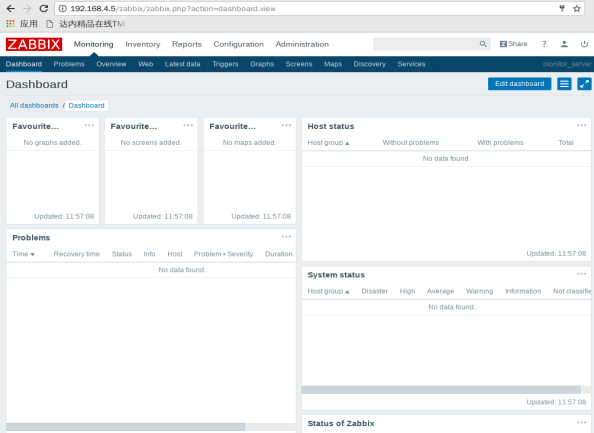
1. 输入用户名密码，点击下一步（左图）
2. zabbix本地设置，host和port默认，Name名字自己起（右图）

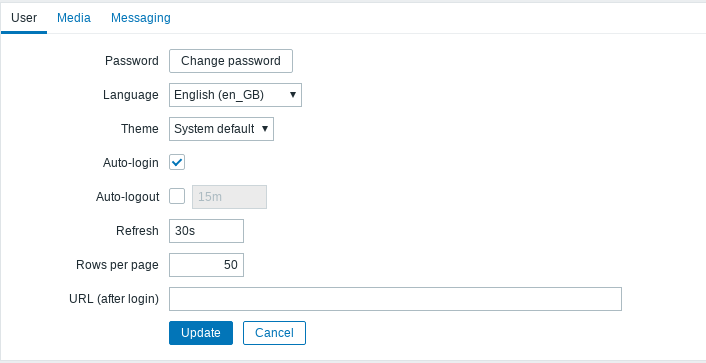
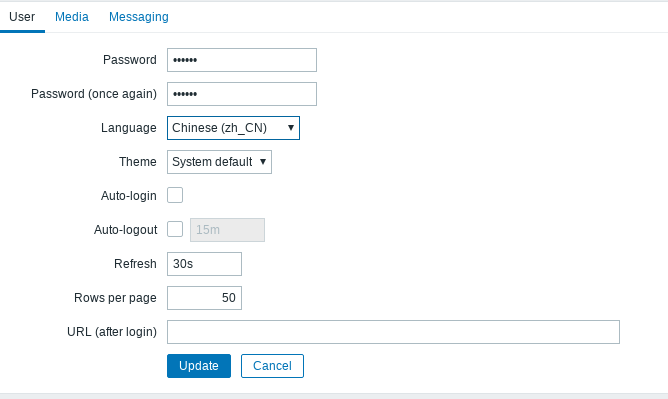
1. 确认信息，点击下一步（左图）
2. 如果之前所有的配置无错，则下一步之后则如（右图）所示

1. 点击下一步，进入登录页面，输入（初始）帐号admin、密码zabbix（左图）
2. 登入之后进行初始管理（修改语言、密码）（右图）

1. 点击左上角的小人图标进行设置，进入设置初始页面（如左图）
2. 点击第一栏change password修改密码（如右图）
3. 设置完成之后点击update完成初始配置

### 修改配置文件，启动zabbix server 服务

[root@node2 zabbix]# vim /usr/local/zabbix/etc/zabbix\_server.conf

38 LogFile=/tmp/zabbix\_server.log //设置日志

85 DBHost=localhost //数据库主机默认被注释

95 DBName=zabbix //设置数据库名称

111 DBUser=zabbix //设置数据库账户

119 DBPassword=zabbix //设置数据库密码，默认被注释

[root@node2 zabbix-3.4.4]# cp misc/init.d/fedora/core/zabbix\_server /etc/init.d/

[root@node2 zabbix-3.4.4]# chmod +x /etc/init.d/zabbix\_server

[root@node2 zabbix-3.4.4]# vim /etc/init.d/zabbix\_server

22 BASEDIR=/usr/local/zabbix //修改为安装时指定的目录

[root@node2 zabbix-3.4.4]# /etc/init.d/zabbix\_server start //启动服务

[root@node2 zabbix-3.4.4]# netstat -natpul | grep zabbix



如果有报错，查看启动日志/tmp/zabbix\_server.log

**zabbix的配置信息保存位置：**

/usr/local/nginx/html/zabbix/conf/zabbix.conf.php

网页zabbix的状态显示如下：



掌握软件的基本使用

查看监控服务器已经监控的主机

查看监控服务器支持的监控模版

查看监控信息

### 监控本机，在本机修改zabbix\_agentd服务

### 修改配置文件，启动zabbix agent（被监控时使用）

[root@node2 zabbix]# vim /usr/local/zabbix/etc/zabbix\_agentd.conf

30 LogFile=/tmp/zabbix\_agentd.log //设置日志文件

93 Server=127.0.0.1 //设置监控服务器IP

134 ServerActive=127.0.0.1:10051 //主动监控服务器IP

145 Hostname=Zabbix server

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

//自定义监控命令的存放路径

280 UnsafeUserParameters=1 //是否允许自定义key

[root@node2 zabbix-3.4.4]# cp misc/init.d/fedora/core/zabbix\_agentd /etc/init.d/ //复制启动脚本到/etc/init.d目录下

[root@node2 zabbix-3.4.4]# chmod +x /etc/init.d/zabbix\_agentd

//给此脚本加x权限

[root@node2 zabbix-3.4.4]# vim /etc/init.d/zabbix\_agentd

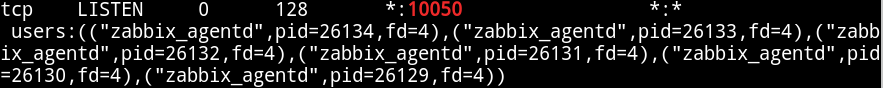
BASEDIR=/usr/local/zabbix //修改为安装时启动的目录

[root@node2 zabbix-3.4.4]# /etc/init.d/zabbix\_agentd start

//使用脚本启动服务启动

[root@node2 zabbix-3.4.4]# ss -natpul | grep 10050

//查看服务是否启动

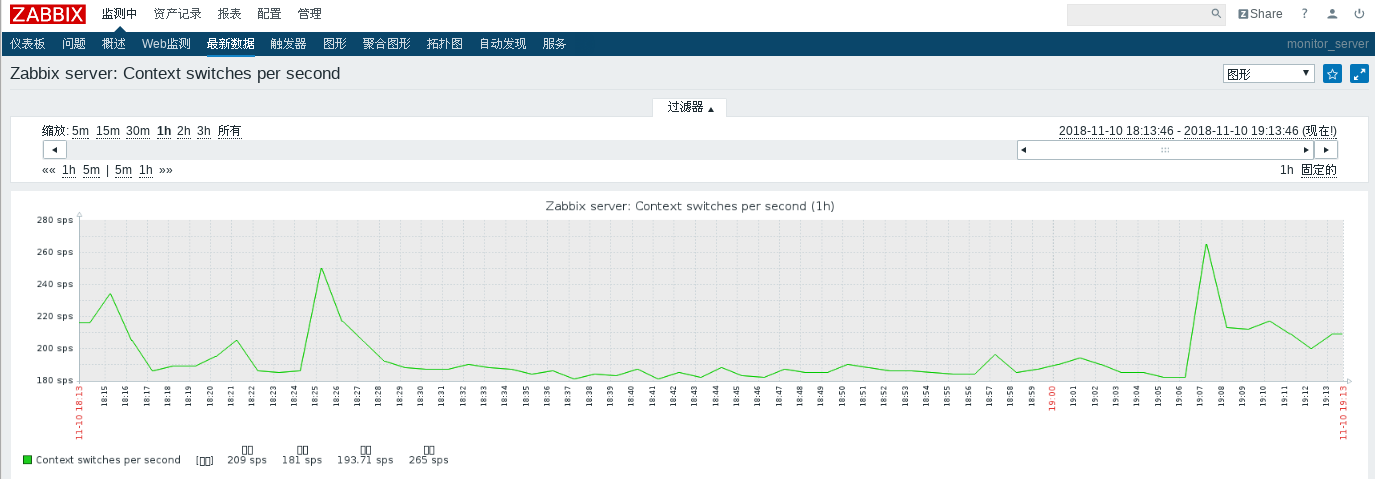


登录web页面，添加监控本机（默认监控本机，直接启用即可）



**点击**“停用的”*，在弹*出的对话框中选择确定即可启用





## 监控远端主机

### 配置远端主机（客户端）

### 被监控主机安装zabbix(50和51做相同操作，以51为例)

[root@client51 zabbix]# tar -xf zabbix-3.4.4.tar.gz

[root@client51 zabbix]# cd zabbix-3.4.4/

[root@client51 zabbix-3.4.4]# useradd zabbix

[root@client51 zabbix-3.4.4]# yum -y install pcre-devel gcc

[root@client51 zabbix-3.4.4]# ./configure --enable-agent --prefix=/usr/local/zabbix



[root@client51 zabbix-3.4.4]# make && make install

**修改配置文件**

[root@client51 zabbix-3.4.4]# vim /usr/local/zabbix/etc/zabbix\_agentd.conf

69 # EnableRemoteCommands=0（默认状态，若需要，自行修改）

//监控异常后，是否允许服务器远程过来执行命令

93 Server=127.0.0.1,192.168.4.5 //谁可以监控本机（被动监控）

134 ServerActive=192.168.4.5:10051 //谁可以监控本机（主动监控）

145 Hostname=Zabbix server //被监控端自己的主机名（自定义）

280 UnsafeUserParameters=1 //是否允许自定义key监控

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

//自定义监控命令的存放路径

**拷贝启动脚本并启动服务**

[root@client51 zabbix-3.4.4]# cd misc/init.d/fedora/core

[root@client51 core]# cp zabbix\_agentd /etc/init.d/

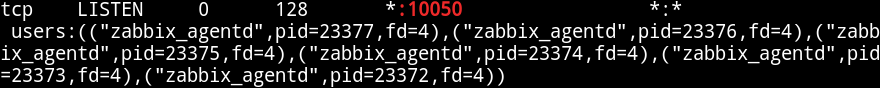
[root@client51 core]# chmod +x /etc/init.d/zabbix\_agentd

[root@client51 zabbix-3.4.4]# vim /etc/init.d/zabbix\_agentd

BASEDIR=/usr/local/zabbix

[root@client51 zabbix-3.4.4]# /etc/init.d/zabbix\_agentd start

[root@client51 zabbix-3.4.4]# ss -natpul | grep :10050



### 添加监控主机

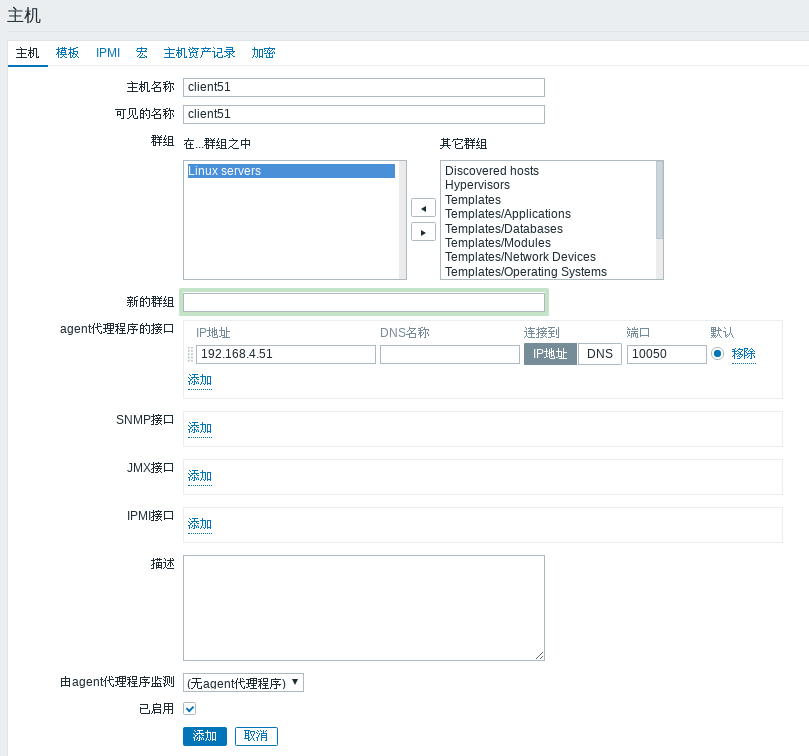
Host（主机）是监控的基本载体

zabbix所有监控都是基于Host

通过Configuration（配置）—>Hosts（主机）—>Create Host（创建主机）创建

根据提示输入

主机名称、可见名称、在...群组之中、IP地址，其余默认即可



添加监控模版

模版-选择合适的模版添加

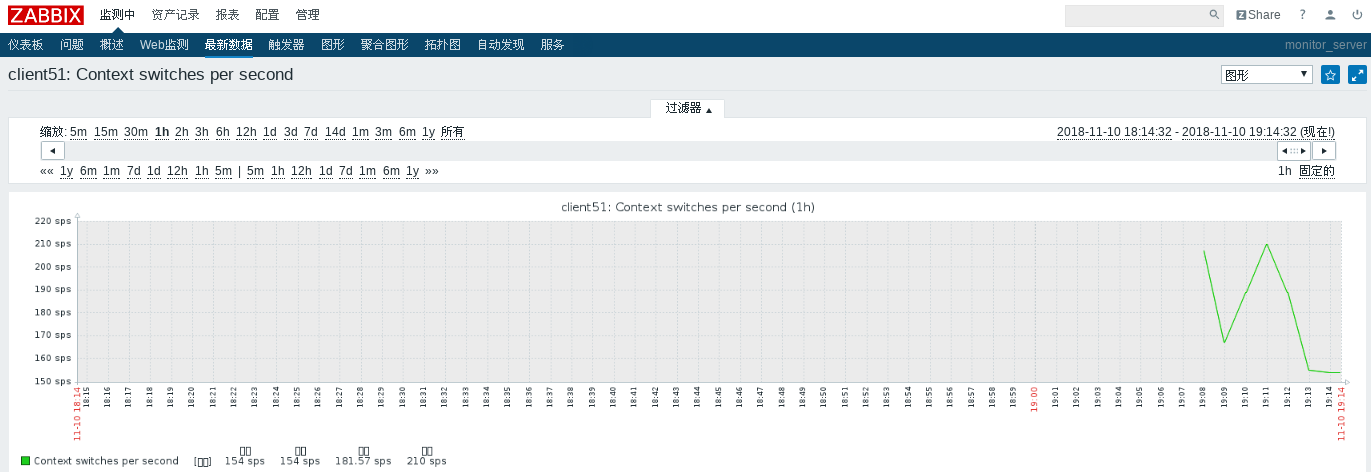


查看监控数据

点击’监测中-最新数据‘，在过滤器中填写条件，根据群组和主机搜索即可



找到需要的数据，点击后面的’图形‘



自定义监控

配置被监控端192.168.4.51

允许自定义监控项

[root@client51 zabbix-3.4.4]# vim /usr/local/zabbix/etc/zabbix\_agentd.conf

280 UnsafeUserParameters=1 //是否允许自定义key监控

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

//自定义监控命令的存放目录

[root@client51 zabbix-3.4.4]# /etc/init.d/zabbix\_agentd stop

[root@client51 zabbix-3.4.4]# /etc/init.d/zabbix\_agentd start

定义监控命令

[root@node2 ~]#vim/usr/local/zabbix/etc/zabbix\_agentd.conf.d/user.count

UserParameter=user.count,wc -l /etc/passwd | awk '{print $1}'

///自定义key语法格式：UserParameter=自定义key名称，命令

[root@client51 ~]# cat /etc/passwd | wc -l

[root@client51 ~]# sed -n '$=' /etc/passwd

[root@client51 ~]# awk 'END{print NR}' /etc/passwd

[root@client51 zabbix-3.4.4]# /etc/init.d/zabbix\_agentd stop

[root@client51 zabbix-3.4.4]# /etc/init.d/zabbix\_agentd start

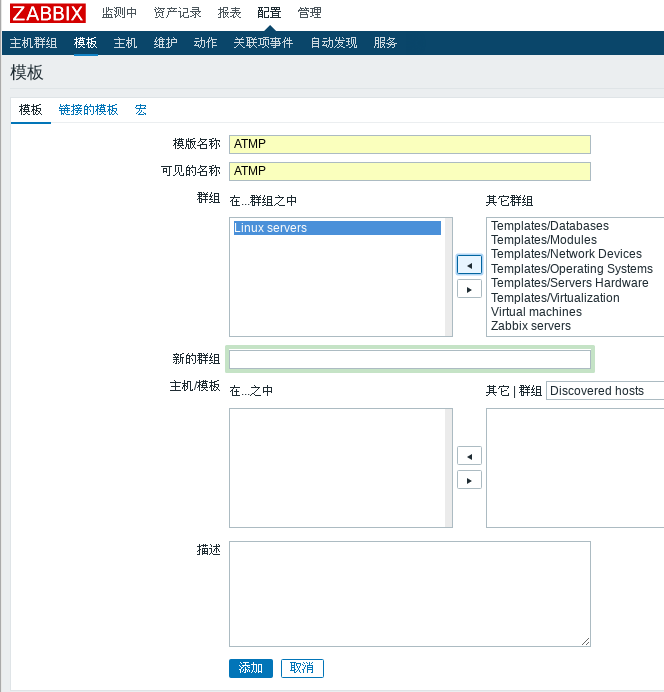
测试定义的监控命令

[root@node2 zabbix-3.4.4]# cd /usr/local/zabbix/bin/

[root@node2 bin]# ./zabbix\_get -s 192.168.4.51 -k user.count

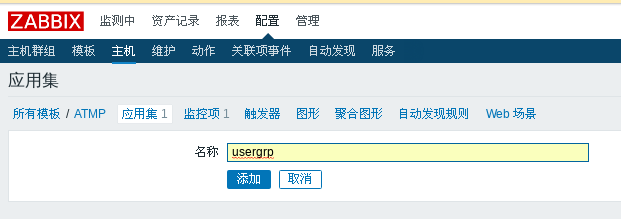
创建监控模版

配置-模版-创建模版-模版名称-可见的名称-群组-添加(下左图)



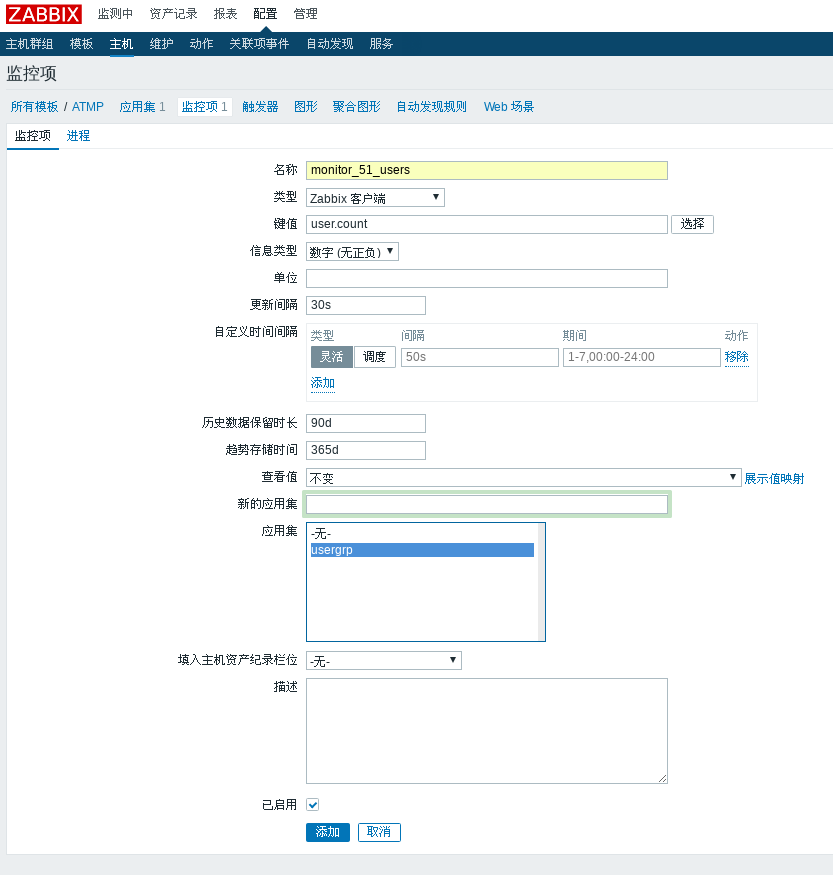
创建应用集（下图）

配置-模版-ATMP（应用集）-创建应用集-名称-添加



创建监控项

配置-模版-ATMP（监控项）-创建监控项（名称，键值，应用集）-添加



监控主机51时调用新创建的模版

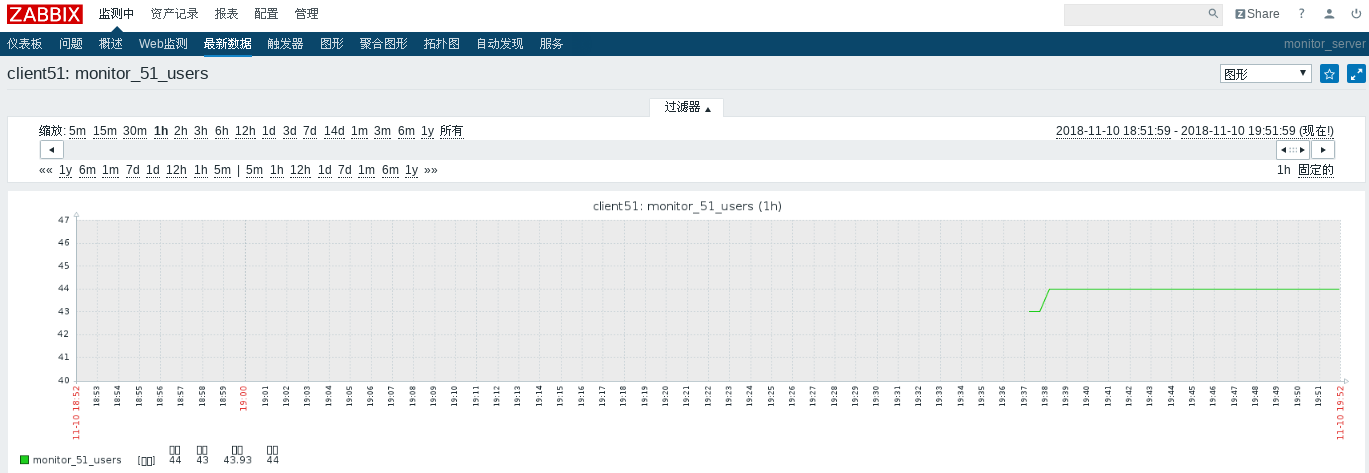
配置-主机-client51-模版-链接指示器-添加-更新



查看监控信息

监测中-最新数据-主机群组-主机-应用-选择要查看的监控项，点击图形





创建图形

配置-模板-ATMP-图形-创建图形（名称-监控[添加]-添加）

