Zabbix\_server端配置（用于redhat7/centos7）

1. 基础环境方面
2. 网络畅通，测试ping [www.baidu.com](http://www.baidu.com)
3. setenforce 0
4. systemctl stop firewalld
5. 基础架构平台lamp的部署
6. 安装lamp

yum install -y httpd mariadb-server mariadb php php-mysql php-gd libjpeg\* php-ldap php-odbc php-pear php-xml php-xmlrpc php-mhash

1. 配置httpd

sed -i 's/DirectoryIndex index.html/DirectoryIndex index.html index.php/g' /etc/httpd/conf/httpd.conf

1. 配置php

sed -i 's/;date.timezone =/date.timezone = PRC/g' /etc/php.ini

1. 启动httpd、mariadb

systemctl start httpd mariadb

查看状态 netstat -anpt|egrep '80|3306'

1. mysql启动后执行初始安全设置

mysql\_secure\_installation

1. 创建测试页,访问测试是否正常

vim /var/www/html/index.php

<?php

phpinfo();

?>

1. 创建用于zabbix存放数据用的数据库并授权

CREATE DATABASE zabbix character set utf8 collate utf8\_bin;

GRANT all  ON zabbix.\* TO 'zabbix'@'%' IDENTIFIED BY '123';

GRANT all  ON zabbix.\* TO 'zabbix'@'localhost' IDENTIFIED BY '123';

flush privileges;

1. 测试zabbix用户是否能够登录数据库

<?php

$link=mysql\_connect('10.0.11.32','zabbix','zz');

if($link) echo "<h1>Success!!</h1>";

else echo "Fail!!";

mysql\_close();

?>

1. zabbix\_server安装
2. zabbix的yum配置

rpm -ivh https://repo.zabbix.com/zabbix/4.0/rhel/7/x86\_64/zabbix-release-4.0-1.el7.noarch.rpm

1. 安装zabbix\_server以及组件

yum install zabbix-server-mysql zabbix-web-mysql

1. 导入zabbix数据库初始模式以及数据

zcat /usr/share/doc/zabbix-server-mysql-4.0.4/create.sql.gz |mysql -uzabbix -p zabbix

1. 调整zabbix的配置文件

vim /etc/zabbix/zabbix\_server.conf

LogFile=/var/log/zabbix/zabbix\_server.log  #日志文件的存放位置

LogFileSize=10 #说明：日志达到多少M里就轮转；若此参数值为0时，则不轮转，日志将不断变大，建议设置成轮转。

PidFile=/var/run/zabbix/zabbix\_server.pid #pid文件的存放位置

DBHost=localhost #数据库主机名，当设置为localhost时，连接mysql通过sock

DBName=Zabbix #指定存 放zabbix数据数据库的名字

DBUser=Zabbix  #指定连接数据库的用户名

DBPassword=123 #用户连接数据库需要的密码

StartIPMIPollers=1 #说明:主要用于IPmi技术用于获取硬件状态场景。若无相关监控项，建议设置为0

SNMPTrapperFile=/var/log/snmptrap/snmptrap.log

Timeout=4  #说明：与AGNET\SNMP设备和其它外部设备通信超时设置，单位为秒；若采集数据不完整或网络繁忙，或从管理页面发现客户端状态变化频繁，可以考虑加大此数值。注意若此数值加大，应该考虑参数StartPollers 是否有相应加大的必要

AlertScriptsPath=/usr/lib/zabbix/alertscripts  #监控报警脚本的存放路径

LogSlowQueries=3000 #说明:用于服务端数据库慢查询功能，单位是毫秒；1毫秒=0.001秒，若有服务端数据库监控慢查询的需求，可以视具体情况调整此数。

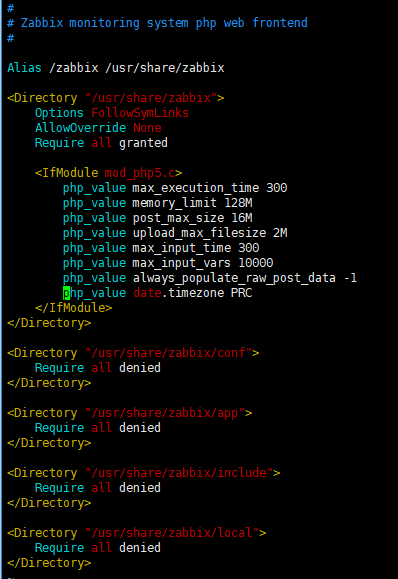
1. 启动zabbix服务进程

systemctl enable zabbix-server

systemctl start zabbix-server

1. 配置zabbix前端

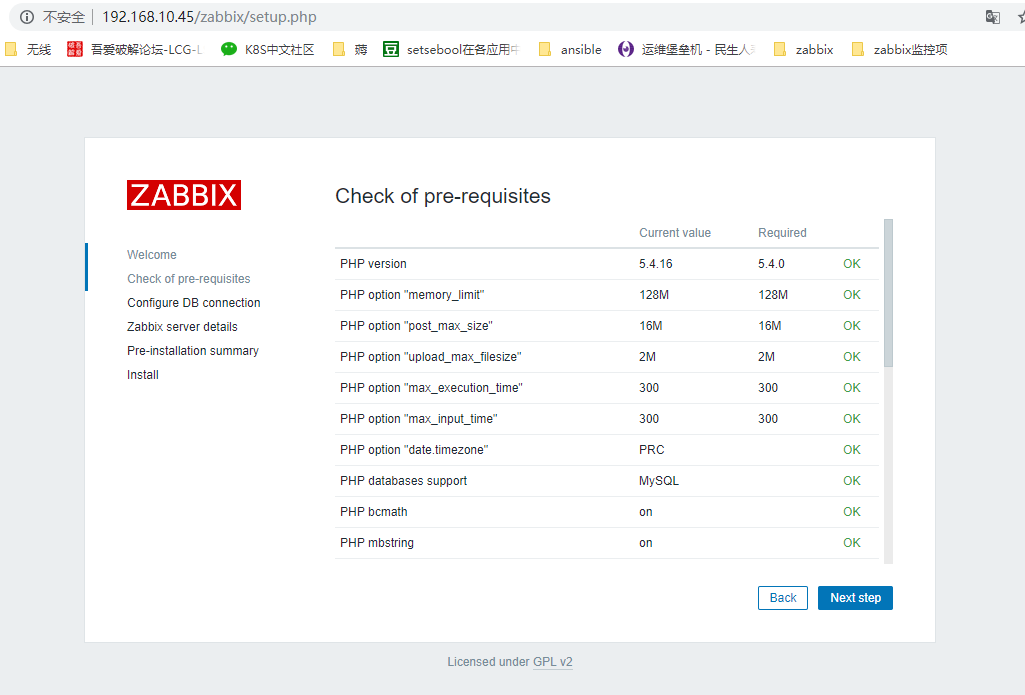
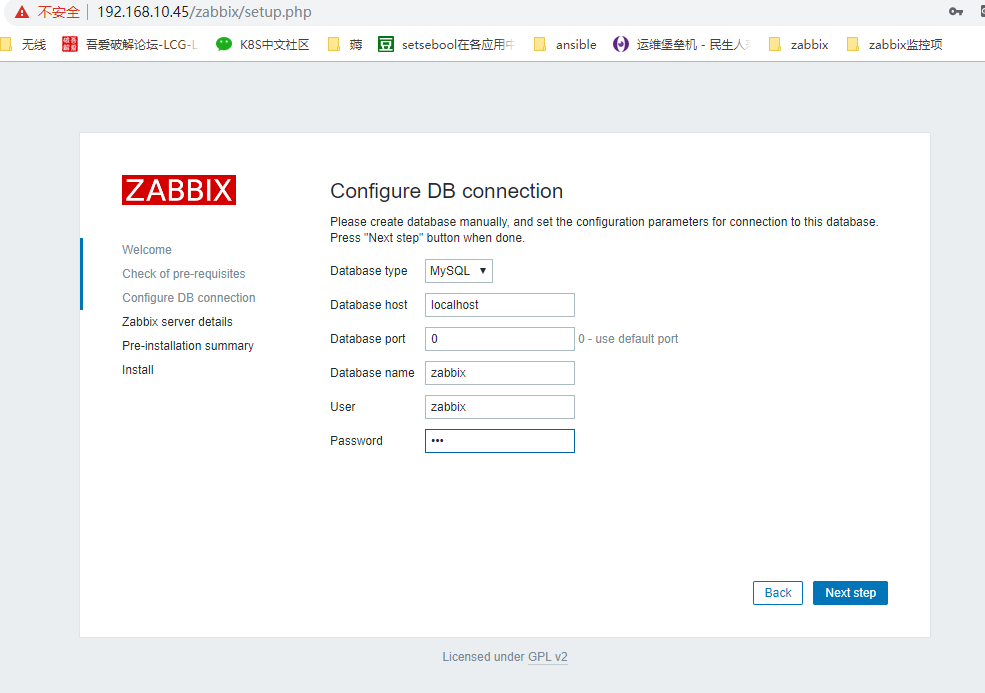
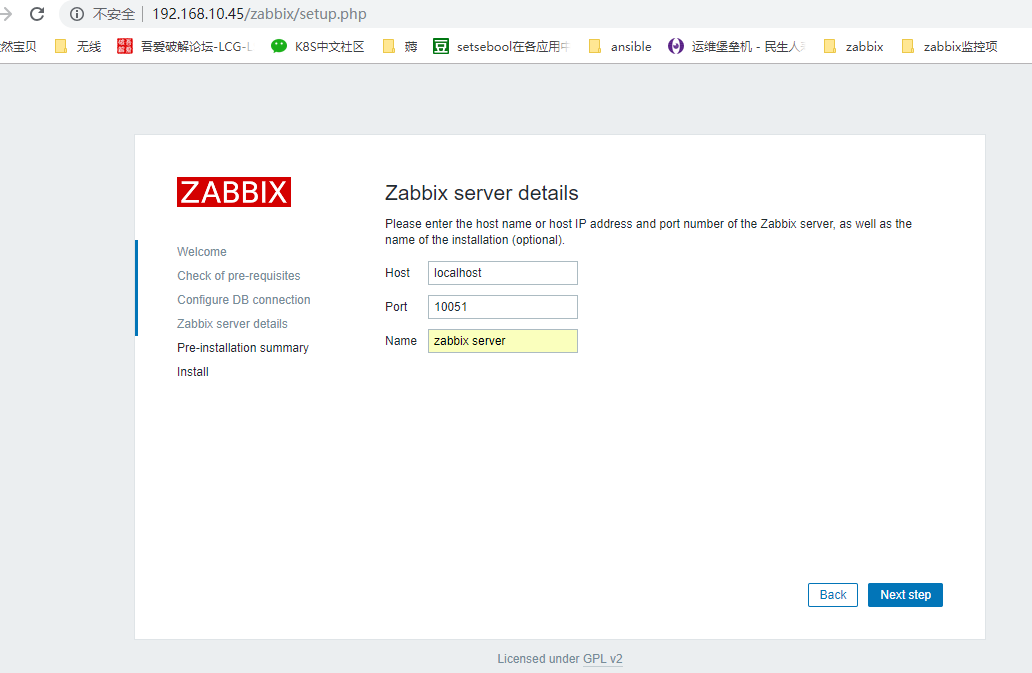
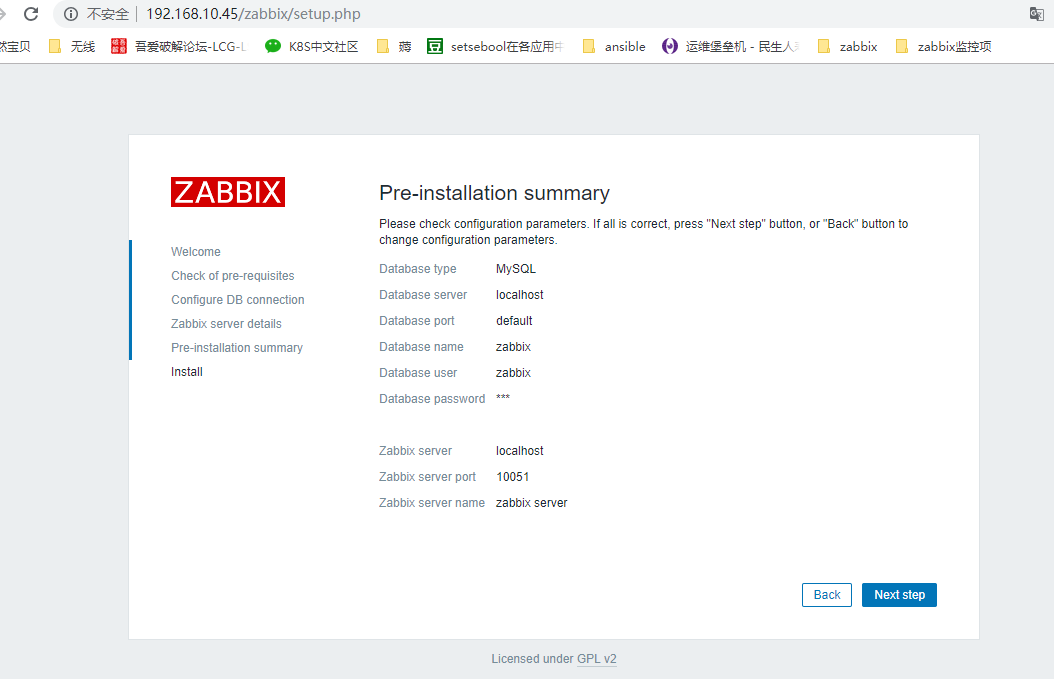
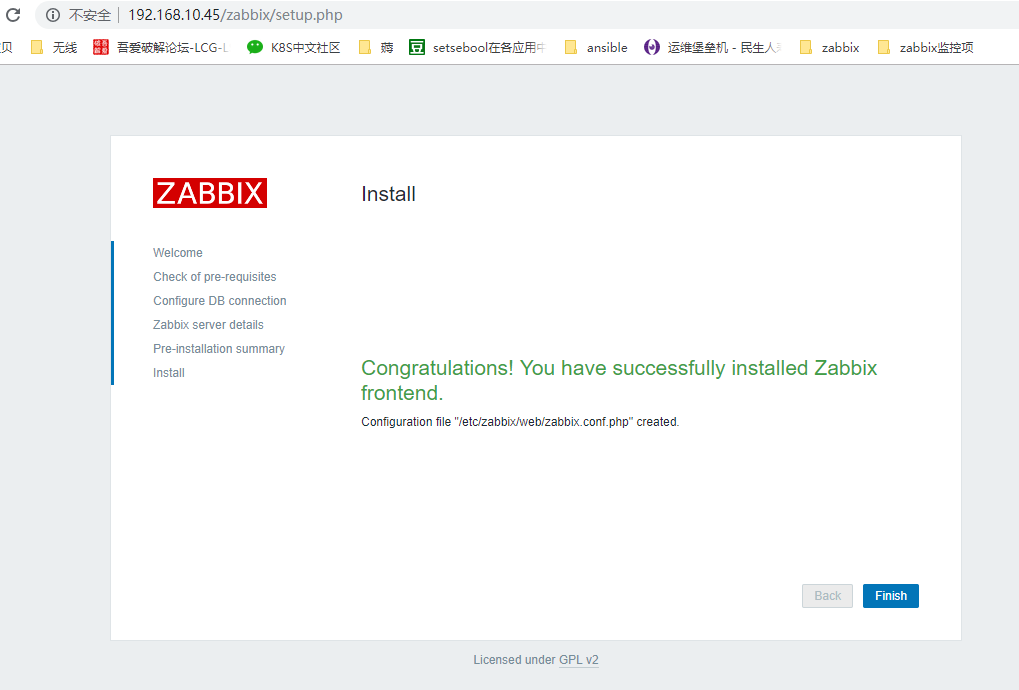
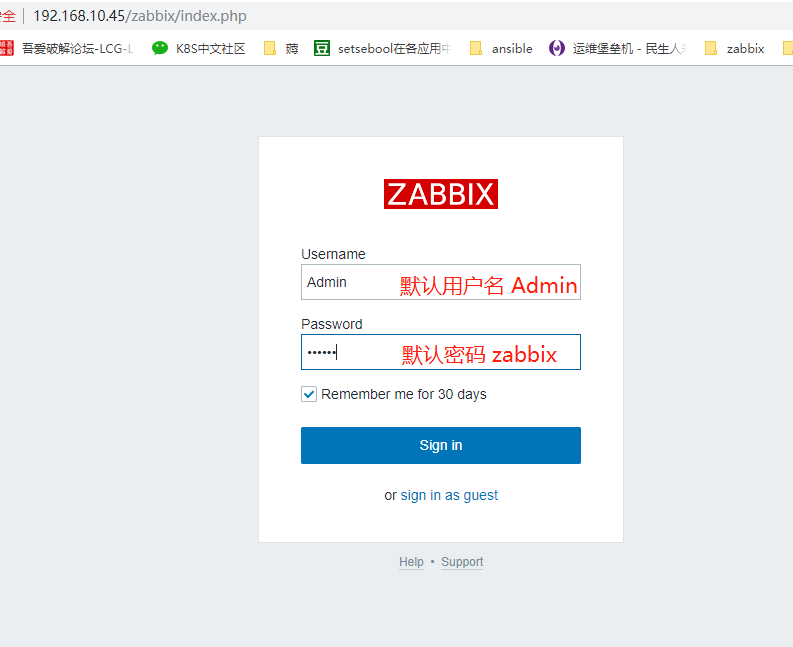
vim /etc/httpd/conf.d/zabbix.conf

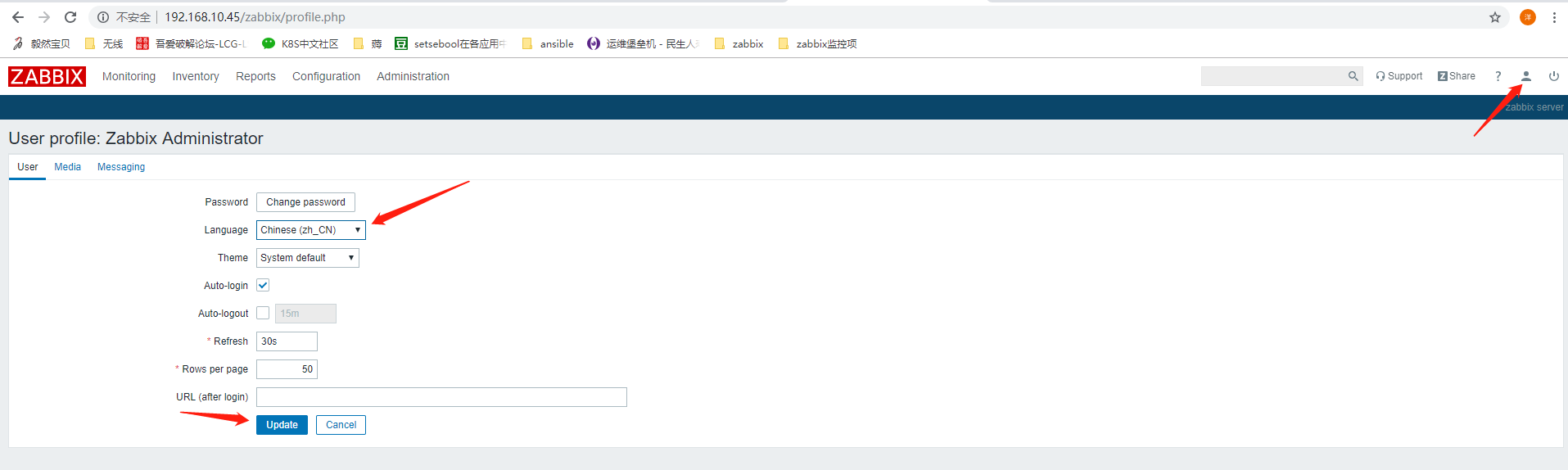


1. 重启httpd，进行zabbix前端的配置

systemctl restart httpd

访问<http://192.168.10.45/zabbix>

1. 
2. 
3. 
4. 
5. 
6. 
7. 
8. 界面设置中文



Wget <http://js.downcc.com/down1/microsoftyaheilight_downcc.zip>

Unzip 解压

Cp 到 /usr/share/zabbix/fonts/mm.ttf

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

define('ZBX\_GRAPH\_FONT\_NAME', 'msyh');

define('ZBX\_FONT\_NAME', 'msyh');

1. Zabbix监控端安装zabbix-agent

yum install zabbix-agent

10、调整zabbix-agent配置文件

LogFileSize=10

SourceIP=192.168.10.45 #通过哪个网卡与server进行数据传输

Server=192.168.10.45 #服务器的ip

#ServerActive=127.0.0.1 #开启主动检查

Hostname=Zabbix\_server #主机名

Include=/etc/zabbix/zabbix\_agentd.d/\*.conf

UnsafeUserParameters=1 #开启自定义监控

备注：主动模式配置

StartAgent=0

ServerActive=主控端ip

1. 启动zabbix-agent

systemctl restart zabbix-agent

1. 完成对zabbix-server端的监控以及配置

Zabbix-agent端4.0版本的配置

1. 配置yum源
2. rpm -ivh https://repo.zabbix.com/zabbix/4.0/rhel/7/x86\_64/zabbix-release-4.0-1.el7.noarch.rpm
3. 安装zabbix-agent

yum -y install zabbix-agenr

1. 修改agent配置文件

vim /etc/zabbix/zabbix\_agent.conf

LogFileSize=10 #日志达到10m重新创建

SourceIP=192.168.10.44 #

Server=192.168.10.45 #

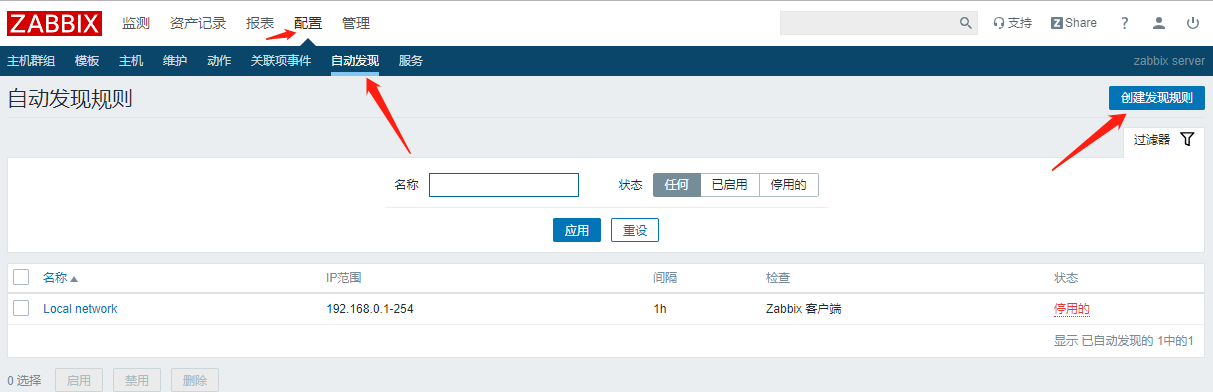
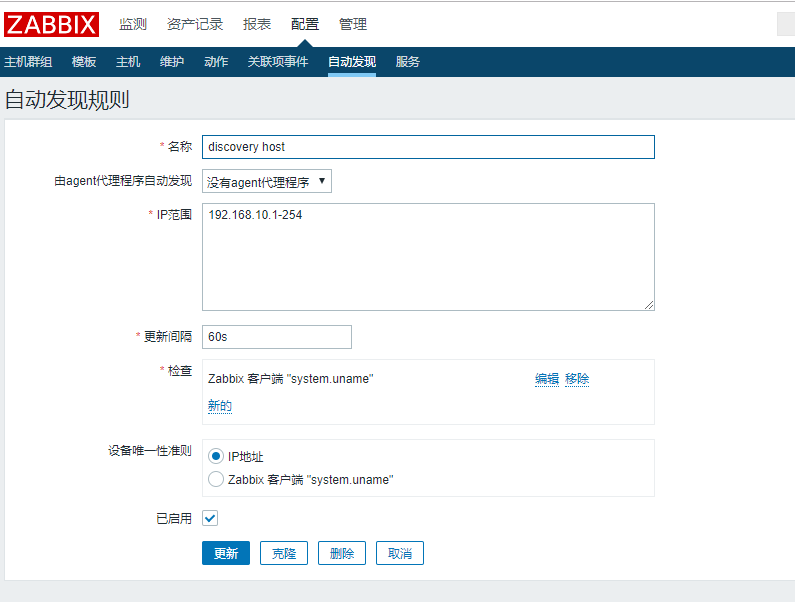
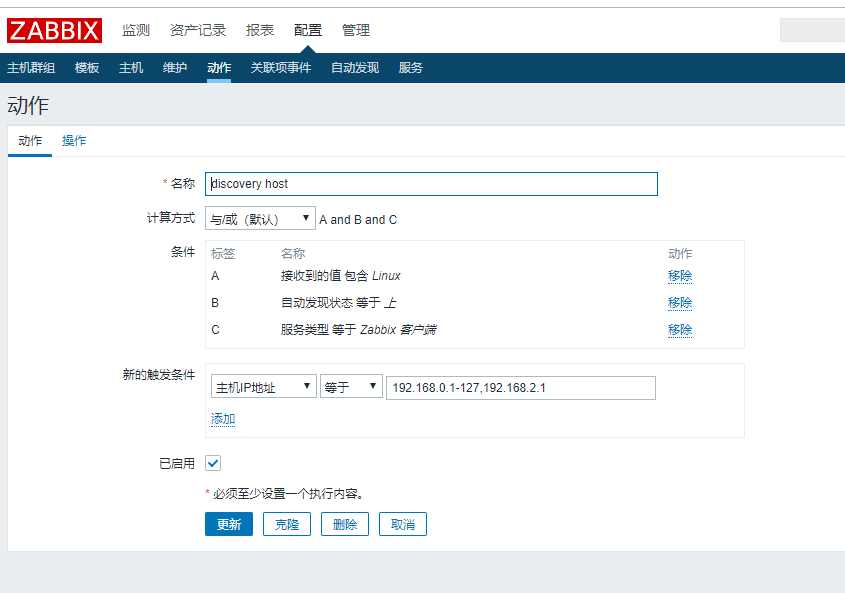
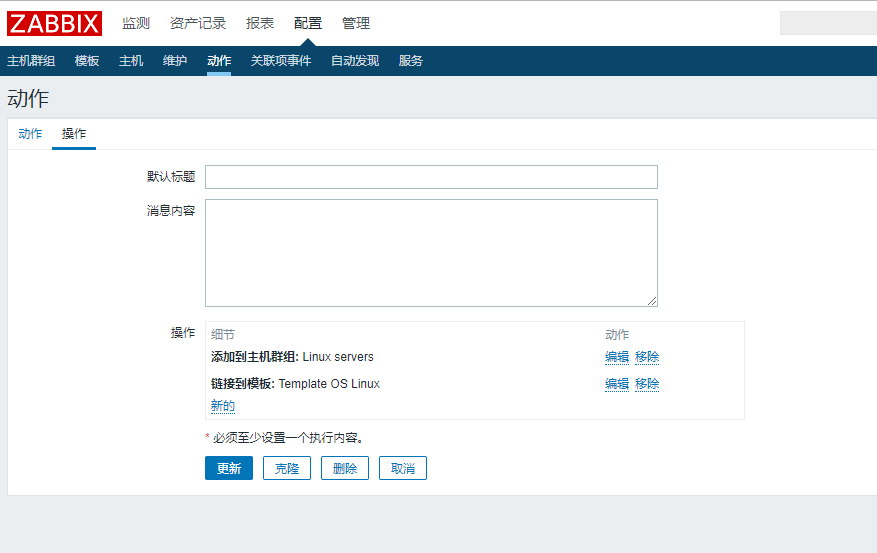
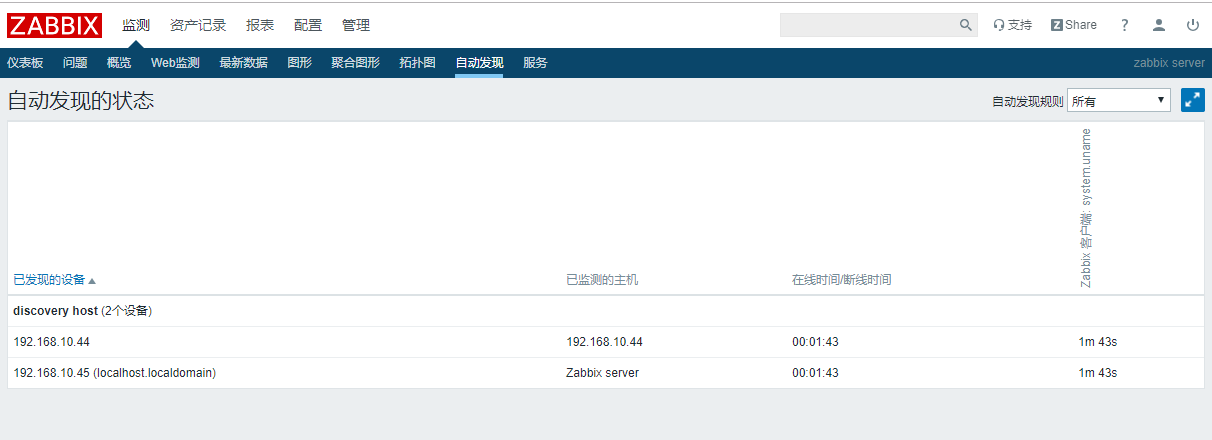
ListenIP=192.168.10.44

UnsafeUserParameters=1

1. 启动zabbix-agent

Systemctl restart Zabbix-agent

简单的自定义发现规则设置

1. 
2. 
3. 
4. 
5. 
6. 

自定义监控项配置

以tcp连接状态为例

1. 自定义键值

vim /etc/zabbix/zabbix\_agentd.d/userparameter\_tcp\_status.conf

UserParameter=tcp.status[\*],/etc/zabbix/scripts/tcp\_conn\_status.sh $1

~

1. 写自定义脚本

vim /etc/zabbix/scripts/tcp\_conn\_status.sh

内容见附件

1. 监控端手动测试能否获取数据

zabbix\_get -s 10.0.11.31 -k 'tcp.status[listen]'

1. Web页面添加监控项items，自定义键值为‘tcp.status[listen]’（详看userparameter\_tcp\_status.conf里面的命名）

告警模板：

【{TRIGGER.STATUS}】

[告警主机]: {HOSTNAME1}

[告警信息]: {TRIGGER.NAME}

[告警等级]: {TRIGGER.SEVERITY}

[告警项目]: {TRIGGER.KEY1}

[问题详情]: {ITEM.NAME}-{ITEM.VALUE}

[当前状态]: {TRIGGER.STATUS}

[告警日期]: {EVENT.DATE}

[告警时间]: {EVENT.TIME}

[事件编号]: {EVENT.ID}

[Glinux].