实训第三天

1.环境

Centos7环境

```
#运行环境
[root@localhost ~]#  cat /etc/redhat-release
CentOS Linux release 7.0.1406 (Core)
```

```
#永久关闭防火墙和SELinux
[root@localhost ~]# systemctl disable firewalld.service
rm '/etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service'
rm '/etc/systemd/system/basic.target.wants/firewalld.service'
[root@localhost ~]# sed -i 's/SELINUX=enforcing/SELINUX=disabled/'
/etc/selinux/config
```

安装LAMP环境

LAMP：Linux + Apache + Mysql / MariaDB + PHP / Perl / Python

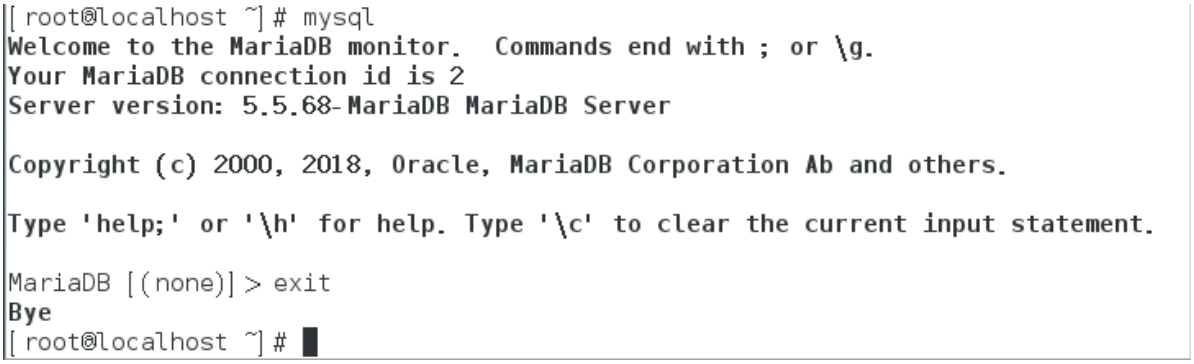
```
#检查网络，刚开机，更新下网络，结果发现学校网络用不了阿里云仓库，手机热点支持
[root@localhost ~]# ping www.baidu.com
[root@localhost ~]# dhclient
```

```
#安装apache
[root@localhost ~]# yum -y install httpd

#设置apache开机自启动
[root@localhost ~]# systemctl enable httpd.service
ln -s '/usr/lib/systemd/system/httpd.service' '/etc/systemd/system/multi-
user.target.wants/httpd.service'

#启动apache
[root@localhost ~]# systemctl start httpd.service
```

```
#修改yum文件，修改使用的python版本为2.7
[root@localhost ~]# vim /usr/bin/yum
#!/bin/python2.7

[root@localhost ~]# vim /usr/libexec/urlgrabber-ext-down
#!/bin/python2.7
```

```
# 安装 MySQL：安装 MySQL 的社区版即可，即 MariaDB
[root@localhost ~]# yum -y install mariadb mariadb-server

#开机自启 MariaDB 服务
[root@localhost ~]# systemctl enable mariadb.service
ln -s '/usr/lib/systemd/system/mariadb.service' '/etc/systemd/system/multi-
user.target.wants/mariadb.service'
```

```
# 启动 MariaDB 服务
[root@localhost ~]#  systemctl start mariadb.service
[root@localhost ~]#

#测试mysql
[root@localhost ~]# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 2
Server version: 5.5.68-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> exit
Bye
[root@localhost ~]#
```




```
# 安装 PHP 环境
[root@localhost ~]# yum -y install php php-mysql
```

准备完毕!

2.Zabbix5.0的安装

Zabbix 官方文档

```
#官方文档，根据自己的环境查看文档并搭建Zabbix
https://www.zabbix.com/download?
zabbix=5.0&os_distribution=centos&os_version=8&db=mysql&ws=apache
```

下载Zabbix库

```
#安装Zabbix库
[root@localhost ~]# rpm -Uvh
https://repo.zabbix.com/zabbix/5.0/rhel/7/x86_64/zabbix-release-5.0-
1.el7.noarch.rpm
```

```
#一些安装了，出现的问题
```

```
curl: (60) The certificate issuer's certificate has expired. Check your system
date and time.
解决:
[root@localhost ~]# yum install ntp -y
[root@localhost ~]# ntpdate -u 0.centos.pool.ntp.org    #时差问题，这里校准
[root@localhost ~]# yum install ca-certificates      #也可能是ca证书问题，这里更新一下
[root@localhost ~]# update-ca-trust extract

curl: (35) Cannot communicate securely with peer: no common encryption
algorithm(s).
解决:
#没错，curl出问题了，这里更新一下
[root@localhost ~]# yum update -y
http://pub.mirrors.aliyun.com/centos/7/os/x86_64/Packages/ca-certificates-
2020.2.41-70.0.el7_8.noarch.rpm
http://pub.mirrors.aliyun.com/centos/7/os/x86_64/Packages/p11-kit-0.23.5-
3.el7.x86_64.rpm http://pub.mirrors.aliyun.com/centos/7/os/x86_64/Packages/p11-
kit-trust-0.23.5-3.el7.x86_64.rpm
[root@localhost ~]# yum update curl -y
[root@localhost ~]# yum makecache fast

curl: (22) The requested URL returned error: 404 Not Found
#大概率是你命令出错了
```

```
#清下yum缓存
[root@localhost ~]# yum clean all

#安装Zabbix服务
[root@localhost ~]# yum install zabbix-server-mysql zabbix-agent -y

#安装Zabbix前端（我的流量啊啊啊啊！！！）
[root@localhost ~]# yum install centos-release-scl -y

#把前端开关打开，把enabled由0改为1
[root@localhost ~]# vim /etc/yum.repos.d/zabbix.repo
[zabbix-frontend]
...
enabled=1
...

#安装Zabbix前端包（我的流量啊，嘤嘤嘤）
[root@localhost ~]# yum install zabbix-web-mysql-scl zabbix-apache-conf-scl -y
```

数据库安全设置

```
[root@localhost ~]# mysql_secure_installation

Enter current password for root (enter for none): //回车即可

Set root password? [Y/n] n   //不设置root密码
 ... skipping.

Remove anonymous users? [Y/n] y    //移除匿名用户
 ... Success!

Disallow root login remotely? [Y/n] n     //允许root远程登陆
```

```
 ... skipping.

Remove test database and access to it? [Y/n] y  //移除test数据库

Reload privilege tables now? [Y/n] y    //重载权限表
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
You have new mail in /var/spool/mail/root

#进行数据库安全设置的作用：
[root@localhost ~]# mysql
MariaDB [(none)]> SHOW DATABASES; //少了test数据库
MariaDB [(none)]> SELECT user,host FROM mysql.user; //多余用户都被移除
```

此步骤旨在对数据库做一个简单的优化，没有这条命令，则只能一个个手动删除用户

创建Zabbix数据库

```
[root@localhost ~]# mysql
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
3 rows in set (0.01 sec)

MariaDB [(none)]> select current_user();
+----------------+
| current_user() |
+----------------+
| root@localhost |
+----------------+
1 row in set (0.00 sec)

MariaDB [(none)]> create database zabbix character set utf8 collate utf8_bin;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> create user zabbix@localhost identified by 'qiye';
Query OK, 0 rows affected (0.01 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]>  SHOW DATABASES;
+--------------------+
```

```
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| zabbix             |
+--------------------+
4 rows in set (0.00 sec)

MariaDB [(none)]>  USE zabbix;
Database changed
MariaDB [zabbix]>  SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| zabbix             |
+--------------------+
4 rows in set (0.00 sec)

MariaDB [zabbix]>  SHOW TABLES;
Empty set (0.00 sec)

MariaDB [zabbix]> exit
Bye
```

导入数据库

```
#首先查询我们要的数据在哪
[root@localhost ~]# rpm -ql zabbix-server-mysql | grep sql
/usr/sbin/zabbix_server_mysql
/usr/share/doc/zabbix-server-mysql-5.0.17
/usr/share/doc/zabbix-server-mysql-5.0.17/AUTHORS
/usr/share/doc/zabbix-server-mysql-5.0.17/COPYING
/usr/share/doc/zabbix-server-mysql-5.0.17/ChangeLog
/usr/share/doc/zabbix-server-mysql-5.0.17/NEWS
/usr/share/doc/zabbix-server-mysql-5.0.17/README
/usr/share/doc/zabbix-server-mysql-5.0.17/create.sql.gz
/usr/share/doc/zabbix-server-mysql-5.0.17/double.sql

#导入初始架构和数据
[root@localhost ~]# zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz |
mysql -uzabbix -pqiye zabbix
```

- -p 处输入自己指定的密码
- zcat，不看内容解压，通过管道符传输到 zabbix 数据库，或者使用以下的方法，手动导入

```
#判断导入是否成功
[root@localhost ~]# zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz |
mysql -uzabbix -pqiye zabbix
```

```
[root@localhost ~]# mysql zabbix -e 'show tables;'
+----------------------------+
| Tables_in_zabbix           |
+----------------------------+
| acknowledges               |
| actions                    |
| alerts                     |
| application_discovery      |
| application_prototype      |
| application_template       |
| applications               |
| auditlog                   |
| auditlog_details           |
| autoreg_host               |
| conditions                 |
| config                     |
| config_autoreg_tls         |
| corr_condition             |
| corr_condition_group       |
| corr_condition_tag         |
| corr_condition_tagpair     |
| corr_condition_tagvalue    |
```

表格出现即代表导入成功

为Zabbix服务器配置数据库和php

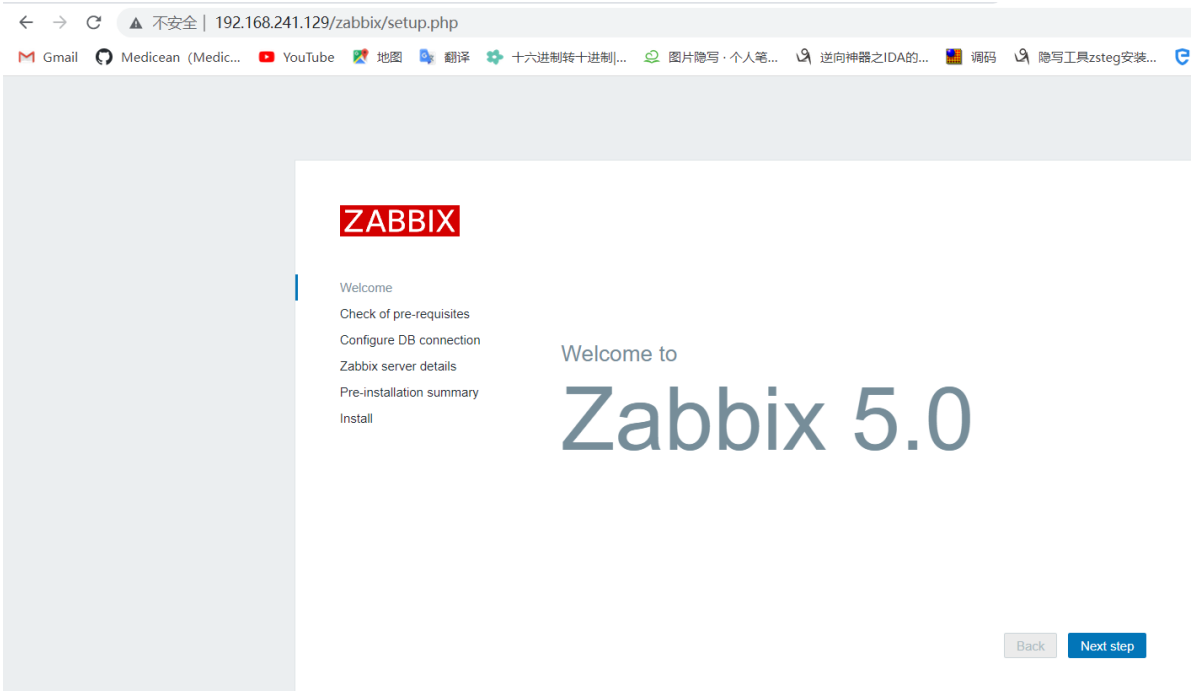
```
#数据库
[root@localhost ~]# vim  /etc/zabbix/zabbix_server.conf
DBUser=zabbix
### Option: DBPassword
#       Database password.
#       Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=qiye


#php
[root@localhost ~]# vim  /etc/opt/rh/rh-php72/php-fpm.d/zabbix.conf
php_value[max_execution_time] = 300
php_value[memory_limit] = 128M
php_value[post_max_size] = 16M
php_value[upload_max_filesize] = 2M
php_value[max_input_time] = 300
php_value[max_input_vars] = 10000
php_value[date.timezone] = Asia/Shanghai    #把前面的分号去掉，后面改为自己的时区，大陆/
城市
```

启动Zabbix服务器和代理进程

```
#重启
[root@localhost ~]# systemctl restart zabbix-server zabbix-agent httpd rh-php72-php-fpm
#自启
[root@localhost ~]# systemctl enable zabbix-server zabbix-agent httpd rh-php72-php-fpm
Created symlink from /etc/systemd/system/multi-user.target.wants/zabbix-server.service to /usr/lib/systemd/system/zabbix-server.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/zabbix-agent.service to /usr/lib/systemd/system/zabbix-agent.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/rh-php72-php-fpm.service to /usr/lib/systemd/system/rh-php72-php-fpm.service.

#检查端口
[root@localhost ~]#  netstat -lntup | grep 10051
tcp        0      0 0.0.0.0:10051           0.0.0.0:*               LISTEN
 4383/zabbix_server
tcp6       0      0 :::10051                :::*                    LISTEN
 4383/zabbix_server
[root@localhost ~]#  lsof -i :10051
```

在我的主物理机上打开zabbix界面

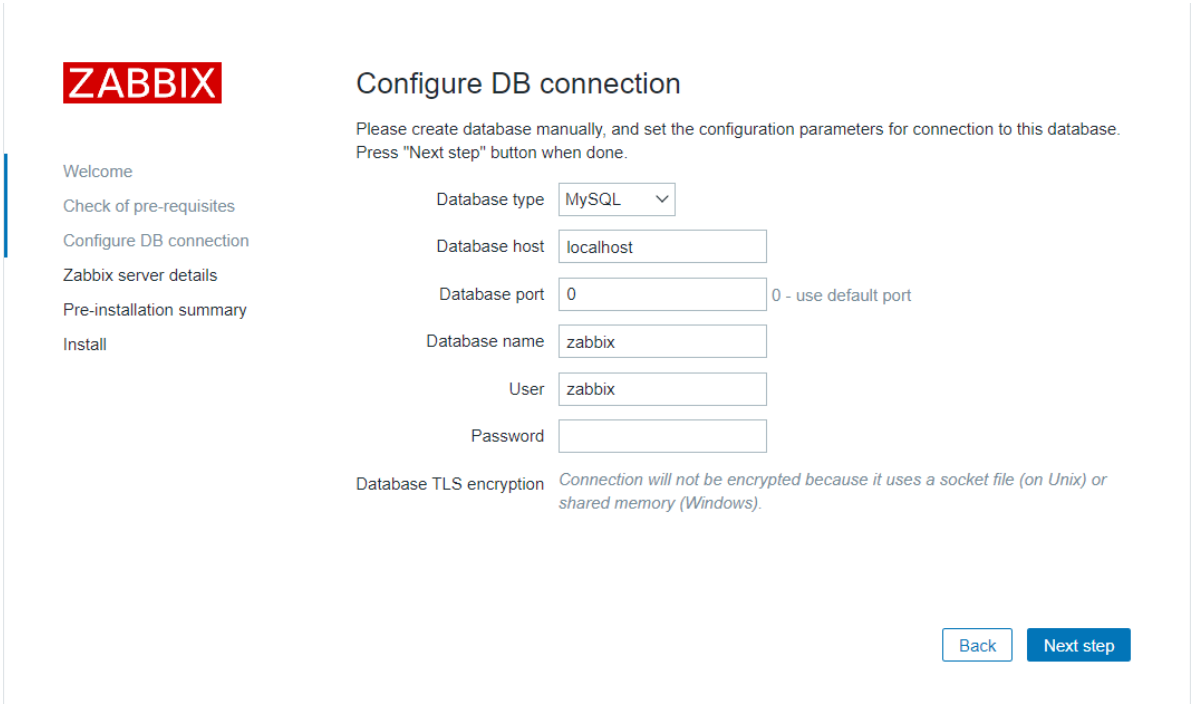
```
访问 http://zabbix服务器ip地址/zabbix/

我这里是:
http://192.168.241.129/zabbix/
```



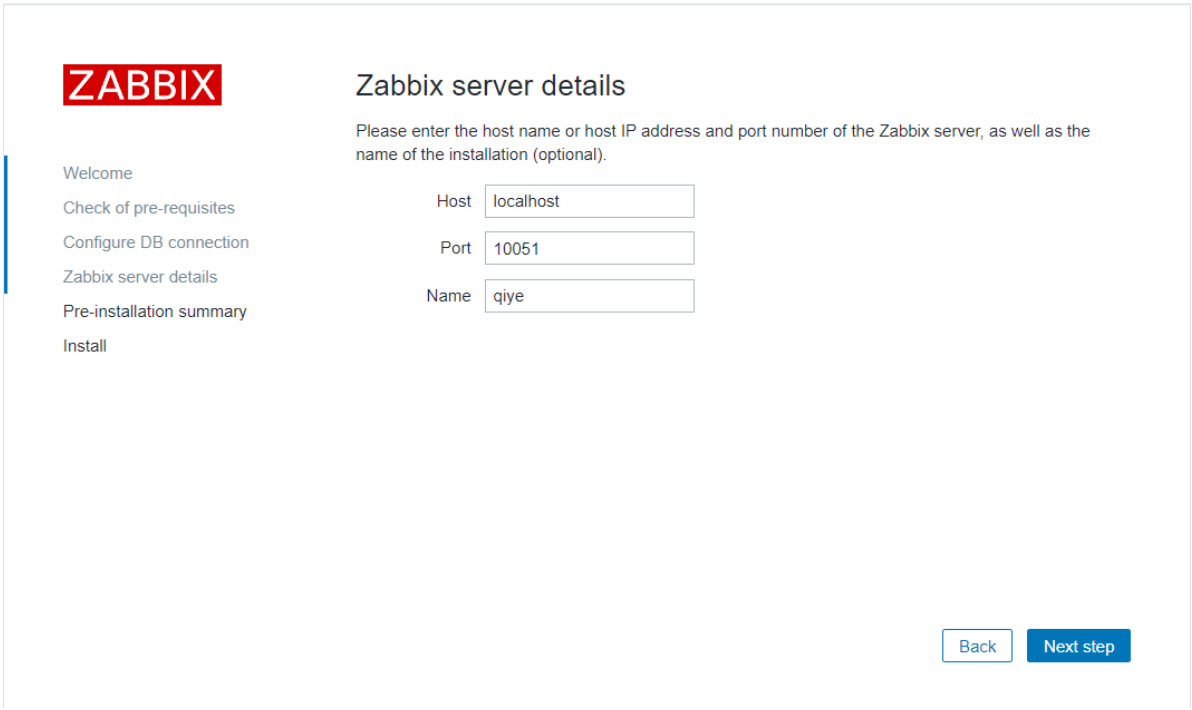
yadaze!

首先确保这个页面全是ok的情况

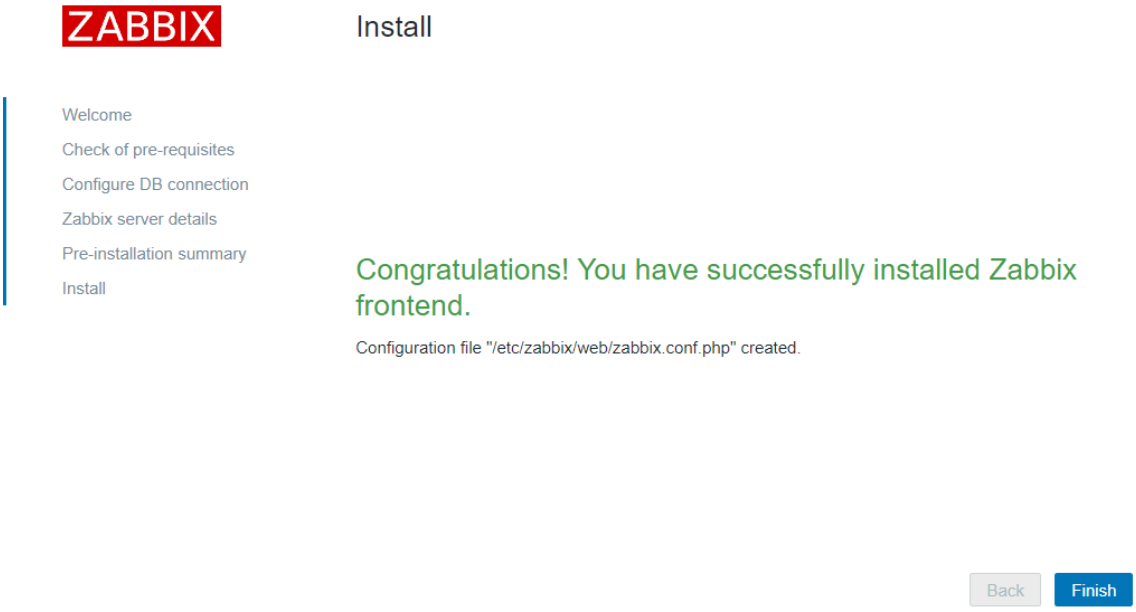
输入连接zabbix数据库密码，我的是qiye



Name的话，都行



ya*da*ze!



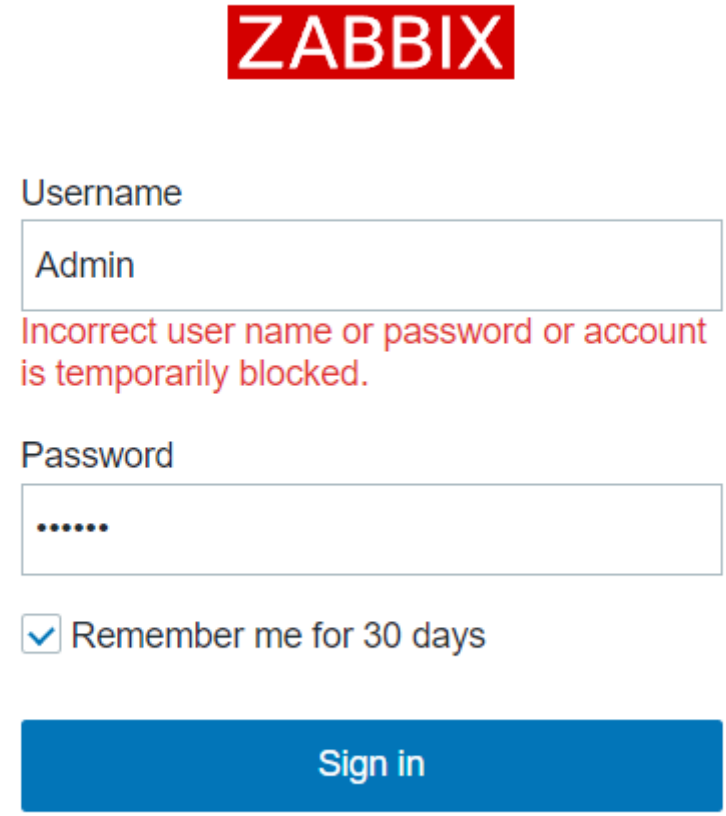
关于/etc/zabbix/web/zabbix.conf.php文件：

```
[root@localhost ~]# vim /etc/zabbix/web/zabbix.conf.php
```

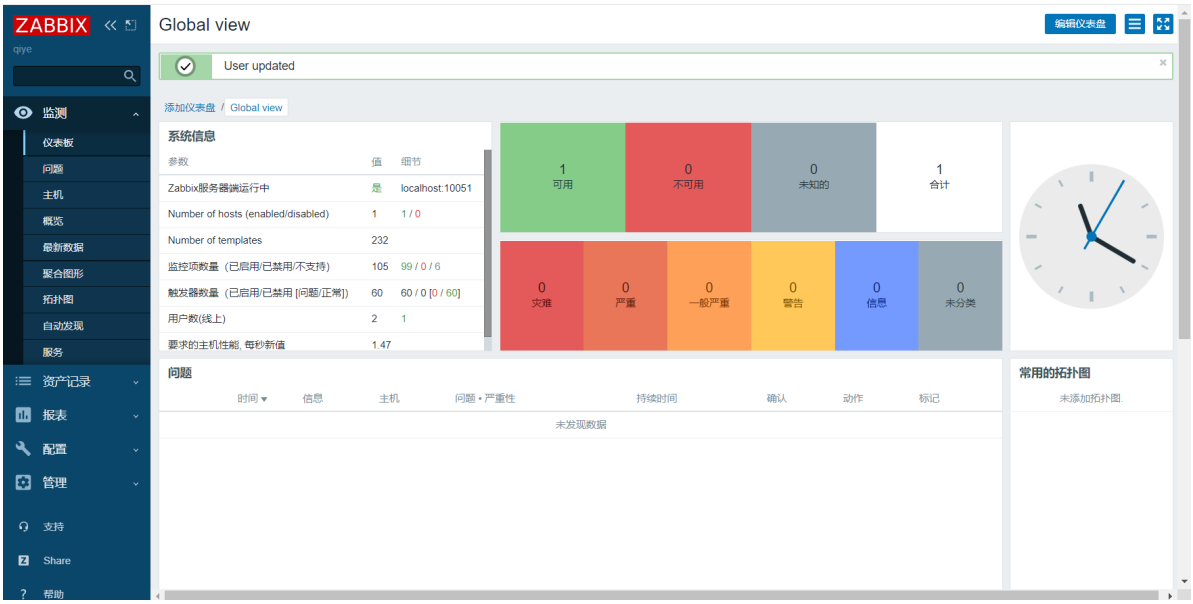
```
<?php
// Zabbix GUI configuration file.

$DB['TYPE']                             = 'MYSQL';
$DB['SERVER']                   = 'localhost';
$DB['PORT']                             = '0';
$DB['DATABASE']                 = 'zabbix';
$DB['USER']                             = 'zabbix';
$DB['PASSWORD']                 = 'qiye';

// Schema name. Used for PostgreSQL.
$DB['SCHEMA']                   = '';

// Used for TLS connection.
$DB['ENCRYPTION']               = false;
$DB['KEY_FILE']                 = '';
$DB['CERT_FILE']                = '';
$DB['CA_FILE']                  = '';
$DB['VERIFY_HOST']              = false;
$DB['CIPHER_LIST']              = '';

// Use IEEE754 compatible value range for 64-bit Numeric (float) history values.
// This option is enabled by default for new Zabbix installations.
"/etc/zabbix/web/zabbix.conf.php" 47L, 1478C                  1,1           Top
```

可以发现，这里存储着关于zabbix的账户和密码，新的渗透姿势增加了.jpg!

这里的账号默认Admin，密码默认zabbix



zabbix安装成功！！！



ya*da*ze!

3.增加Zabbix监控主机

在客户端安装zabbix-agent

前面的只是监控自己的主机，但在实际情况下，更多的是一台监控多台服务器，因为你不可能为了监控每一台服务器打开每台服务器的zabbix前端页面

```
#与前面安装步骤一样
[root@localhost ~]# rpm -Uvh
https://repo.zabbix.com/zabbix/5.0/rhel/7/x86_64/zabbix-release-5.0-
1.el7.noarch.rpm
[root@localhost ~]# yum clean all
[root@localhost ~]# yum -y install zabbix-agent
```

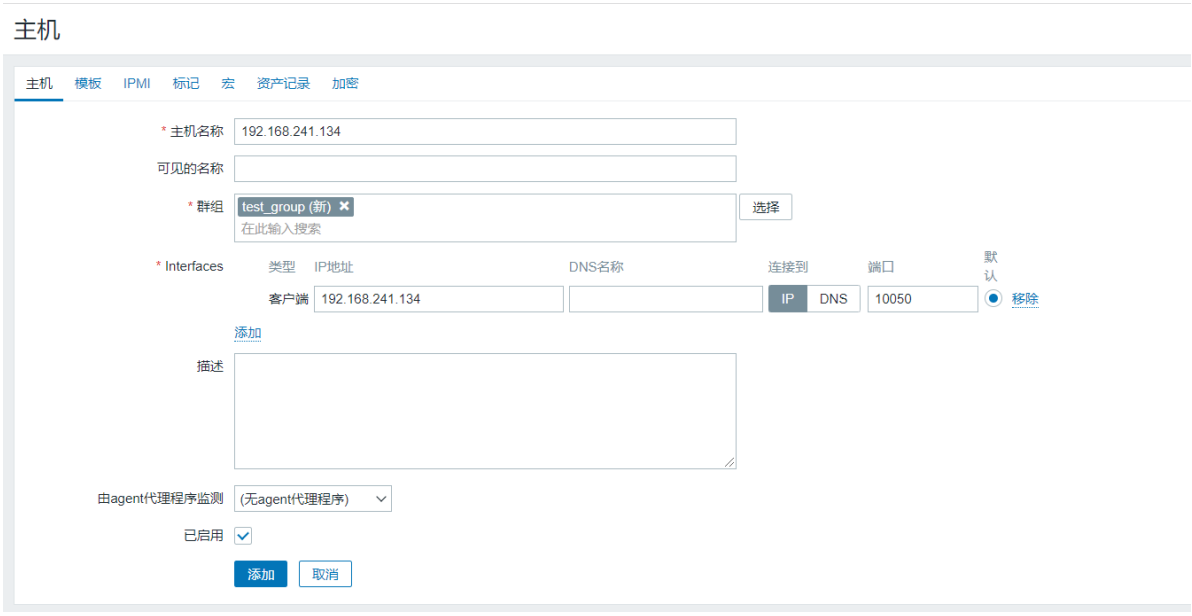
PS：**谢谢你，zabbix**

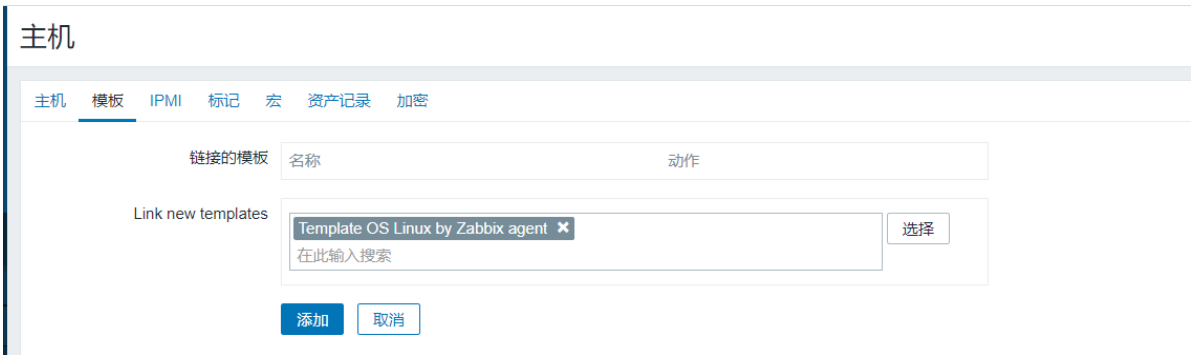
在客户端配置zabbix-agent

```
[root@localhost ~]# vim /etc/zabbix/zabbix_agentd.conf
:/^Server       #vim开头查询
Server=192.168.241.129       #主zabbix服务器ip地址
```

在客户端启动zabbix-agent

```
#重启与自启动
[root@localhost ~]# systemctl restart zabbix-agent.service
[root@localhost ~]# systemctl enable zabbix-agent.service
```

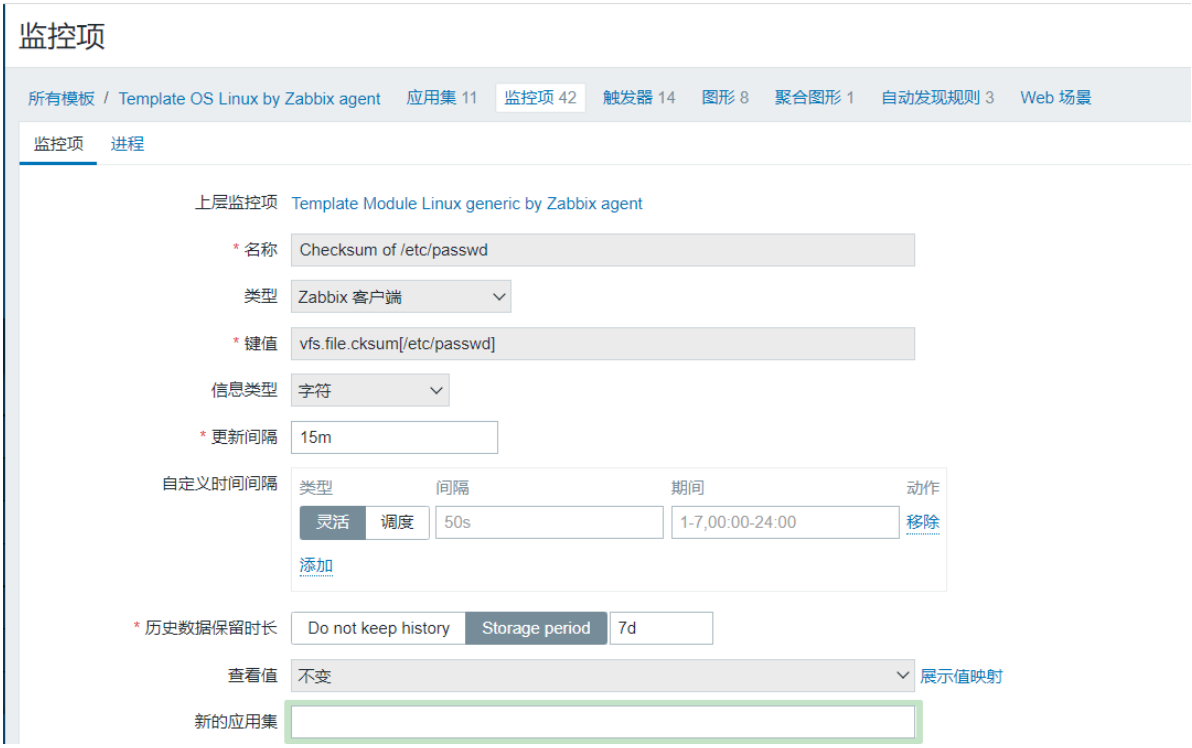




增加即可，如果不增加模板，不会有以下

4.自定义监控

模板自定义监控



可以发现，它对/etc/passwd进行监控，没错，对用户的变化进行监控，为了确保安全性

这就是为什么，平时在渗透时，提权一般不优先创建用户，因为被发现的可能性非常大，所以一般已有用户进行横向渗透。

自定义监控项

模板不包含并发连接数、TPS值（iostat命令），只使用模板远远不够，很多时候我们需要添加自定义的监控项

命令行手动取值

```
[root@localhost ~]# iostat | awk '/sda/'
sda               8.58       219.30       118.61    2116225    1144610
[root@localhost ~]# iostat | awk '/sda/{print $2}'
8.58
```

server端修改zabbix-agent配置文件

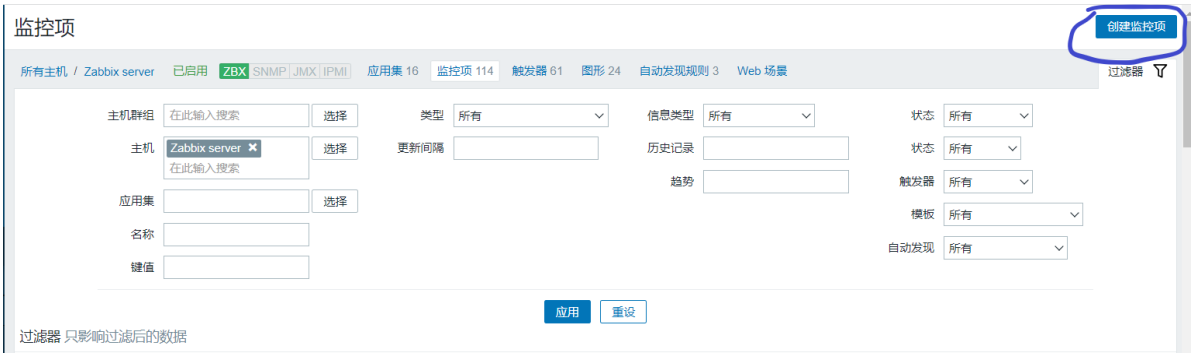
```
#修改 UserParameter=
[root@localhost ~]# vim /etc/zabbix/zabbix_agentd.conf
UserParameter=sda_tps,iostat|awk '/sda/{print $2}'

[root@localhost ~]# systemctl restart zabbix-agent.service
```

server端zabbix-server测试监控项取值

```
[root@localhost ~]# yum -y install zabbix-get.x86_64 &>/dev/null

# 若返回值为 0，代表上条命令成功执行
[root@localhost ~]# echo $?
0
[root@localhost ~]# zabbix_get -s 127.0.0.1 -k vfs.file.cksum[/etc/passwd]
1696492884
--s 后跟 agent 的 IP 地址
--k 后跟 key 值

[root@localhost ~]# zabbix_get -s 127.0.0.1 -k sda_tps
11.79
# 可见自定义 key 已成功导入
```

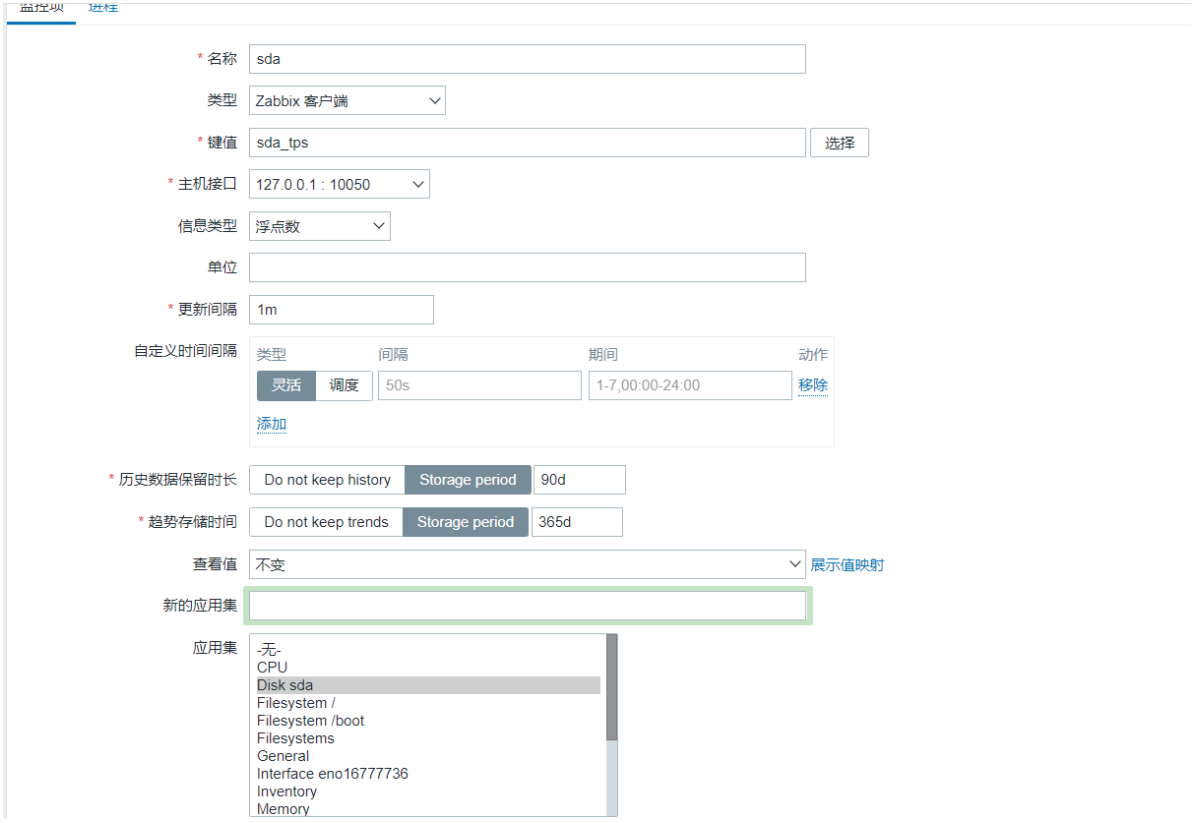
在web界面增加自定义监控项

来到对应主机处，点击**监控项**，主机选择zabbix主服务器，右上角创建监控项

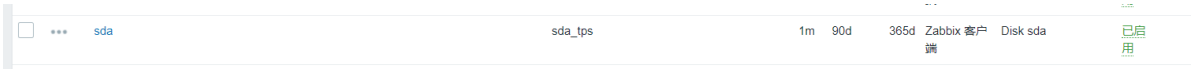


名称可用中文，键位必须用英文

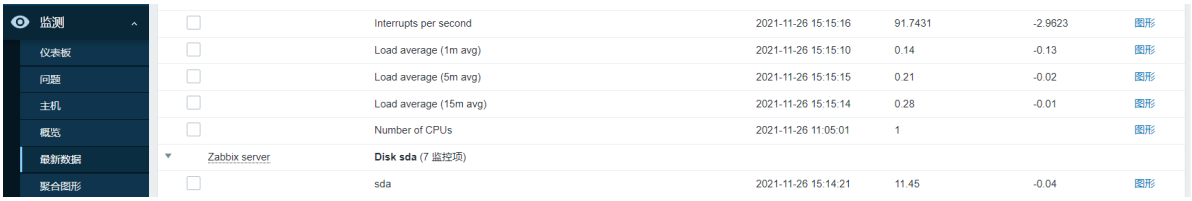
由于 tps 值存在小数，信息类型处，需要选择单位为浮点数



可以发现它进了监控



在监控-》最新数据中，可以找到他的身影



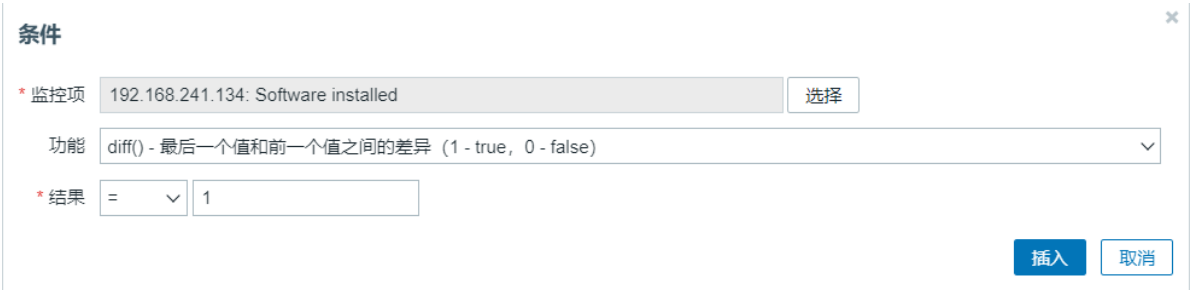
自定义触发器

我这里以system.sw.packages为测试，为了方便听到警报声，只要安装一个软件则报警

监控项：

触发器：

直接点右边添加，选择表达式



只要有软件安装，这个值就会变

在192.168.241.134的主机上随便装点东西：

```
#这里装装ruby语言
[root@localhost ~]# yum install -y ruby
```

很快啊！

如何定义恢复触发器？

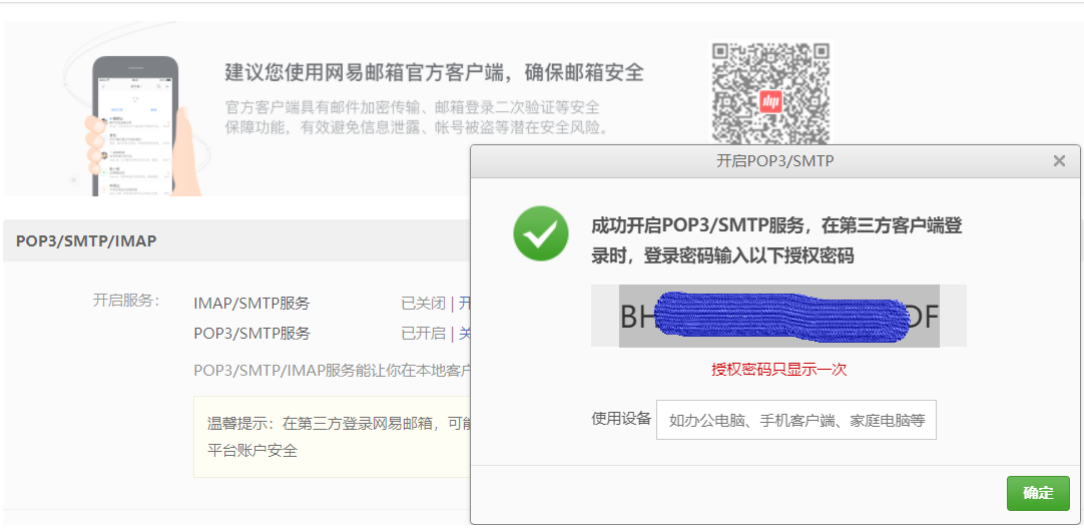
进入对应触发器编辑页面 -> 恢复表达式 -> 输入恢复表达式 -> 更新

把软件卸了就行

5.邮件报警

环境：

1.进入 **设置 -> POP3/SMTP/IMAP**->开启POP3/SMTP服务，获取163邮箱授权码



假如你是163邮箱的使用者，则下面会用到

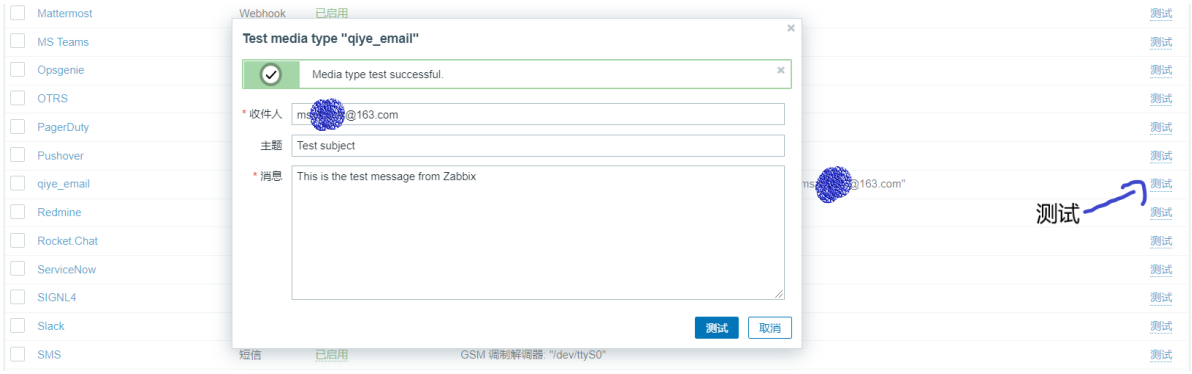
网易163免费邮箱相关服务器信息：

服务器名称	服务器地址	SSL协议端口号	非SSL协议端口号
IMAP	imap.163.com	993	143
SMTP	smtp.163.com	465/994	25
POP3	pop.163.com	995	110

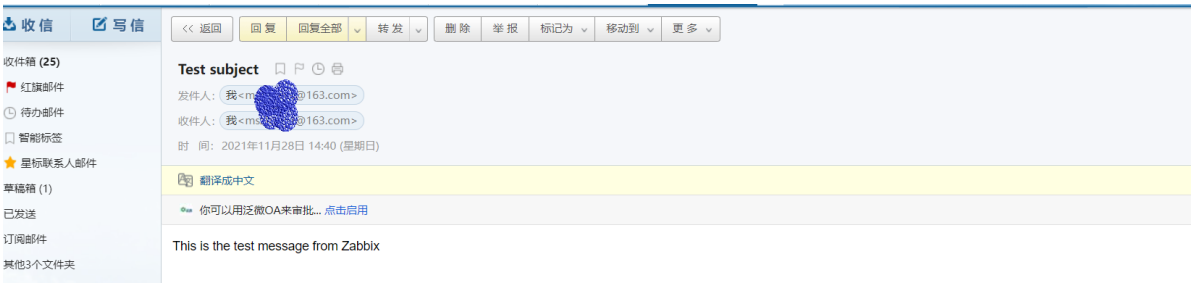
2.进入 zabbix**管理 -> 报警媒介类型 ->** 右上角**创建媒体类型**

可以发现qiye_email

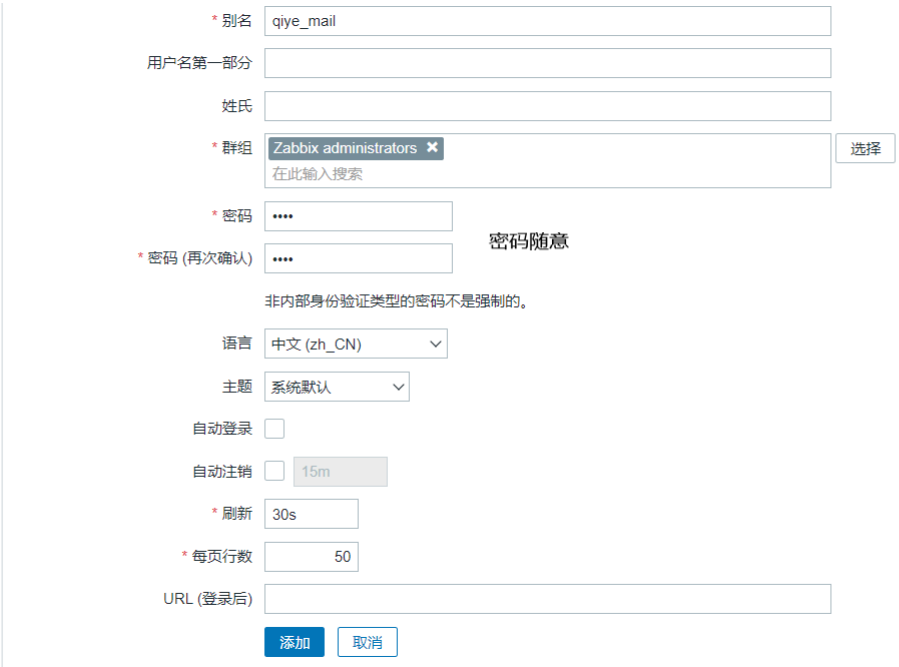
我们测试一下



正常收到!

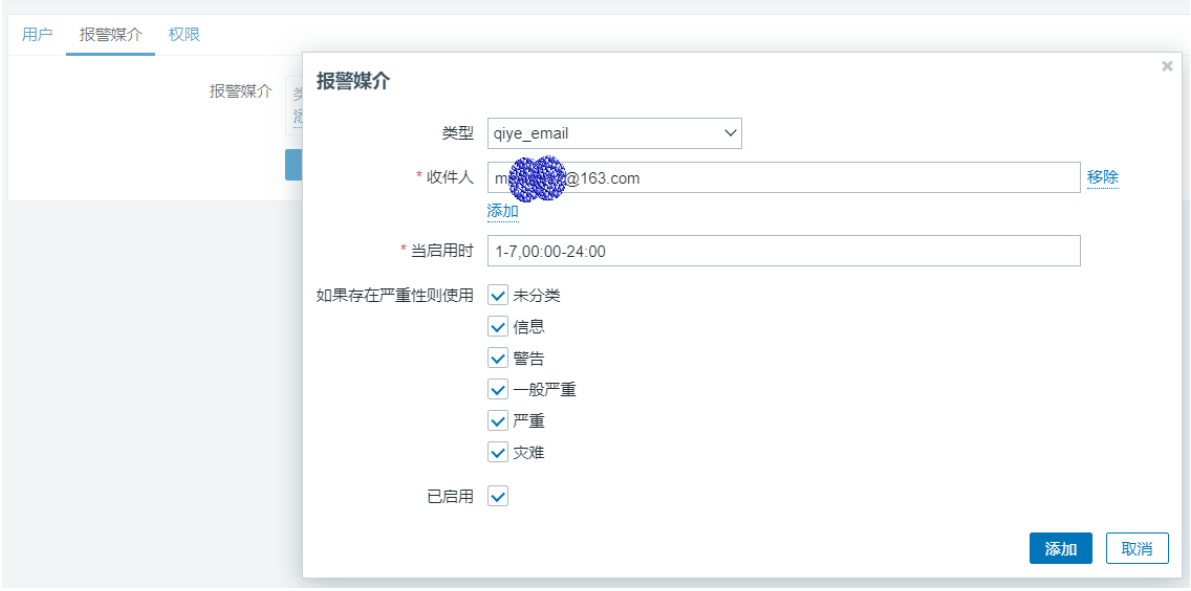


3.进入 **管理 -> 用户 ->** 右上角**创建用户**

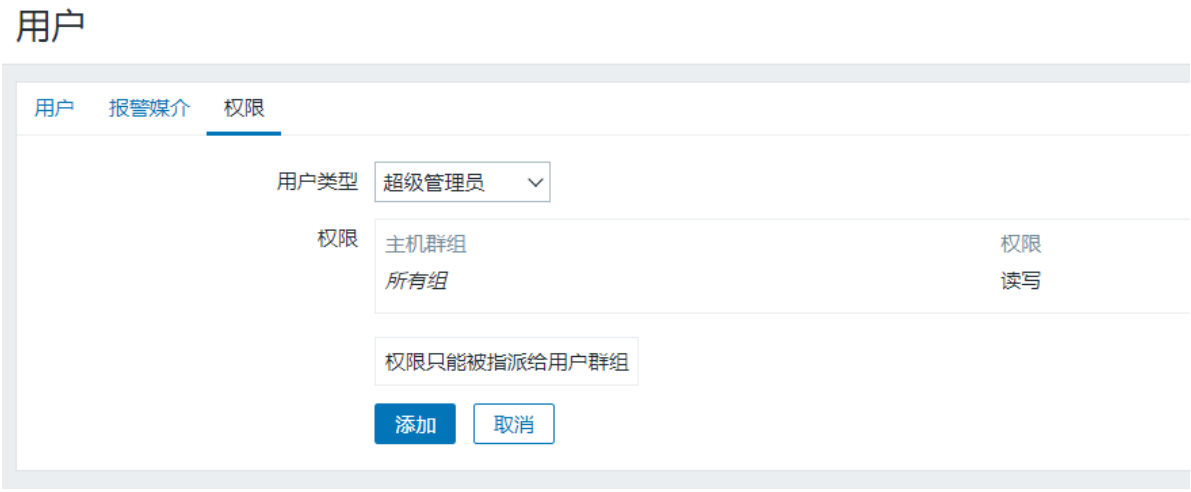


设置报警媒介

用户



然后是权限



添加即可!

4.进入 **配置 -> 动作 ->** 右上角**创建动作**

设置多个动作条件，并选择计算方式为 或

然后是操作界面，自己根据需求设置

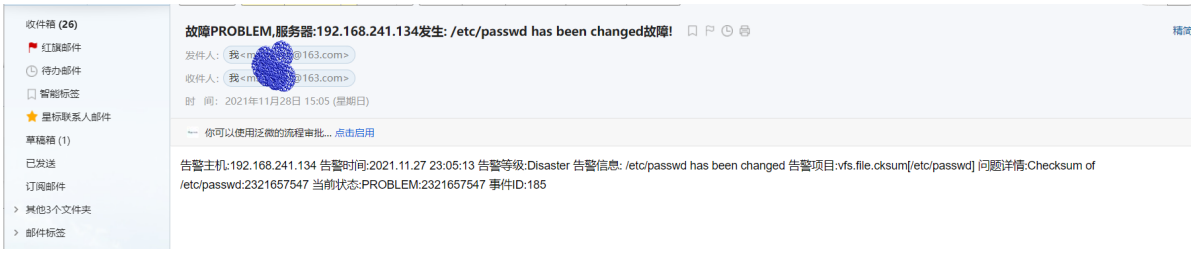
配置操作

```
主题:
故障{TRIGGER.STATUS},服务器:{HOSTNAME1}发生: {TRIGGER.NAME}故障!

消息:
告警主机:{HOSTNAME1}
告警时间:{EVENT.DATE} {EVENT.TIME}
告警等级:{TRIGGER.SEVERITY}
告警信息: {TRIGGER.NAME}
告警项目:{TRIGGER.KEY1}
问题详情:{ITEM.NAME}:{ITEM.VALUE}
当前状态:{TRIGGER.STATUS}:{ITEM.VALUE1}
事件ID:{EVENT.ID}
```

更新即可

报警

```
# 192.168.241.134端新增用户
[root@localhost ~]# useradd test1
[root@localhost ~]# echo "123" | passwd --stdin test1
更改用户 test1 的密码 。
passwd: 所有的身份验证令牌已经成功更新。
[root@localhost ~]# systemctl restart zabbix-server.service
```



yadaze!