一、自动发现

P1 部署被监控端主机 web2

部署被控端主机 Web2

[root@zabbixserver ~]# scp -r lnmp_soft/zabbix-3.4.4 root@192.168.2.200:/root/ # 将 zabbix 解压源码包发送到 web2 主机的 root 目录下

[root@web2 ~]# yum -y install gcc pcre-devel autoconf #安装源码包安装的相关依赖包

[root@web2 ~]# cd zabbix-3.4.4/

[root@web2 zabbix-3.4.4]# ./configure --enable-agent

[root@web2 zabbix-3.4.4]# make install

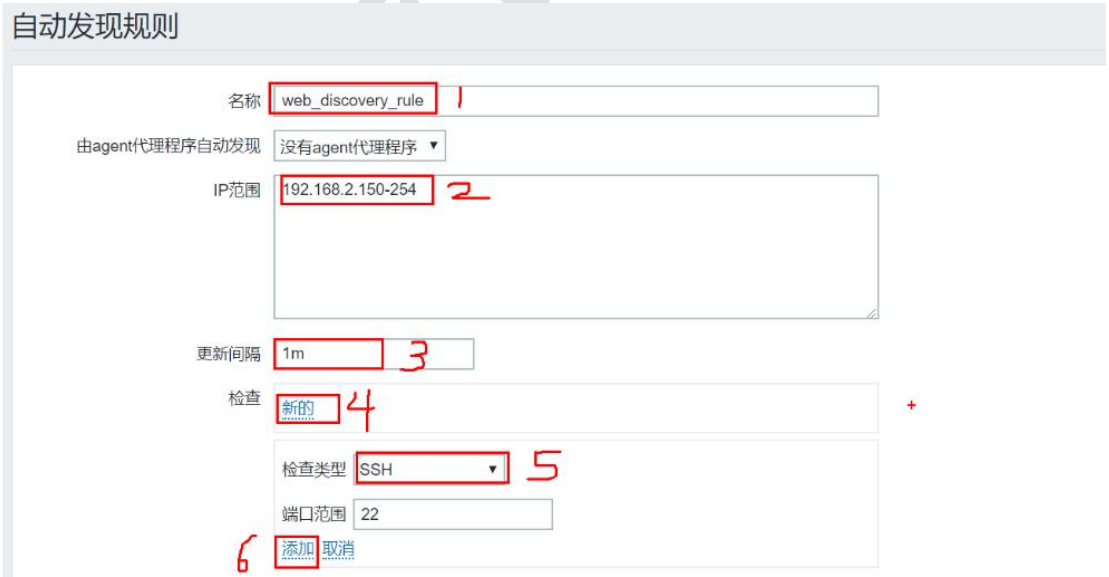
[root@web2 zabbix-3.4.4]# useradd zabbix #创建 zabbix 用户，

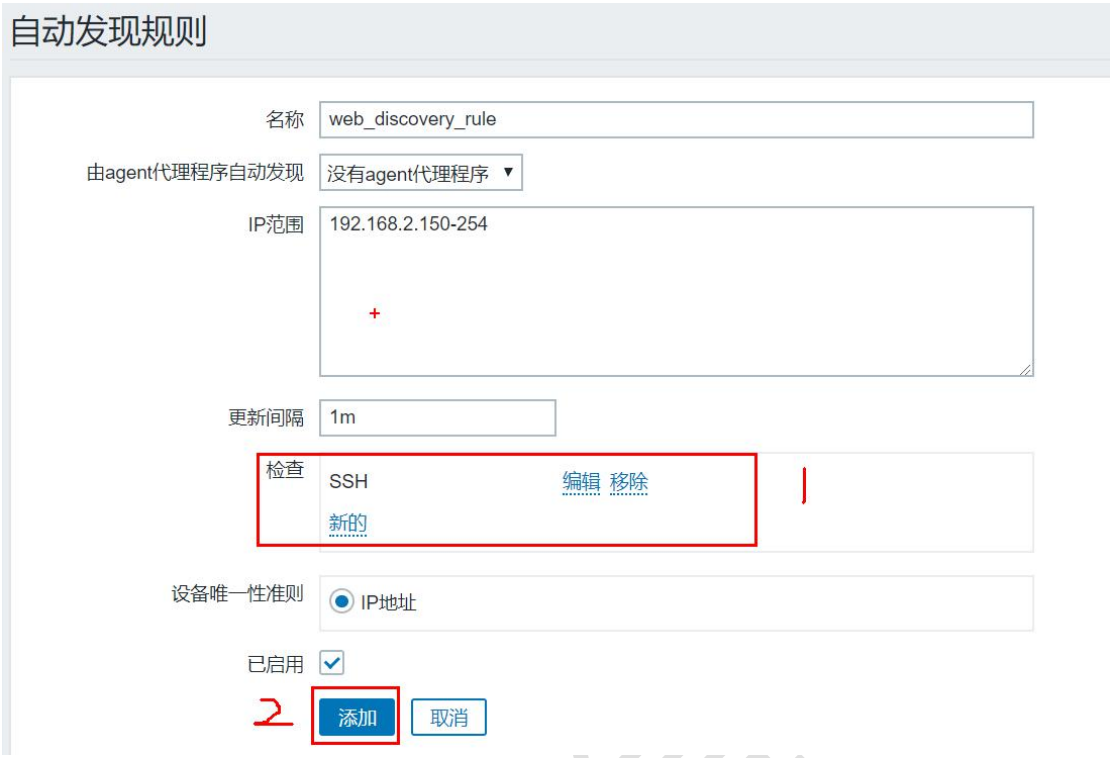
[root@web2 zabbix-3.4.4]# zabbix_agentd #启动客户端服务

[root@web2 zabbix-3.4.4]# ss -antlp | grep 10050

选择“配置”，选择“自动发现”，选择“创建自动发现规则”

创建自动发现规则

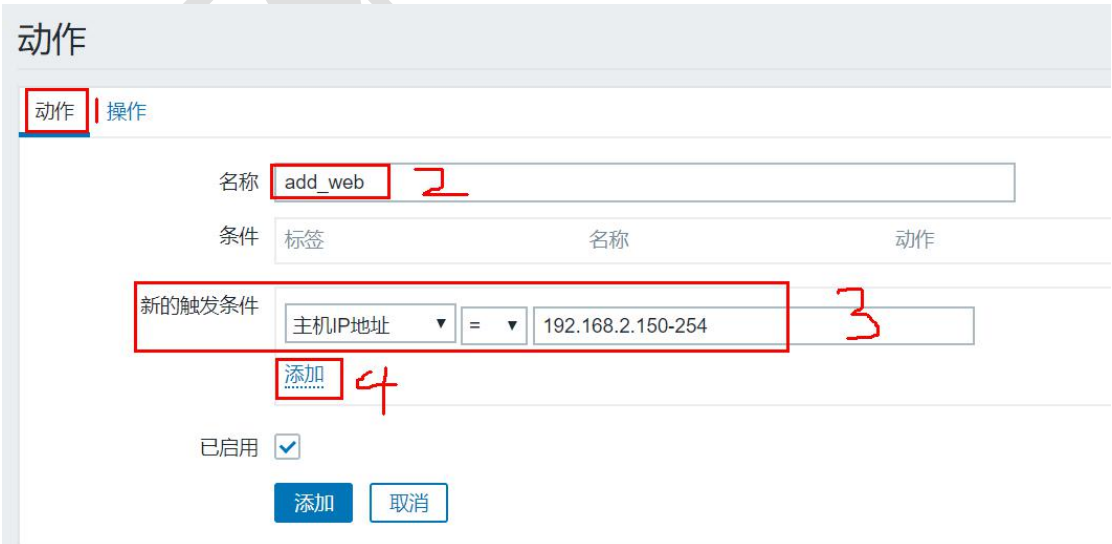


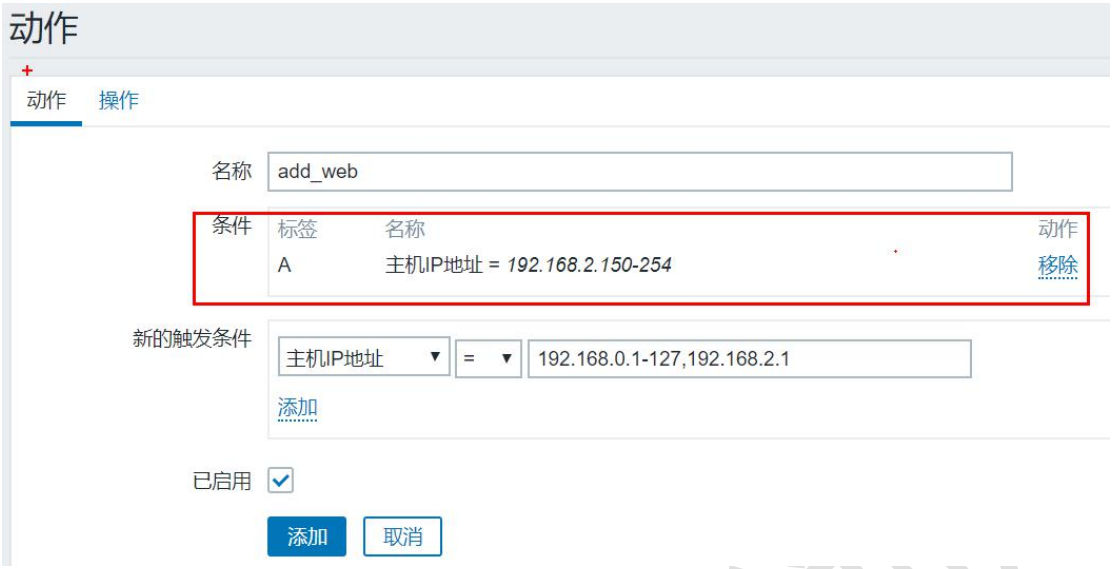


创建动作

选择“配置”，选择“动作”，事件源选择“自动发现”，选择“创建动作”

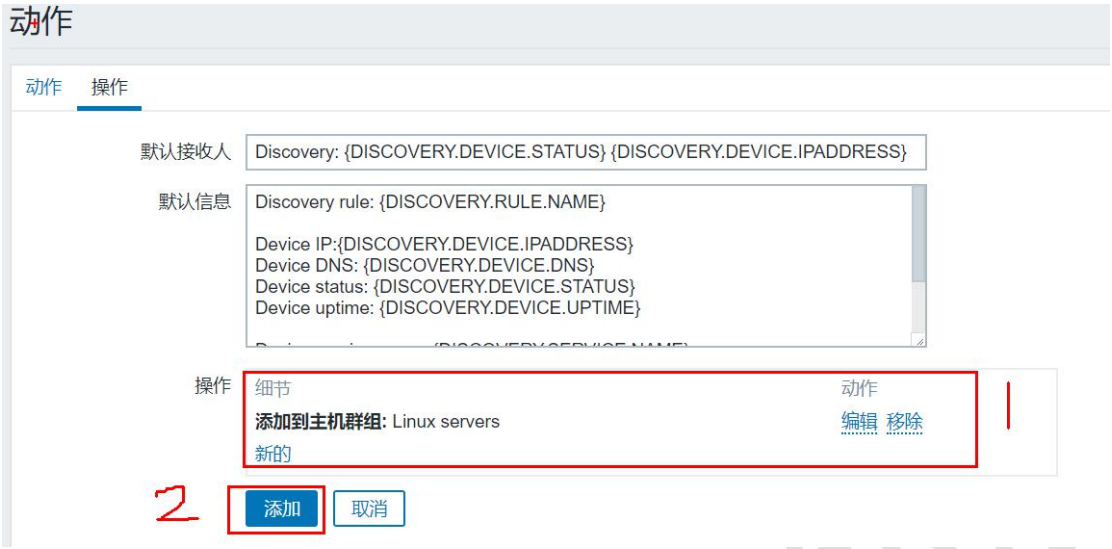
添加动作“名称”，选择“新的触发条件” (进一步过滤要发现的主机)，选择“添加”

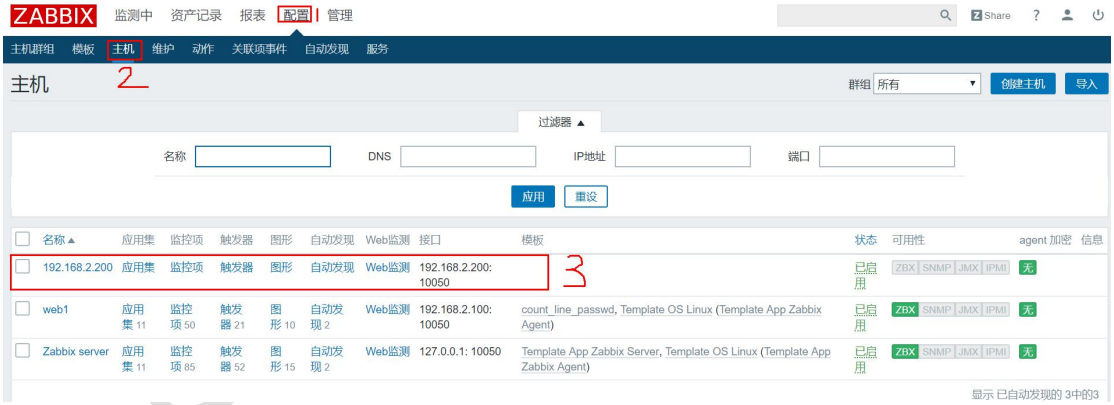



动作
动作
操作
名称
add_web
条件
标签
名称
动作
A
主机IP地址 = 192.168.2.150-254
移除
新的触发条件
主机IP地址
=
192.168.0.1-127,192.168.2.1
添加
已启用
添加
取消


动作
动作
操作
1
默认接收人
Discovery: {DISCOVERY.DEVICE.STATUS} {DISCOVERY.DEVICE.IPADDRESS}
默认信息
Discovery rule: {DISCOVERY.RULE.NAME}
Device IP:{DISCOVERY.DEVICE.IPADDRESS}
Device DNS: {DISCOVERY.DEVICE.DNS}
Device status: {DISCOVERY.DEVICE.STATUS}
Device uptime: {DISCOVERY.DEVICE.UPTIME}
操作
细节
动作
新的
2


动作
动作
操作
默认接收人
Discovery: {DISCOVERY.DEVICE.STATUS} {DISCOVERY.DEVICE.IPADDRESS}
默认信息
Device status: {DISCOVERY.DEVICE.STATUS}
Device uptime: {DISCOVERY.DEVICE.UPTIME}
Device service name: {DISCOVERY.SERVICE.NAME}
Device service port: {DISCOVERY.SERVICE.PORT}
Device service status: {DISCOVERY.SERVICE.STATUS}
Device service uptime: {DISCOVERY.SERVICE.UPTIME}
操作
细节
动作
操作细节
操作类型
添加到主机群组
1
主机群组
Linux servers
3
在此输入搜索
2
选择
4
添加
取消
添加
取消





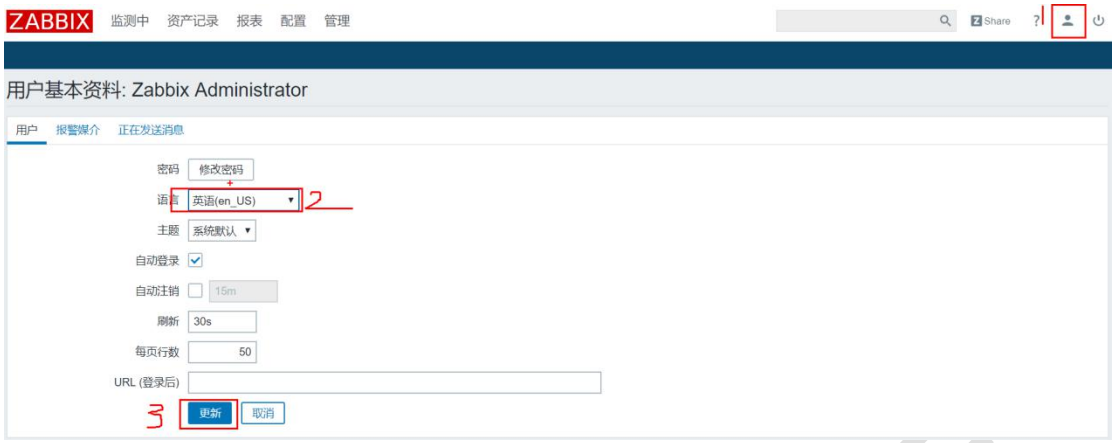
二、监控触发器

P1 触发器

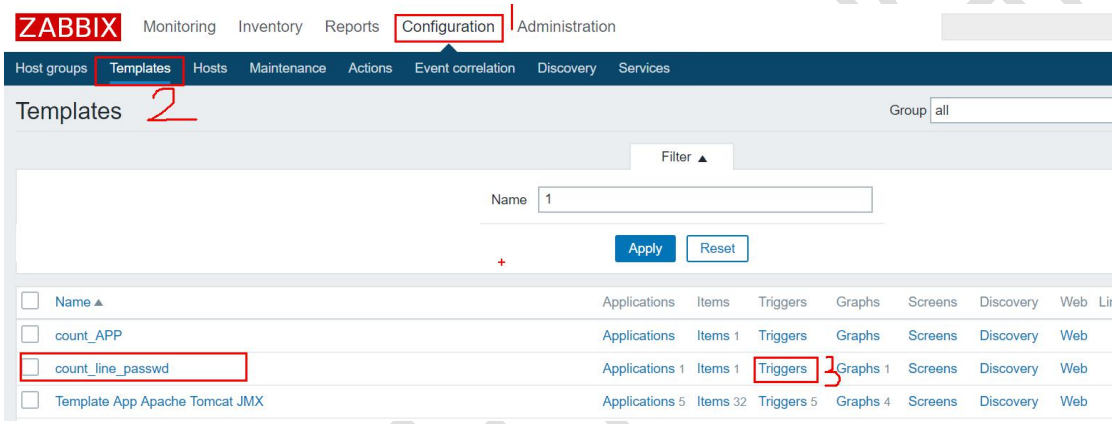
创建触发器（推荐使用英文）

1）通过 Confifiguration —> Templates

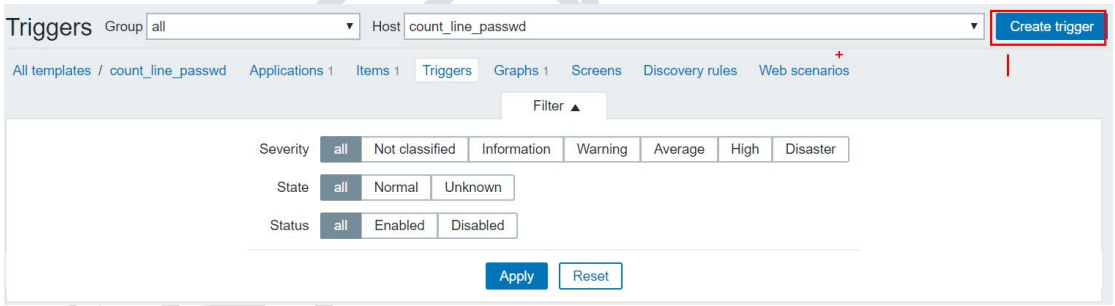
2）选择模板点击后面的 Triggers —> Create trigger



3）选择“Confifiguration”，选择"Templates"，选择对应模板后的“Triggers”



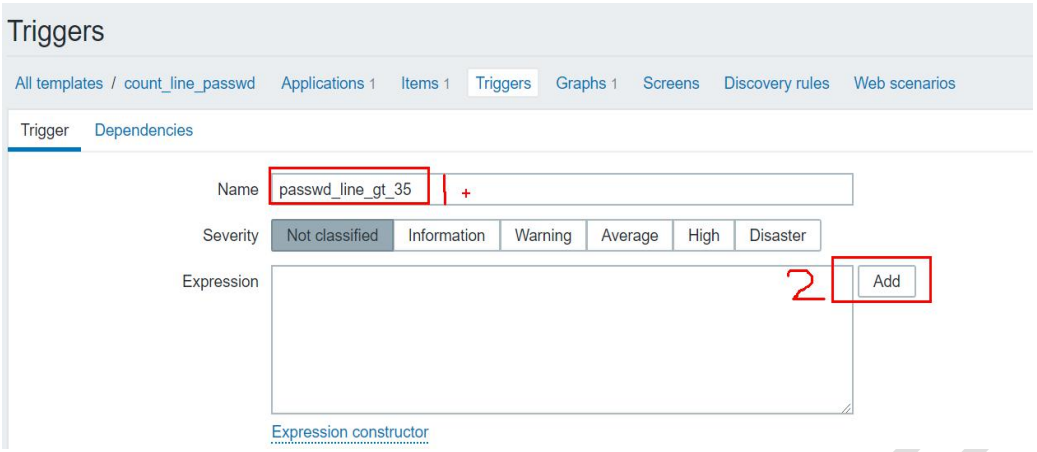
4）选择 “Create trigger”，创建触发器



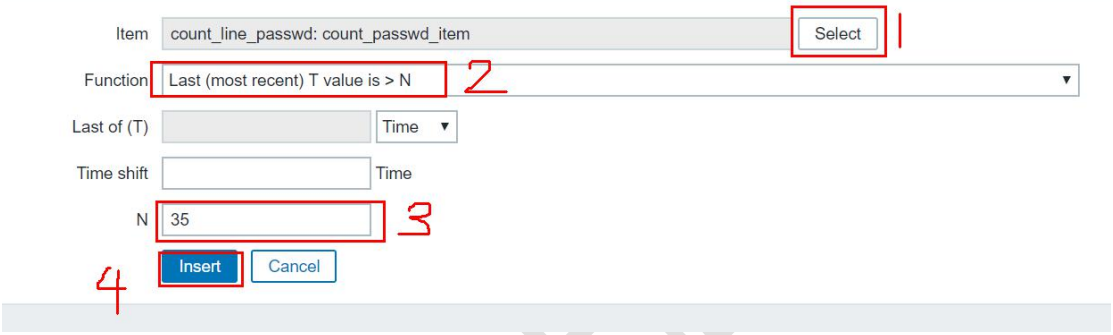
配置触发器

1）设置触发器名称，点击 add 添加表达式

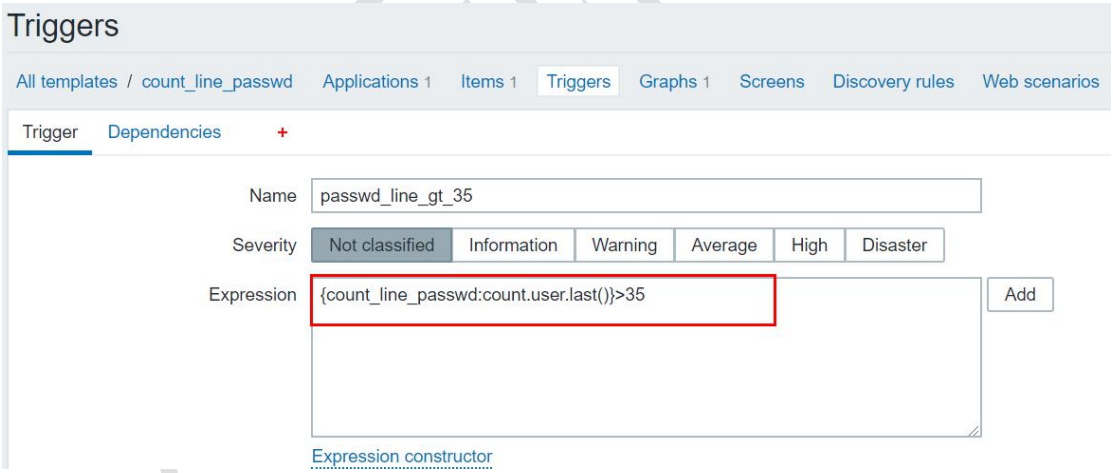
2）填写表达式（监控项为账户数量，最近账户数量大于 35）



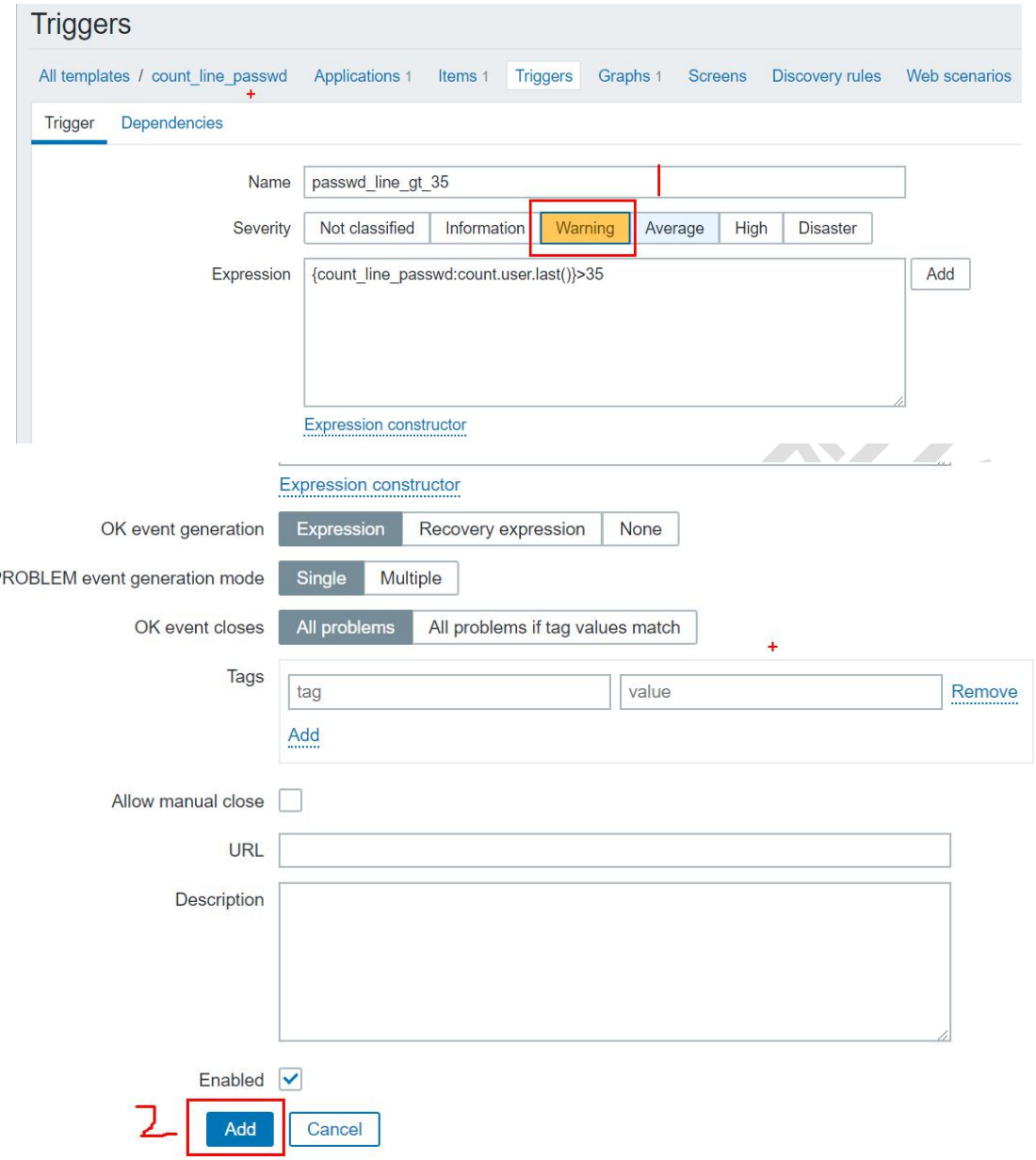
3）本案例触发器定义



针对模板【count_line_passwd】中的监控项【count_passwd_item】设置触发条件；
使用函数判断：当最新的监控数据大于 N(N=35)时，被触发；



6）选择触发器报警级别，Add 创建该触发器



######报警级别，从上到下，越来越严重

【Not classified】 #灰色，未定义

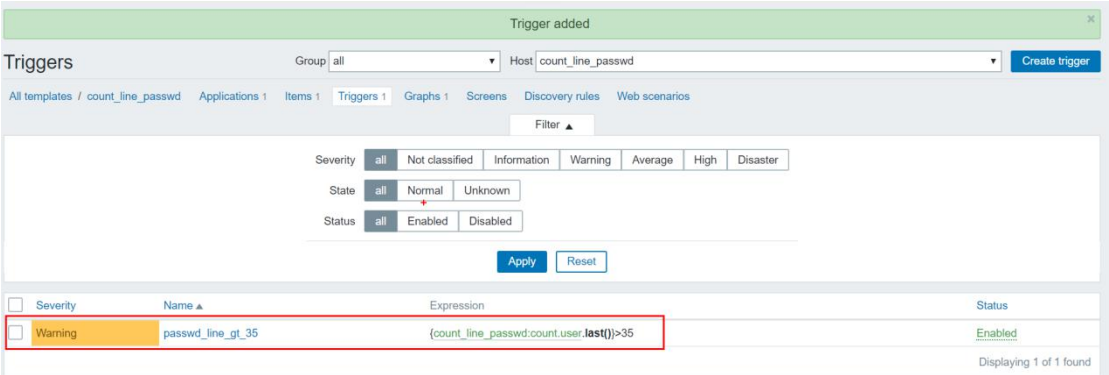
【Information】 #蓝色，一般信息提示

【Warning】 #橘色，警告信息

【Average】 #橘色加深，进一步警告信息

【High】 #橘红色，高威警告

【Disaster】 #深红色，灾难警告

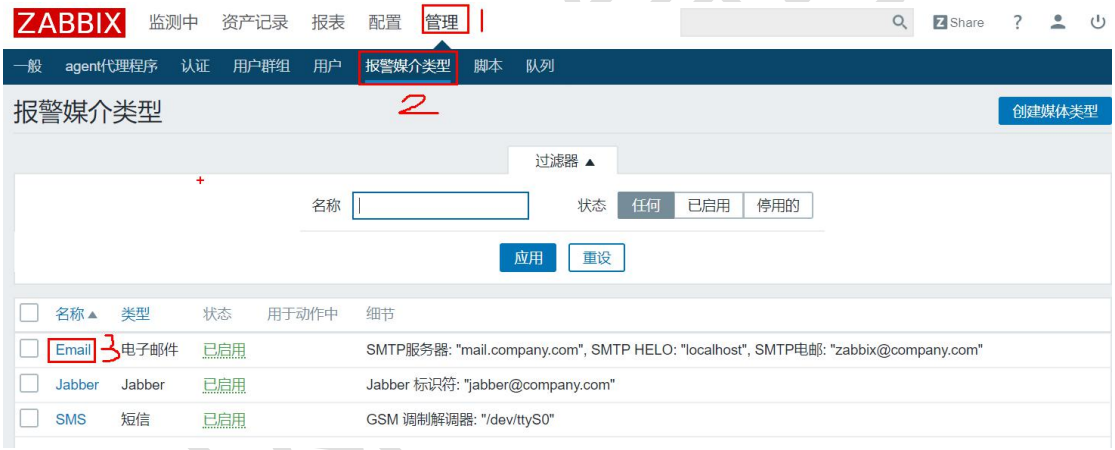


二、报警邮件

P1 设置邮件

创建 Media，设置邮件服务器

1）选择”管理“，选择”报警媒介类型“，点击”Email“电子邮件



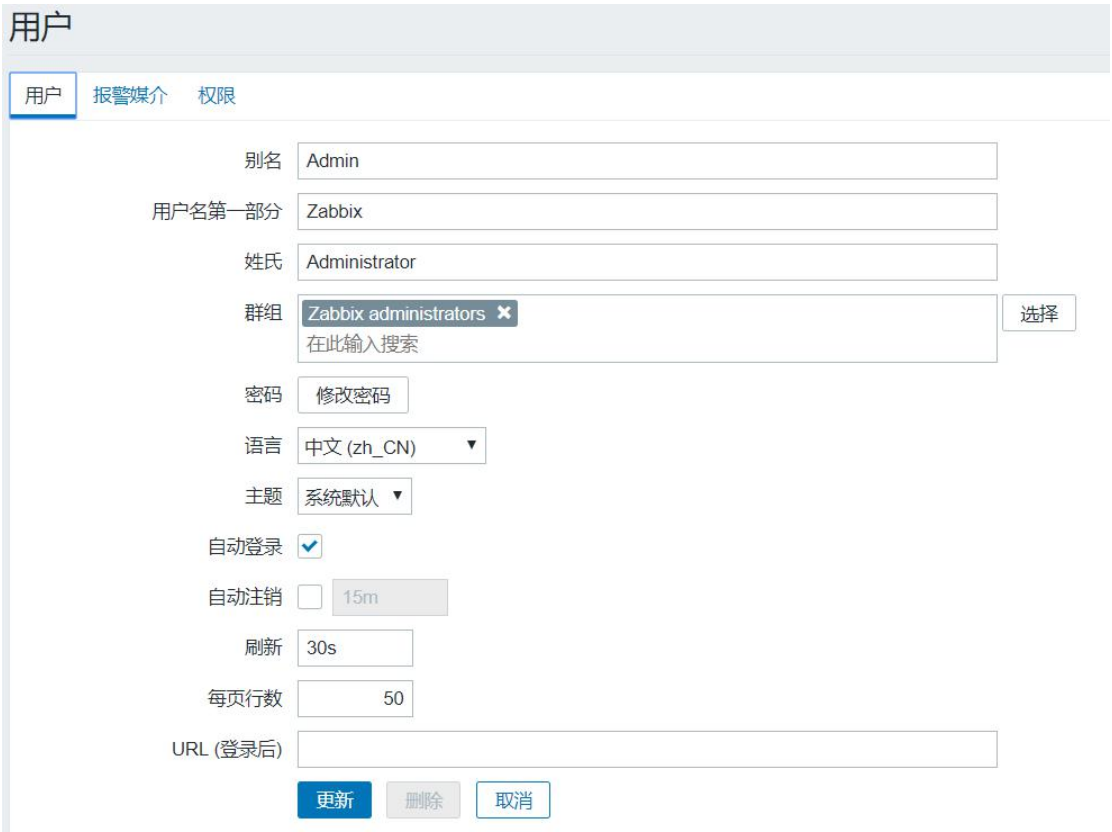
设置报警媒介

3）为账户添加 Media（收件人）

在 Adminstration —> Users 中找到选择 admin 账户

4）给管理员”Admin“ 设置报警

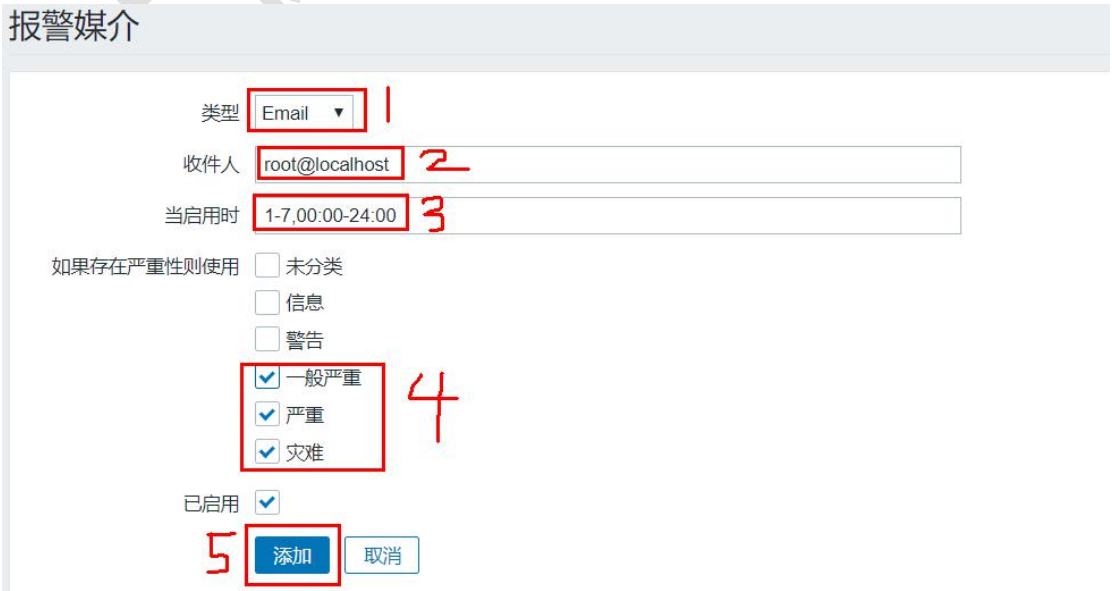
选择”管理“，选择”用户“，点击”Admin“



5）给用户添加报警方式，”选择报警媒介“，选择 ”添加“

设置报警方式

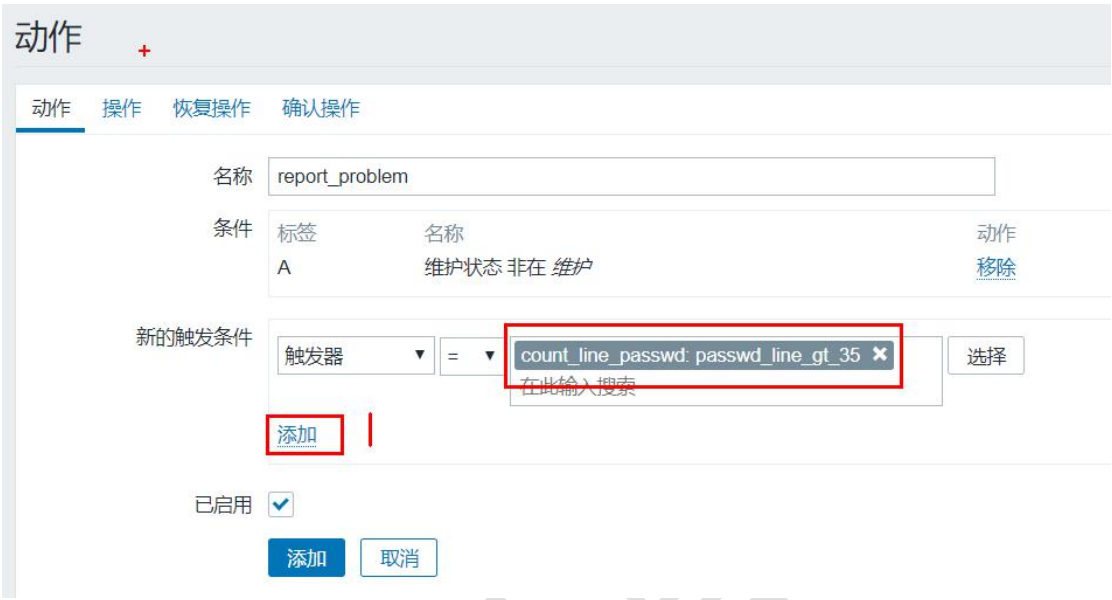
选择更新

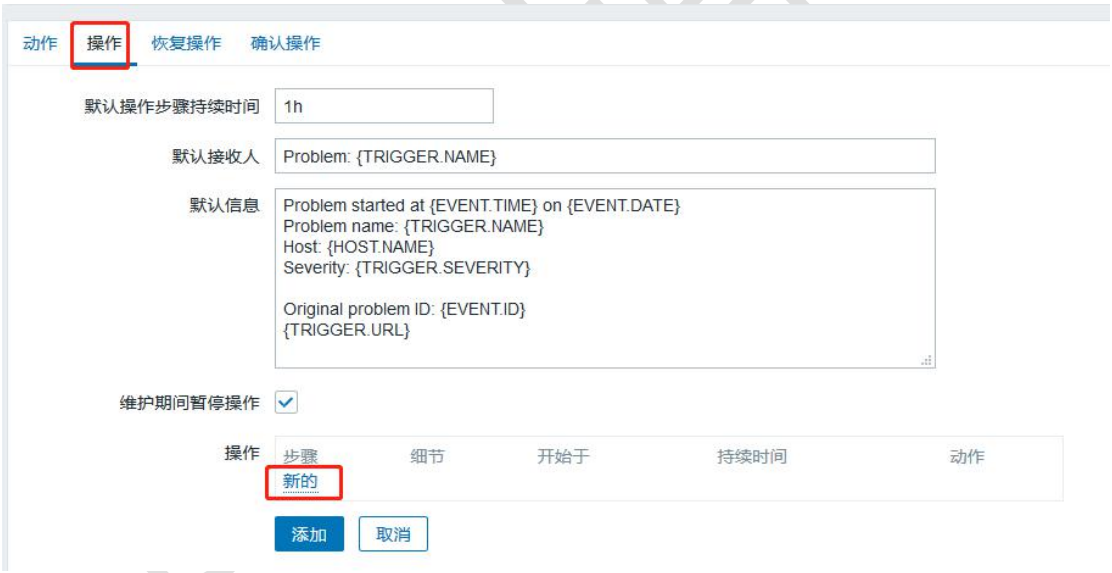


创建动作

选择 ”配置“，选择”动作“，选择"触发器"，根据触发器来”创建动作“

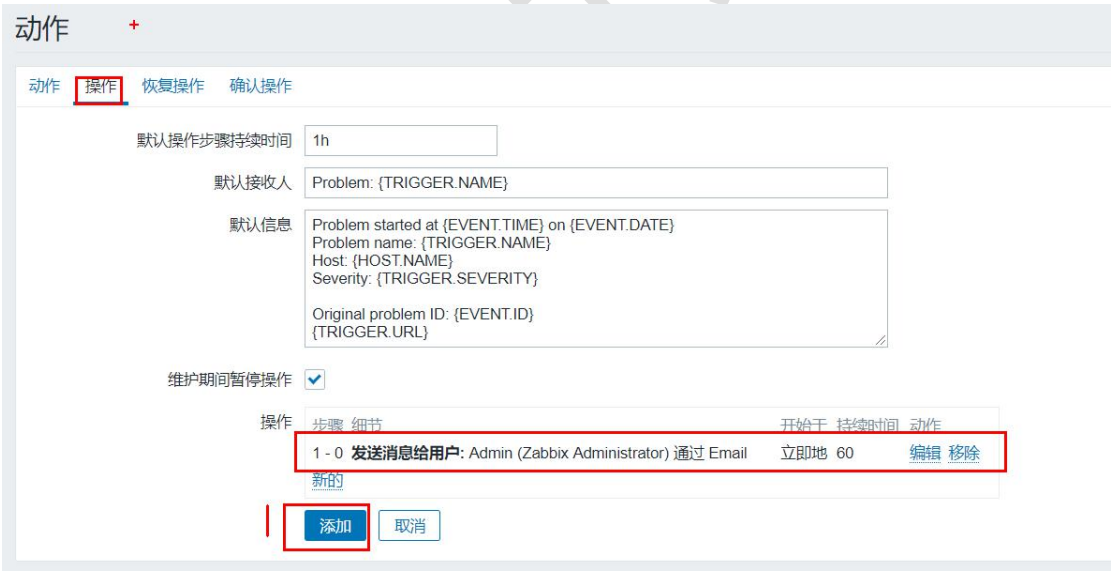
2)配置 Action（填写名称） 配置导致动作的触发条件（账户大于 35）





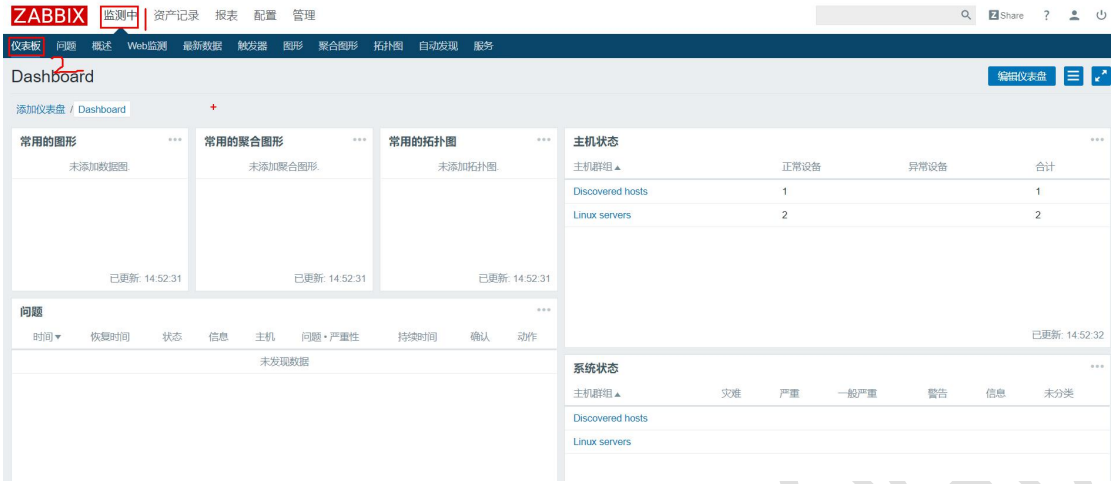
无限次数发送邮件，60 秒 1 次，发送给 Admin 用户


维护期间暂停操作
操作
步骤
细节
开始于
持续时间
动作
操作细节
步骤 1 - 0 (0 - 无穷大)
步骤持续时间 60 (0 - 使用默认)
操作类型 发送消息
发送到用户群组
用户群组
动作
添加
发送到用户
用户
动作
Admin (Zabbix Administrator)
移除
添加
仅送到 Email
默认信息
条件
标签
名称
动作
新的
添加 取消
添加
取消


动作
动作
操作
恢复操作
确认操作
默认操作步骤持续时间 1h
默认接收人 Problem: {TRIGGER.NAME}
默认信息
Problem started at {EVENT.TIME} on {EVENT.DATE}
Problem name: {TRIGGER.NAME}
Host: {HOST.NAME}
Severity: {TRIGGER.SEVERITY}
Original problem ID: {EVENT.ID}
{TRIGGER.URL}
维护期间暂停操作
操作
步骤 细节
开始于 持续时间 动作
1 - 0 发送消息给用户: Admin (Zabbix Administrator) 通过 Email
立即地 60
编辑 移除
新的
添加
取消


动作已添加
动作
事件源 触发器
创建动作
过滤器
名称
状态 任何 已启用 停用的
应用
重设
名称
条件
操作
状态
Report problems to Zabbix administrators
发送消息给用户群组: Zabbix administrators 通过 所有介质
停用的
report_problem
维护状态 非在 维护
触发器 = count_line_passwd_passwd_line_gt_35
发送消息给用户: Admin (Zabbix Administrator) 通过 Email
已启用

3)选择”监测中”，选择 “仪表盘”，查看监控信息

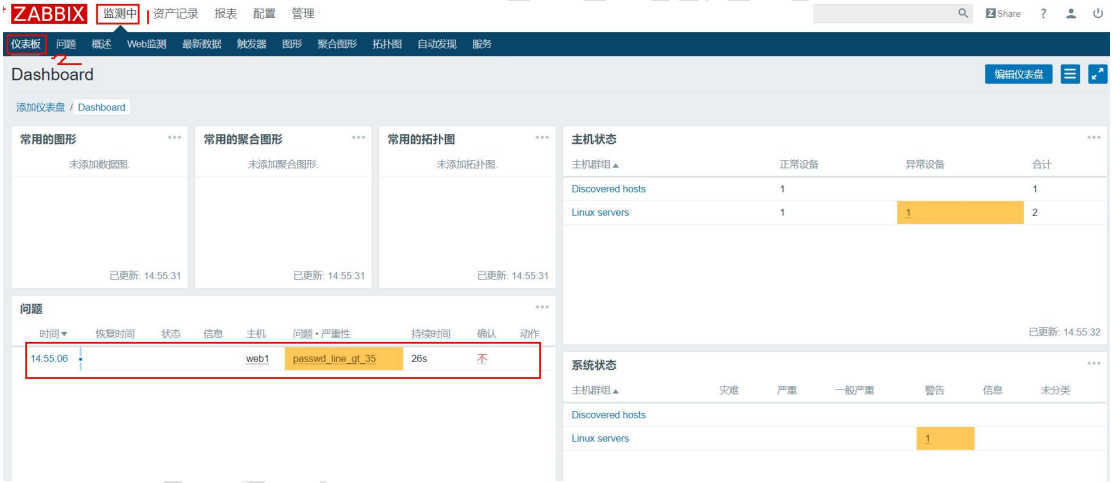


效果测试

在被监控主机创建账户 登录监控端 Web 页面，在仪表盘中查看问题

web1 上批量创建用户

```
[root@web1 ~]# for i in {1..10}
> do
> useradd test$i
> done
```



2）在监控服务器上使用 mail 命令查收报警邮件

```
[root@zabbixserver ~]# yum -y install mailx
[root@zabbixserver ~]# mail
```