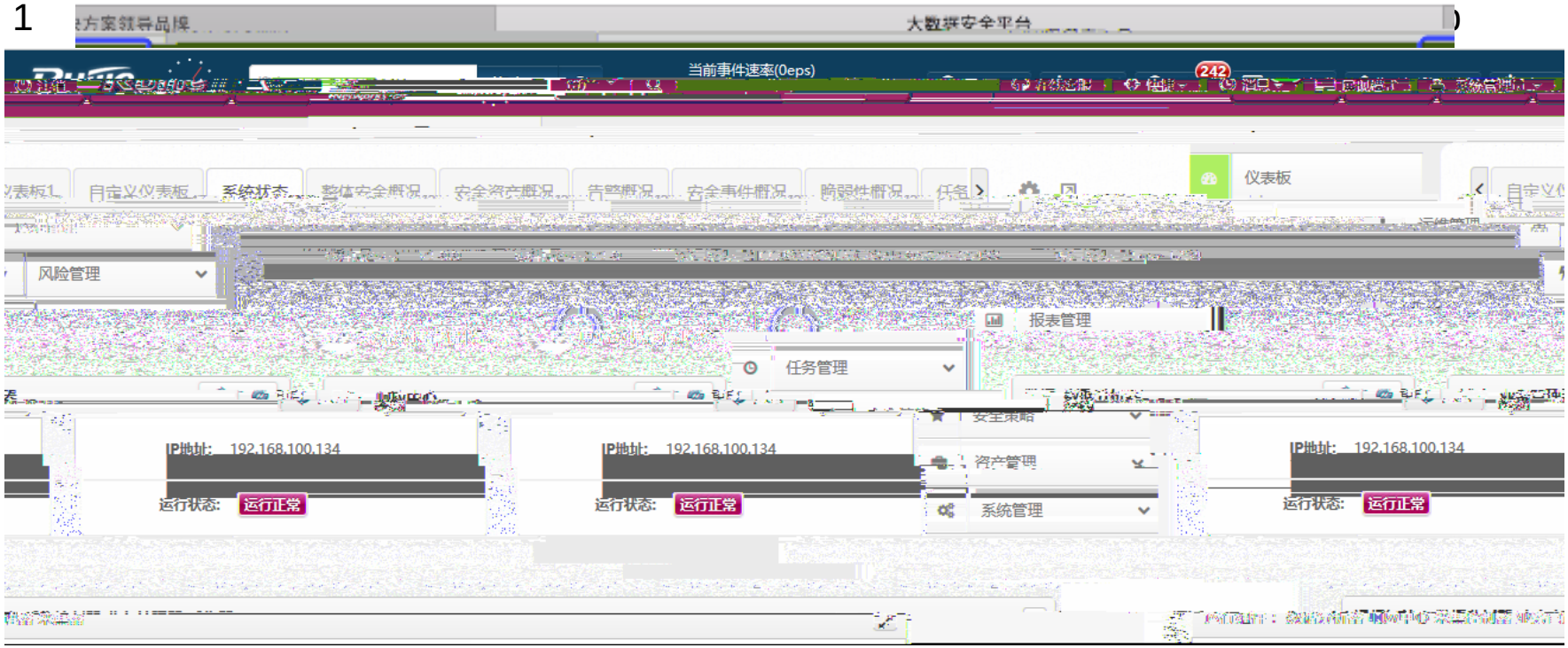
RG-BDS -A

ぐ

1



https://192.168.0.100

س admin س ruijie123 ث د

BDS

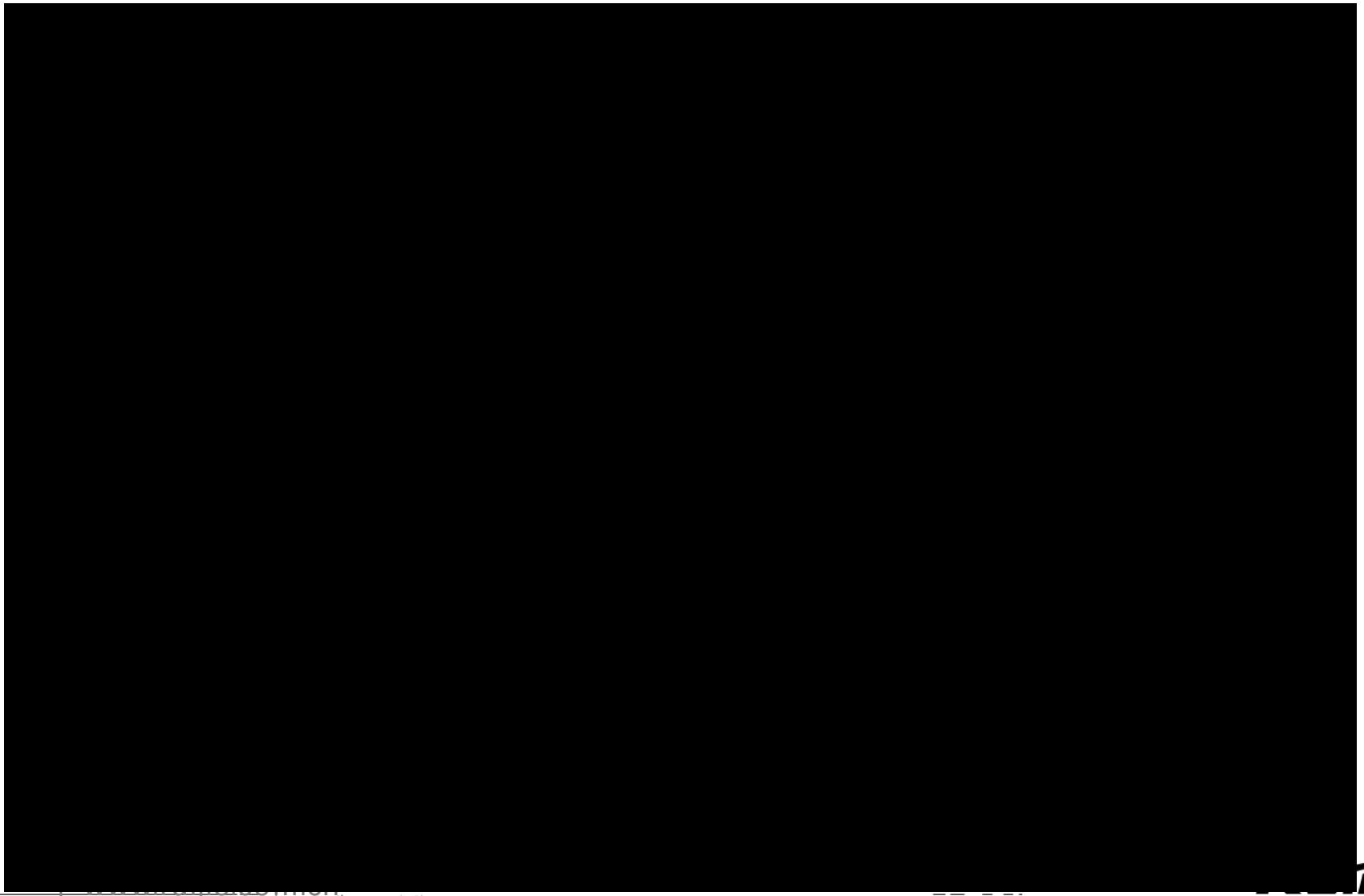
1 ڼ BDS ا -> ip

2 ٮ ٮ -> ->ip ip ٮ ٮٰ

3

VS

1 windows server2008 ip 5.5.5.5



BDS ث ـ / /

/ BDS

° ٻ ° ج

1 BDS

2 BDS ٻ ٺپ

ٺپ گي ڱ

1 Syslog گي Linux/Unix

2 SNMP Trap گي

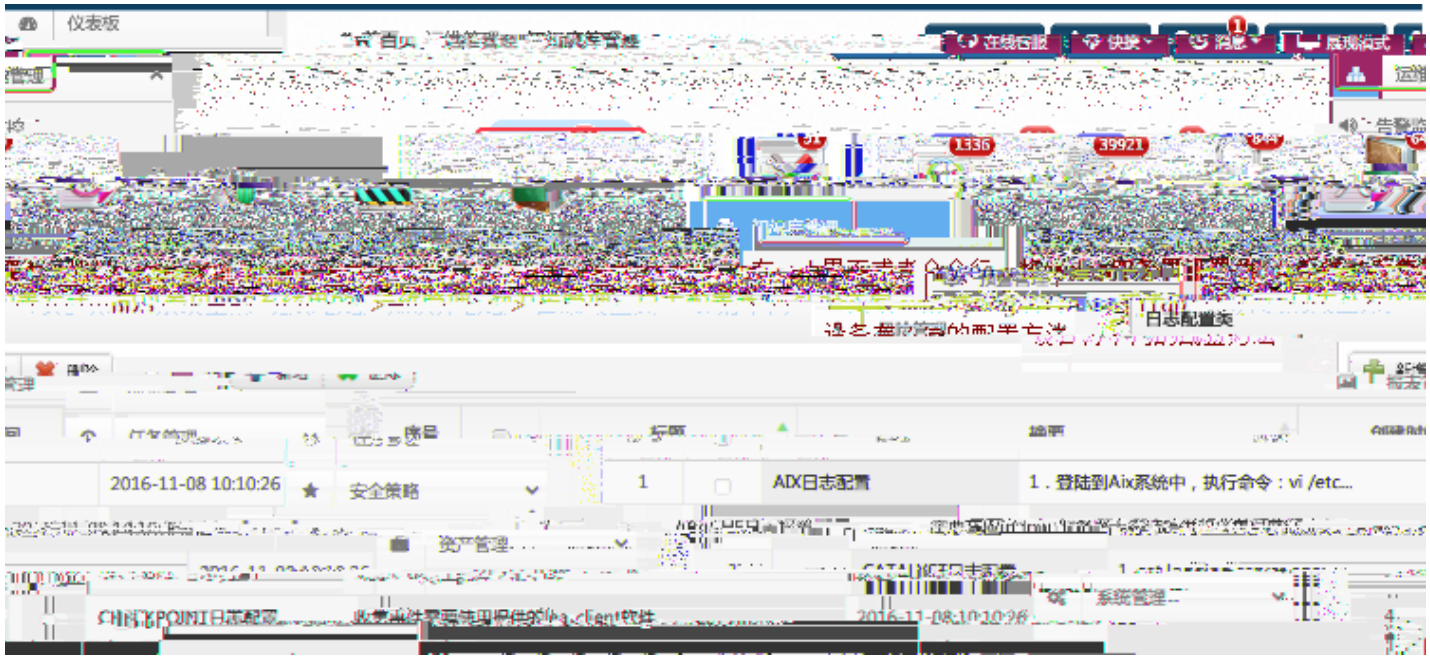
3 WMI گي Windows

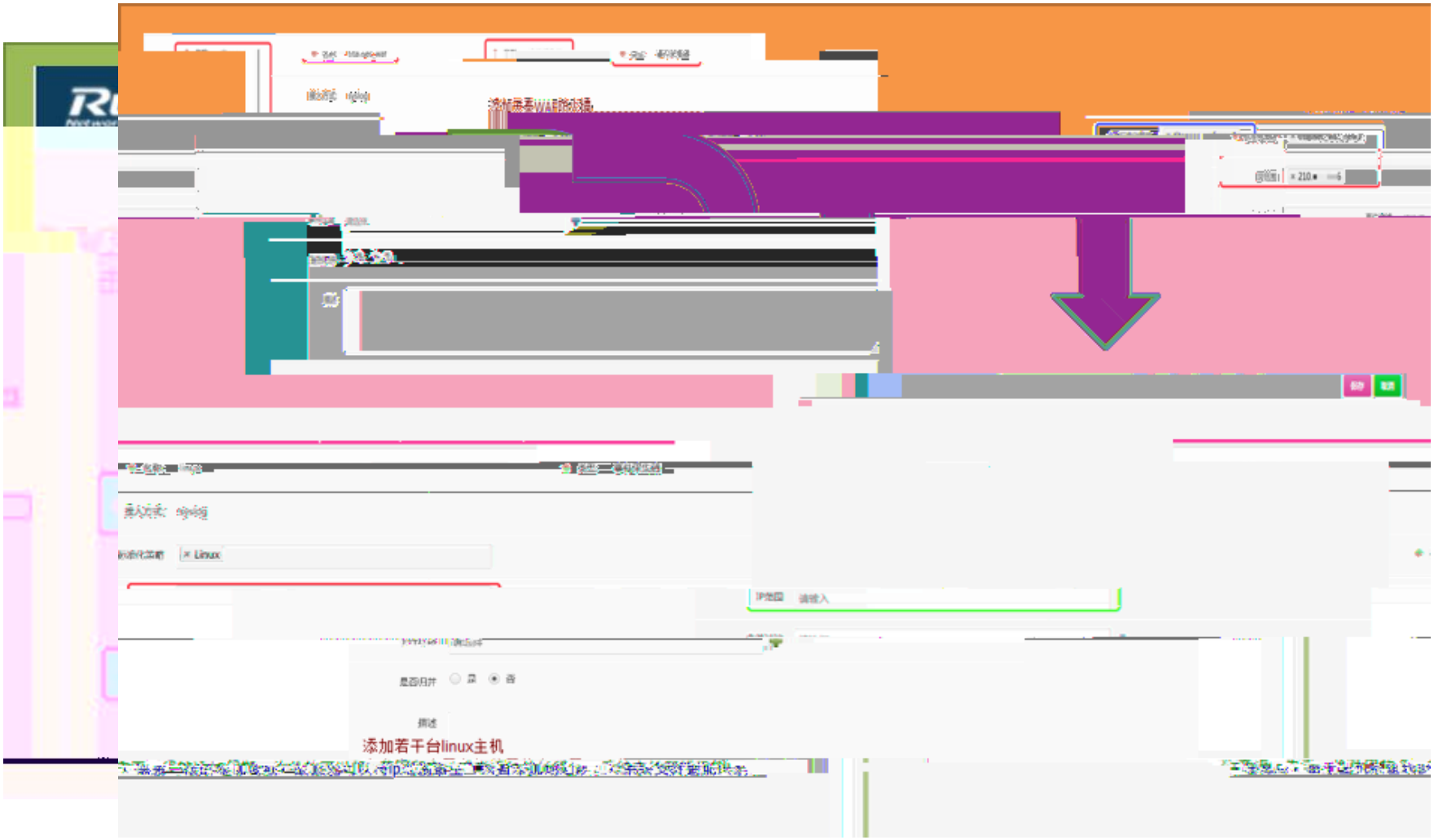
4 گي ٱڳ

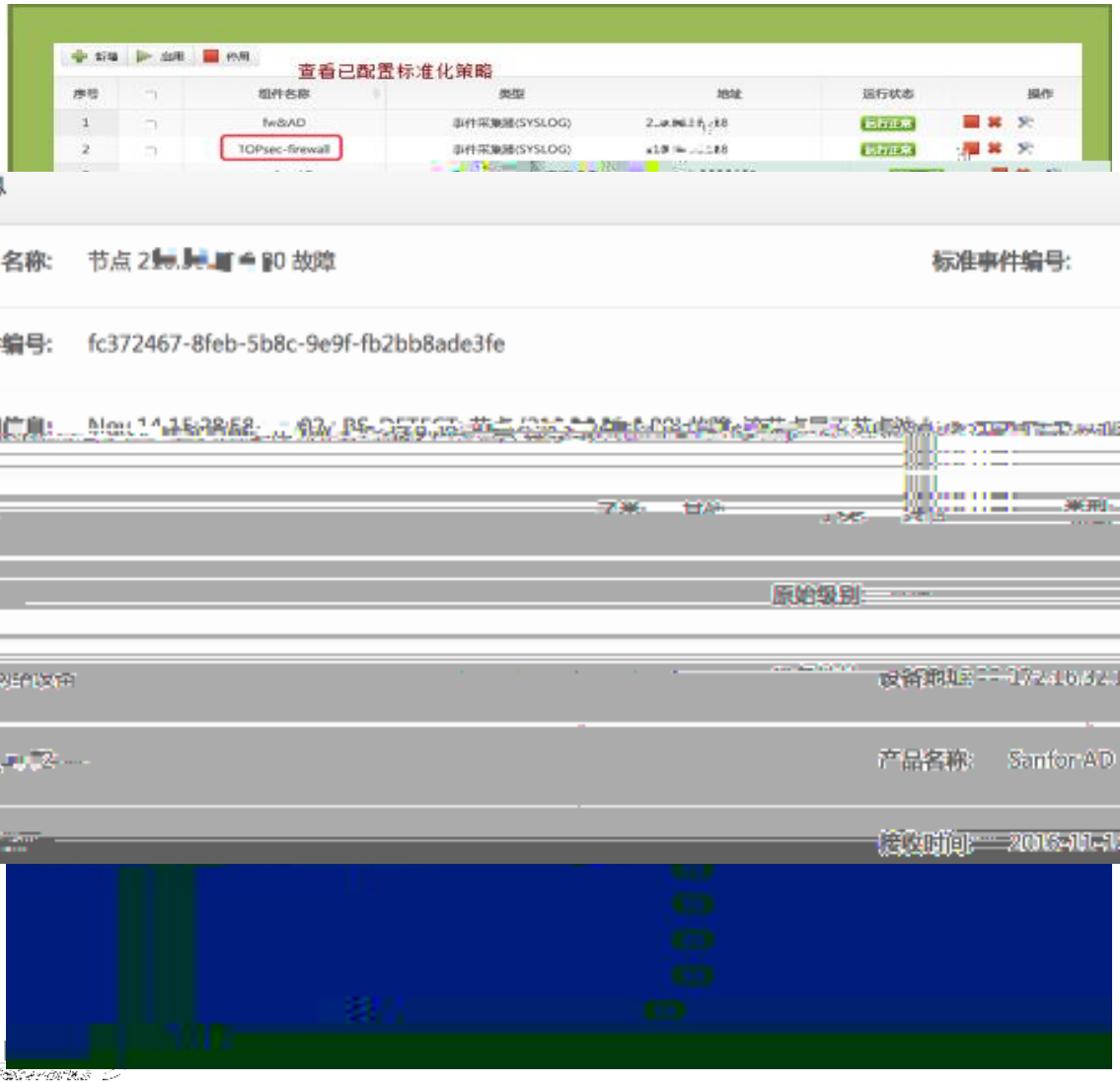
Symantec ڄ ڪ Ḥ ᴍ ٻ ٧

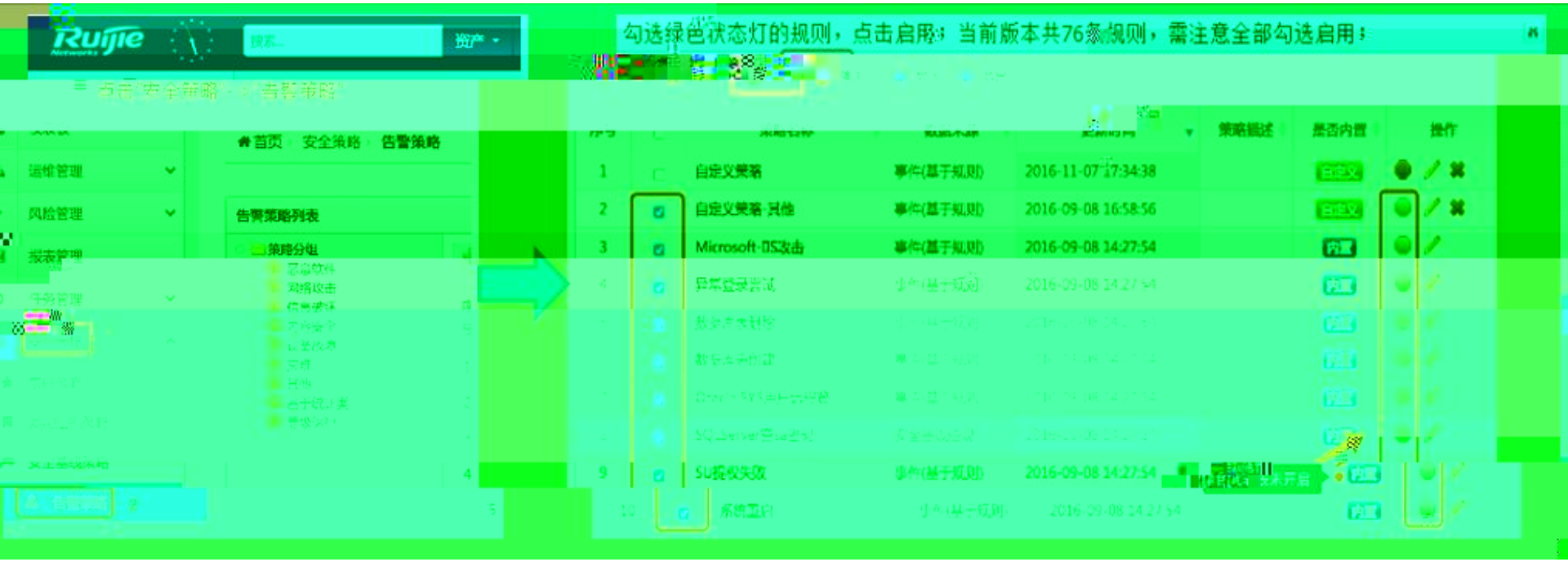
BDS 。 2 1 1 linux

2 172.16.32.11 172.16.32.12
210.x.x.x
1 waf 210.x.x.x
linux ip 。




添加若干台linux主机


查看已配置标准化策略
序号
组件名称
类型
地址
运行状态
操作
1
fw&AD
TOPsec-firewall
基本信息
名称:
节点 2
故障
标准事件编号:
事件编号:
fc372467-8feb-5b8c-9e9f-fb2bb8ade3fe
详细信息:
信息
原始级别
级别
设备名称:
产品名称:
Sanfor AD
产品版本:
接收时间:


勾选绿色状态灯的规则，点击启用；当前版本共76条规则，需注意全部勾选启用；

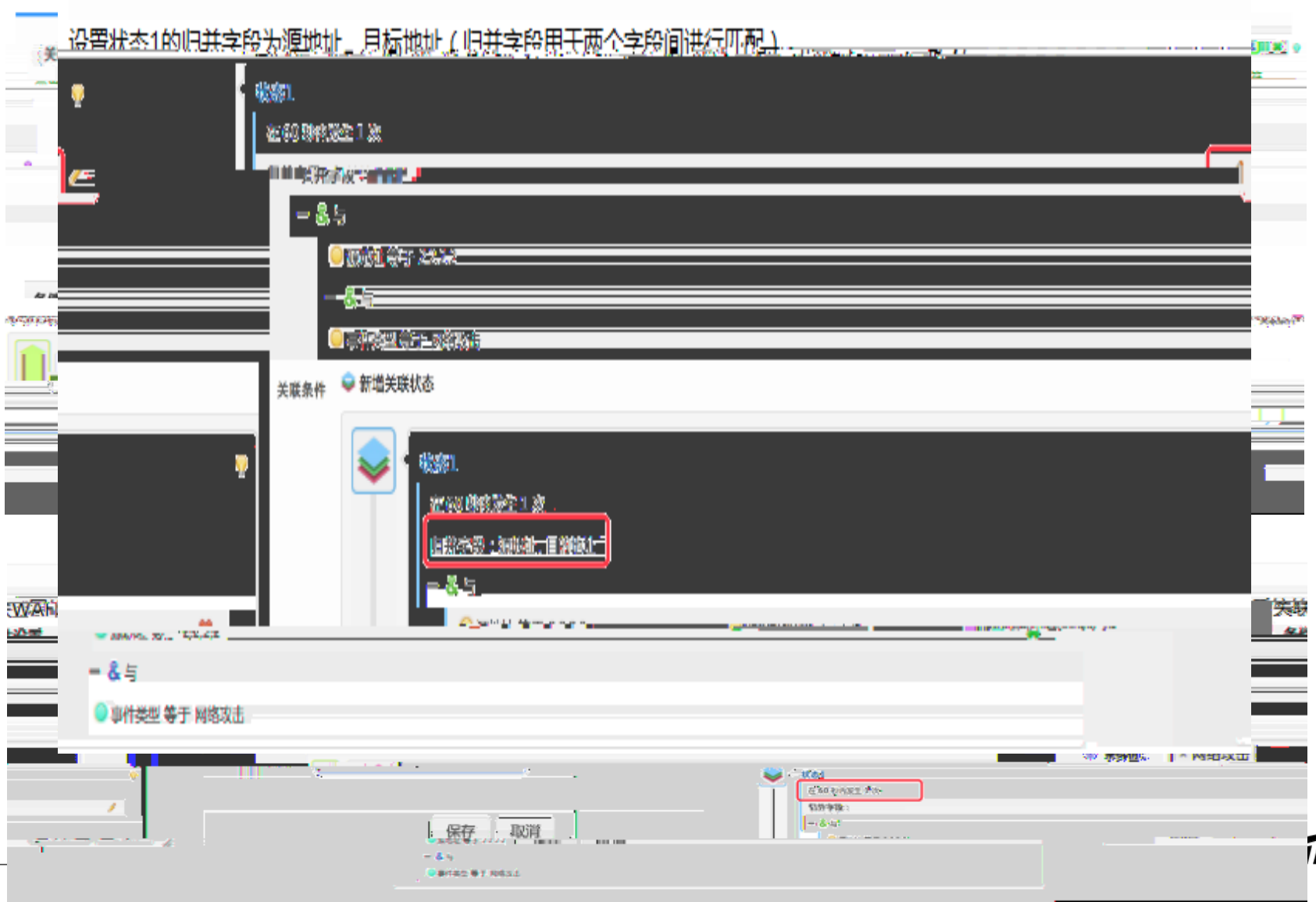
1 1 waf web 60 a b
2.2.2.2

2 2 60 10 a b ip
3.3.3.3

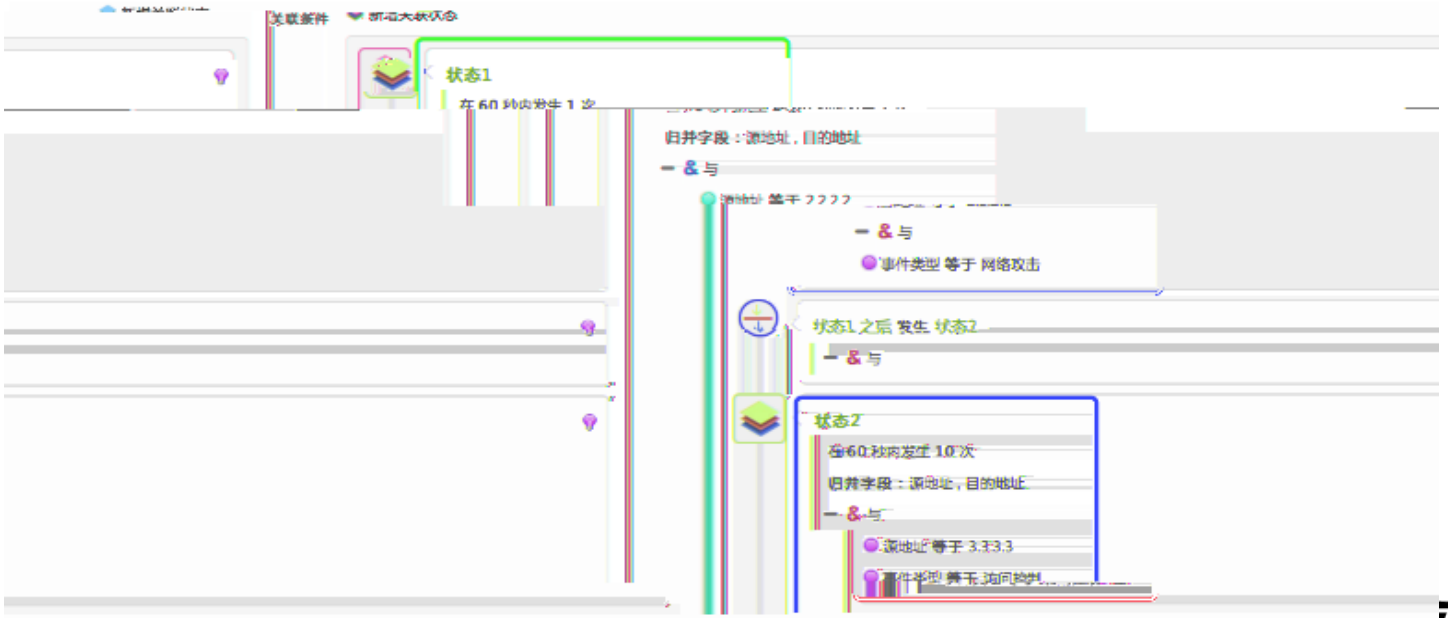
3 1 2

Ruijie Networks
搜索...
资产
"安全策略->告警策略->网络攻击"，点击"新增"
仪表板

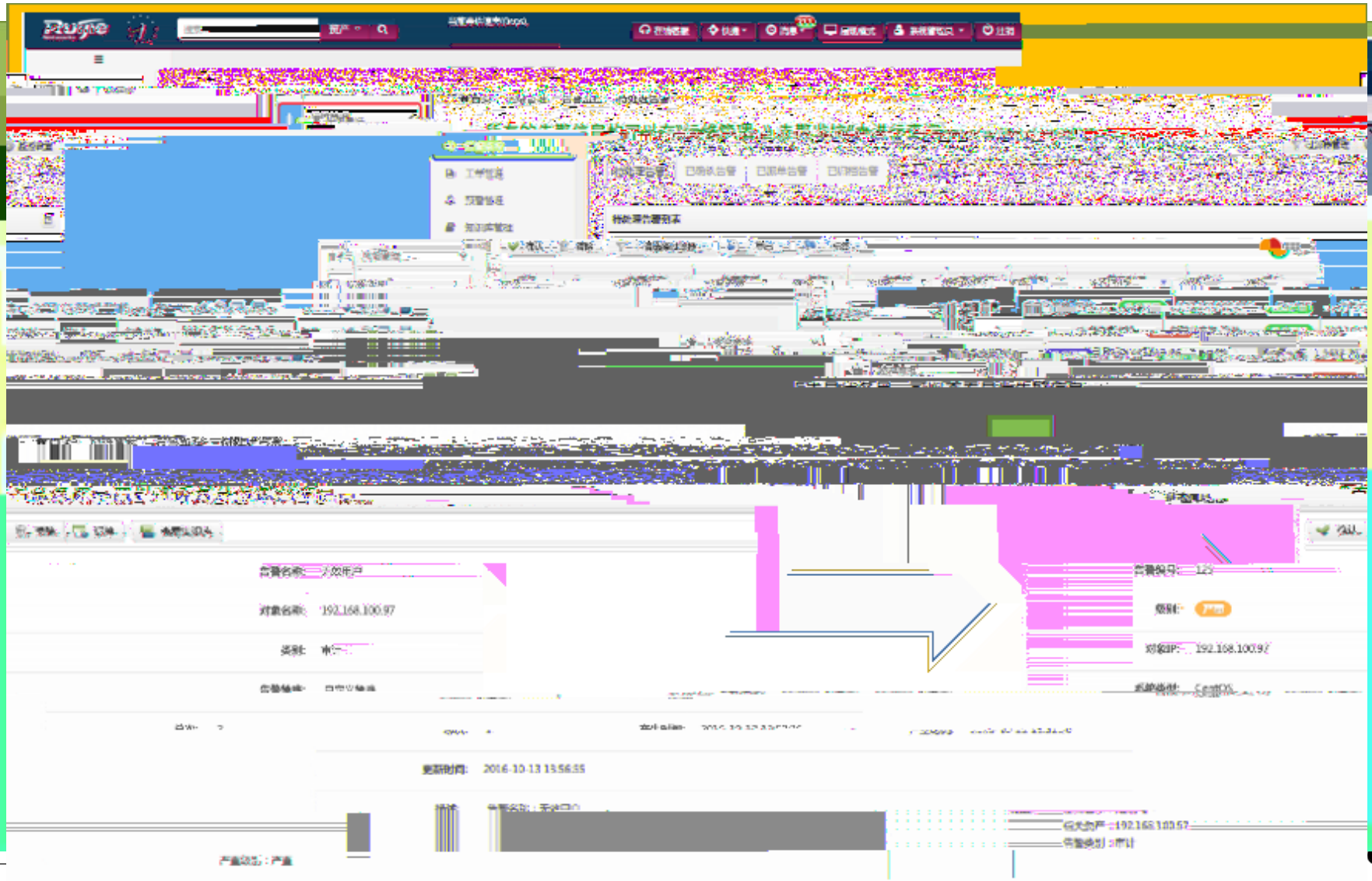
设定关联策略类型
点击运算符&符号，如图
条件设置
条件：
严重级别
信息
保存
取消


设置状态1的归并字段为源地址，目标地址（归并字段用于两个字段间进行匹配）
关联条件
新增关联状态
&与
事件类型 等于 网络攻击
保存
取消

完成的设置结果如下图

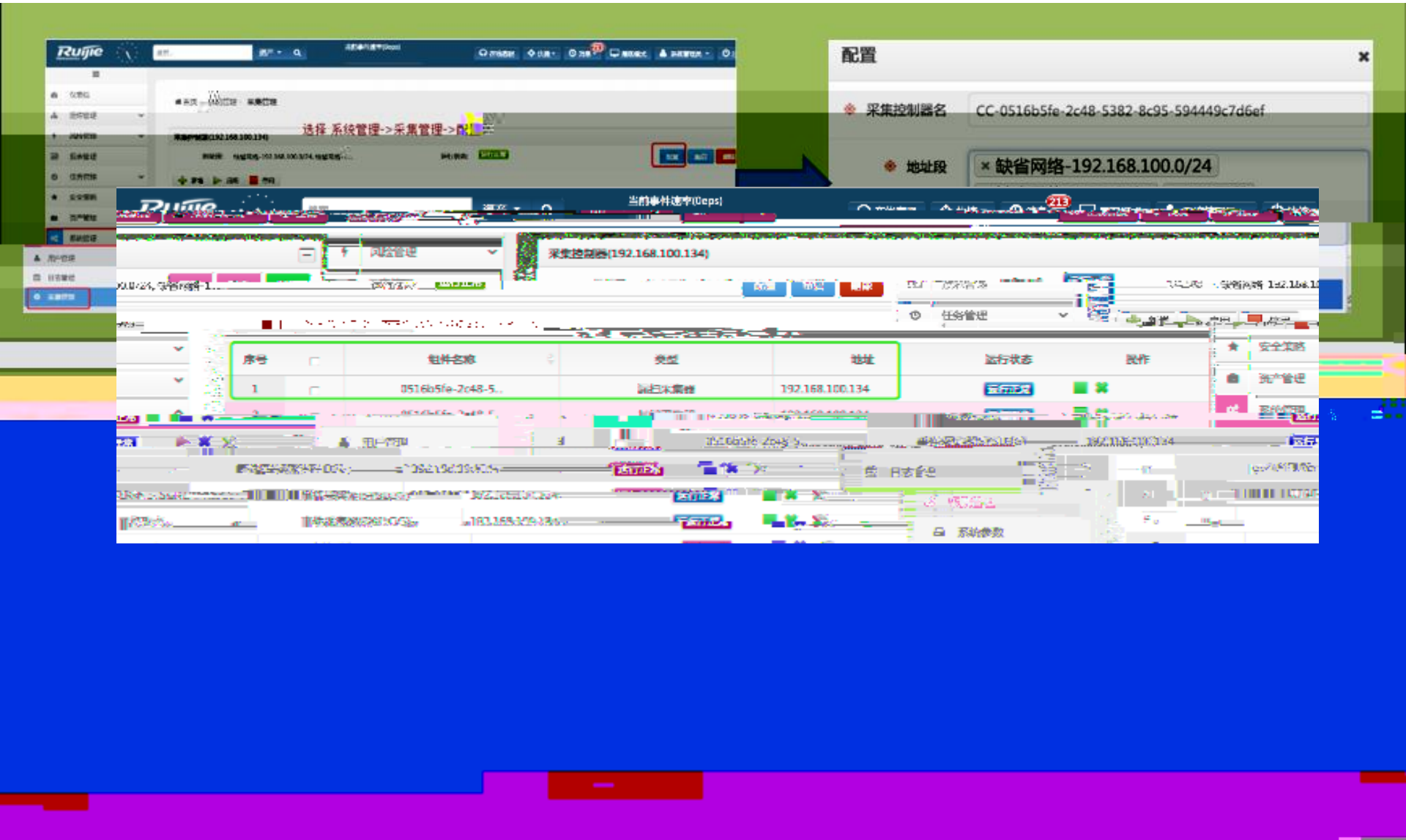

状态1
归并字段：源地址，目的地址
与
与
事件类型 等于 网络攻击
状态1 之后 发生 状态2
与
状态2
归并字段：源地址，目的地址
与

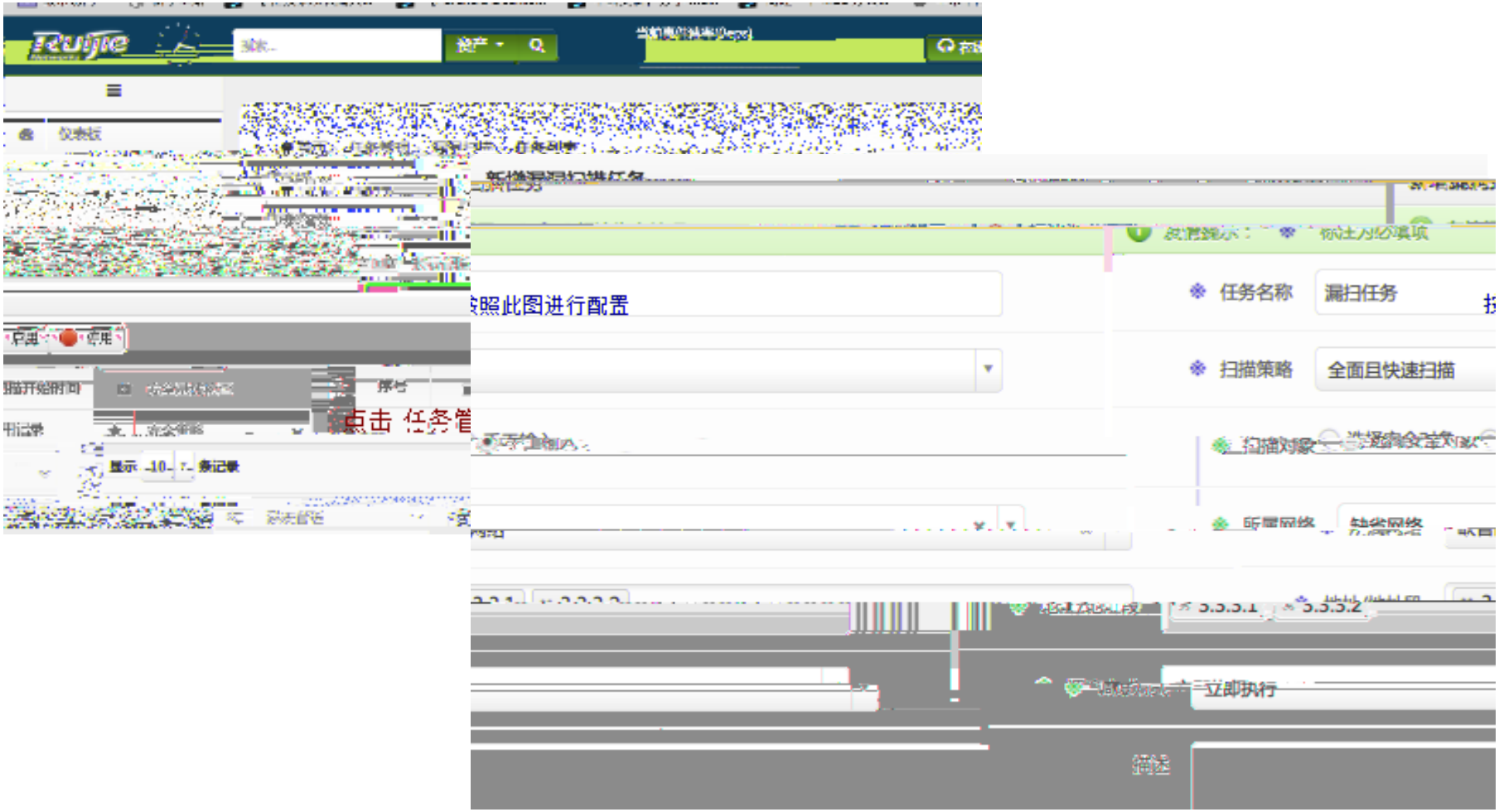
点击&符号
状态1
在 60 秒内发生 1 次
归并字段：
& 与
源地址 等于 2.2.2.2
& 与
响应方式
产生告警
转发外系统
执行程序
活动列表
产生告警
友情提示：当告警名称生成方式选择"自动"时,产生告警的事件名称将作为告警名称。
告警名称生成方式
自动
自定义



ù© Ï Ä ¶ Ï D g%²) ê u É Ä öb Tožð

;


选择 系统管理->采集管理->配
配置
采集控制器名
CC-0516b5fe-2c48-5382-8c95-594449c7d6ef
地址段
缺省网络-192.168.100.0/24
采集控制器(192.168.100.134)
序号
组件名称
类型
地址
监控状态
操作
1
192.168.100.134


Ruijie
资产
仪表板
照此图进行配置
任务名称
漏扫任务
扫描策略
全面且快速扫描
立即执行

漏洞结果、漏洞解决方法显示

ٻ

ٻ گ ئ

ئ

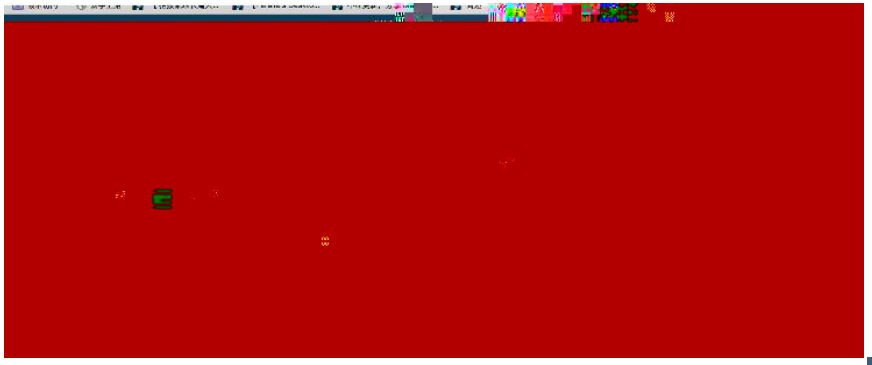
ئ

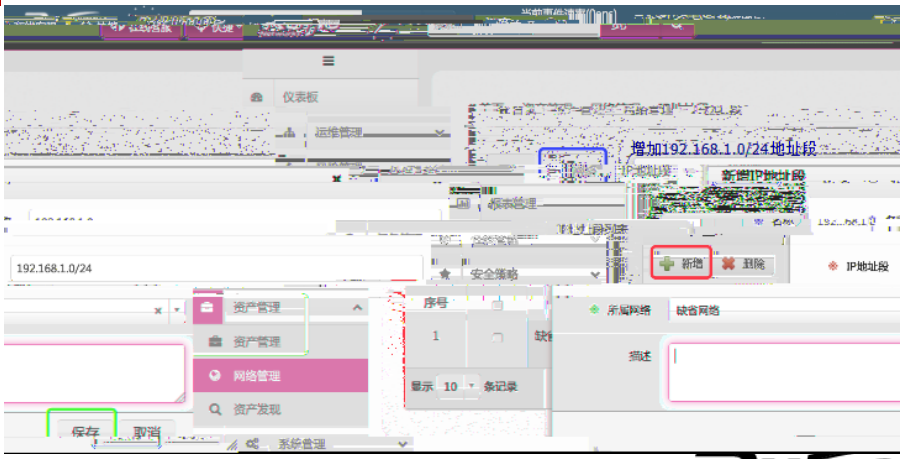
ئ

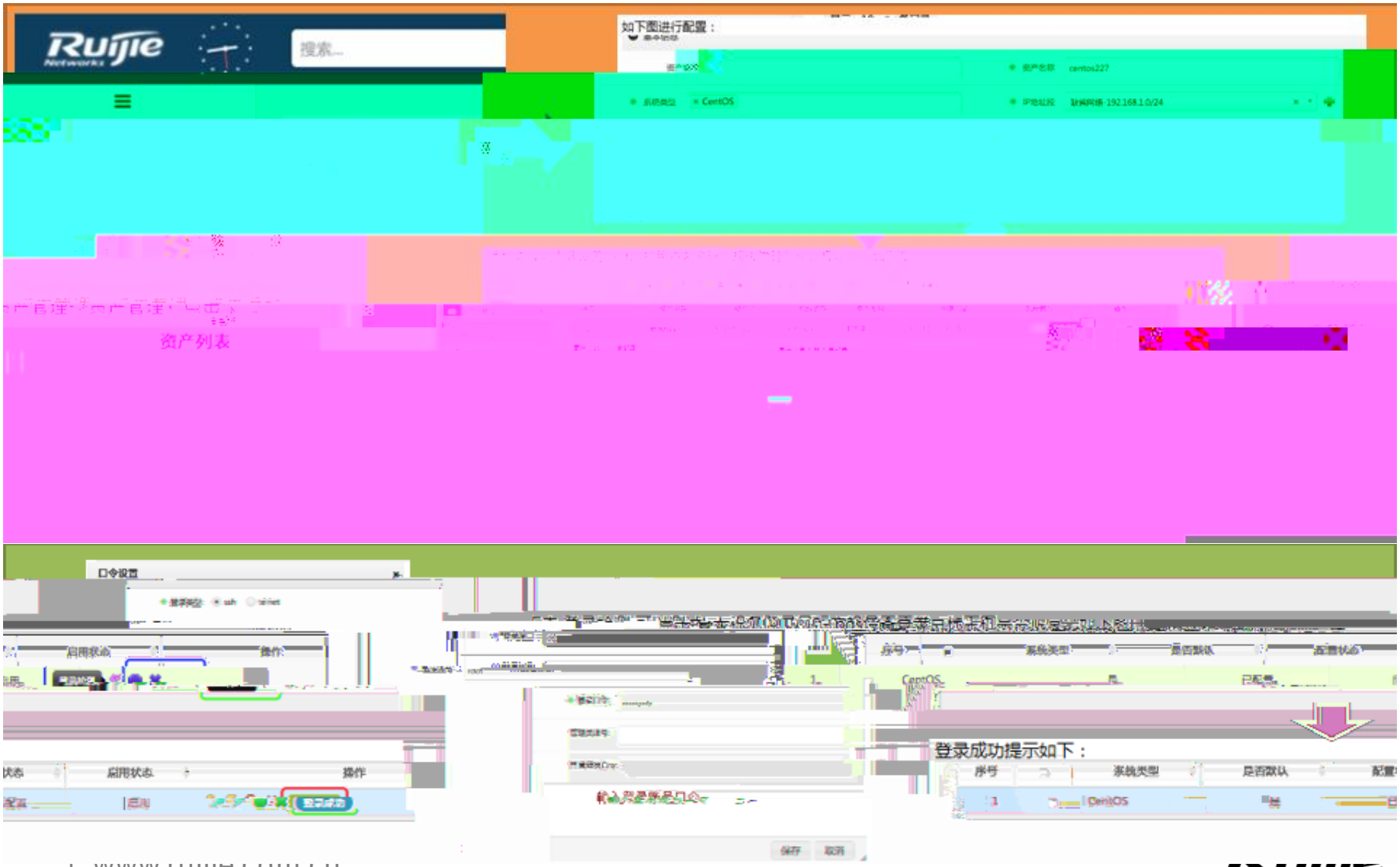
ئ

;

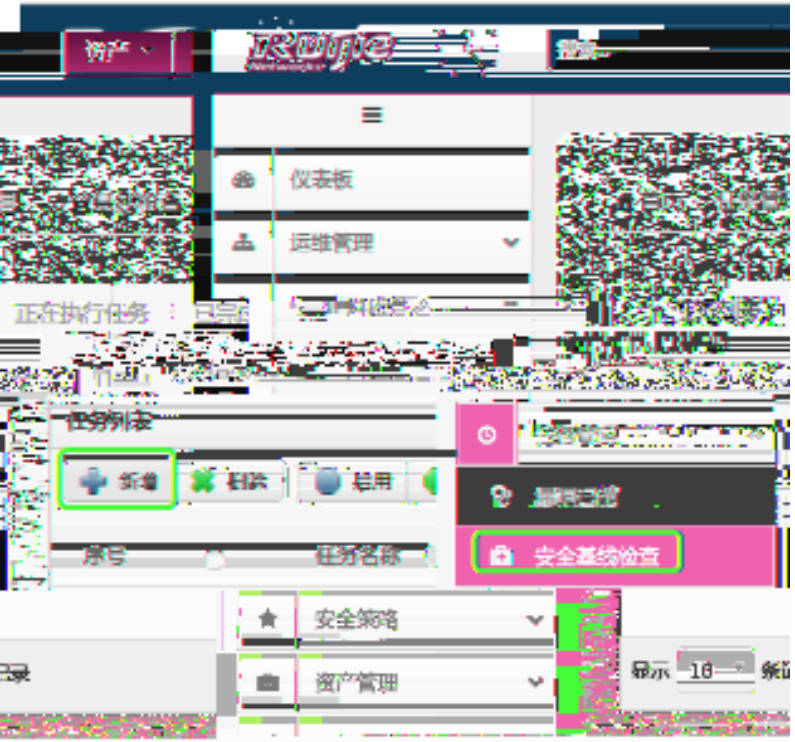
1:192.168.1.174:/24(windows 2008)
2:192.168.1.227/24(centos)



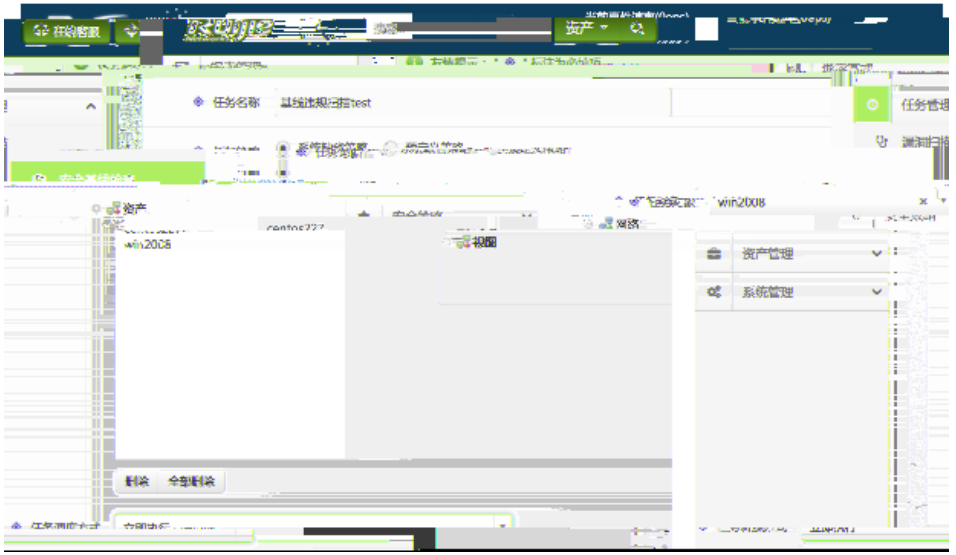



Ruijie Networks
搜索...
如下图进行配置：
CentOS
资产列表
口令设置
启用状态
操作
登录成功提示如下：
序号
系统类型
是否默认
CentOS

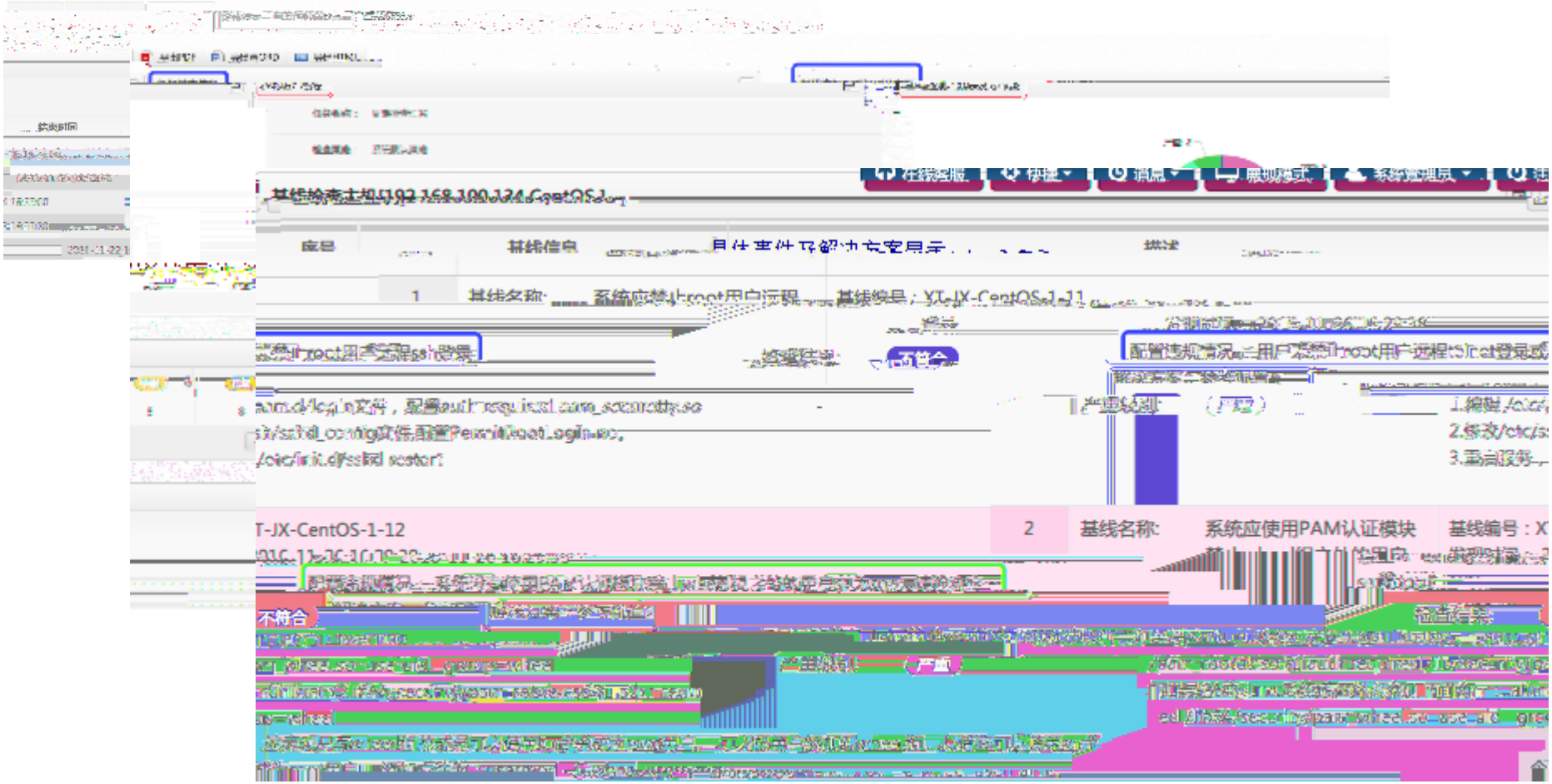
点击 任务管理->安全基线扫描->新增



按照如下图进行配置



点击“查看具体报告”，可以查看相应基线检查具体结果



ش ّ www.ruijie.com.cn

www.ruijie.com.cn/service.aspx

bbs.ruijie.com.cn

webchat.ruijie.com.cn

4008-111-000