How to calculate connections from IP address with shell script and log to Zabbix graphic

Author : admin

We had to test the number of connections incoming IP sorted by its TCP / IP connection state.

For example:

TIME_WAIT, ESTABLISHED, LISTEN etc.

The reason behind is sometimes the IP address '192.168.0.1' does create more than 200 connections, a Cisco firewall gets triggered and the connection for that IP is filtered out. To be able to know in advance that this problem is upcoming. a Small userparameter script is set on the Linux servers, that does print out all connections from IP by its STATES sorted out.

The script is calc_total_ip_match_zabbix.sh is below:

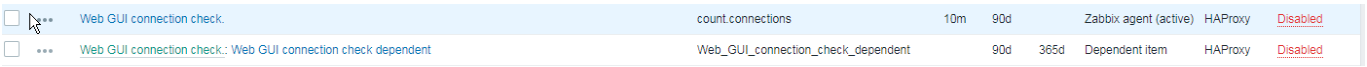
```
#!/bin/bash
#  check ESTIMATED / FIN_WAIT etc. netstat output for IPs and calculate total
# UserParameter=count.connections,(/usr/local/bin/calc_total_ip_match_zabbix.sh)
CHECK_IP='192.168.0.1';
f=0;

for i in $(netstat -nat | grep "$CHECK_IP" | awk '{print $6}' | sort | uniq -c | sort -n); do

echo -n "$i ";
f=$((f+i));
done;
```

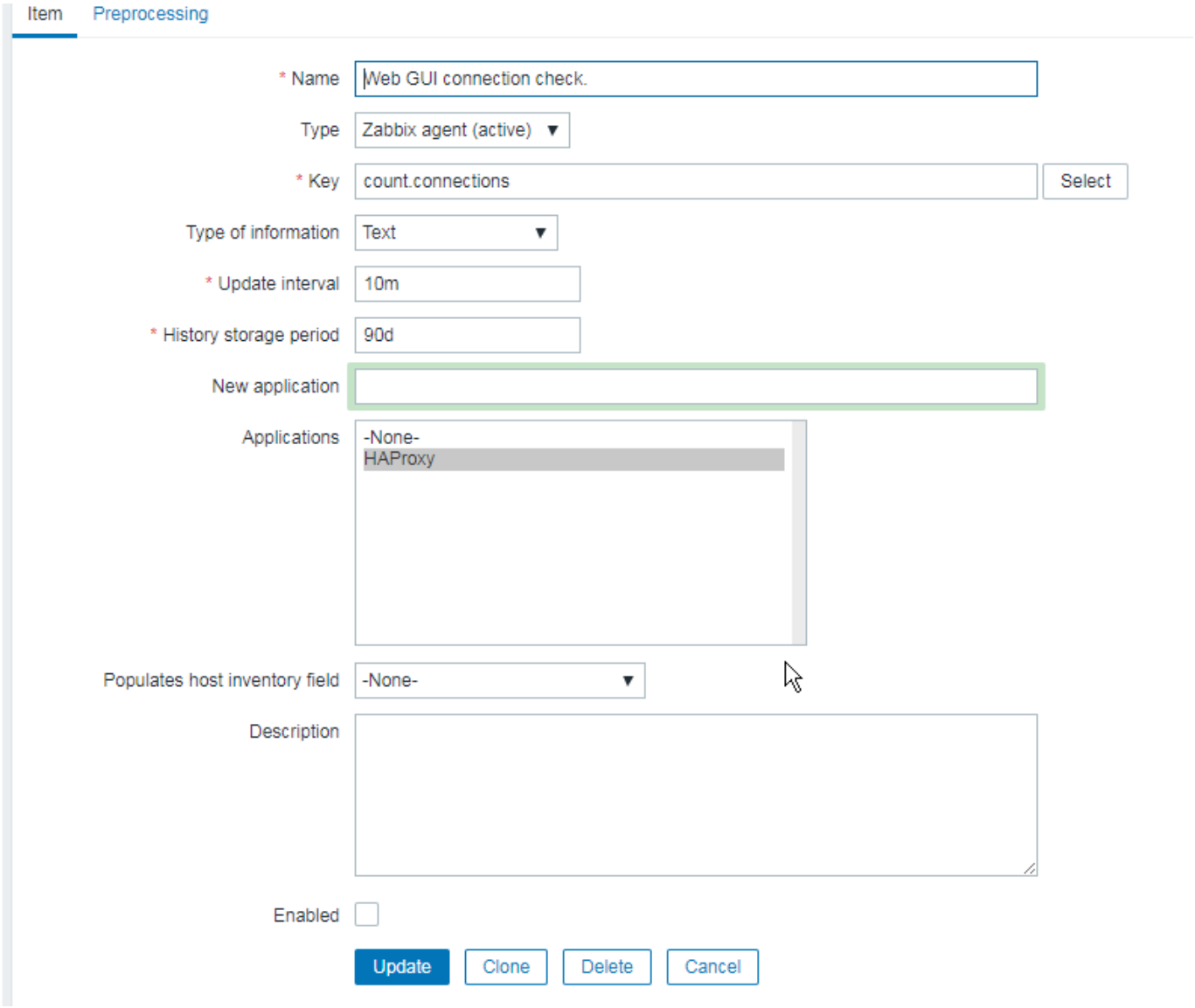
```
echo
echo "Total: $f"
```

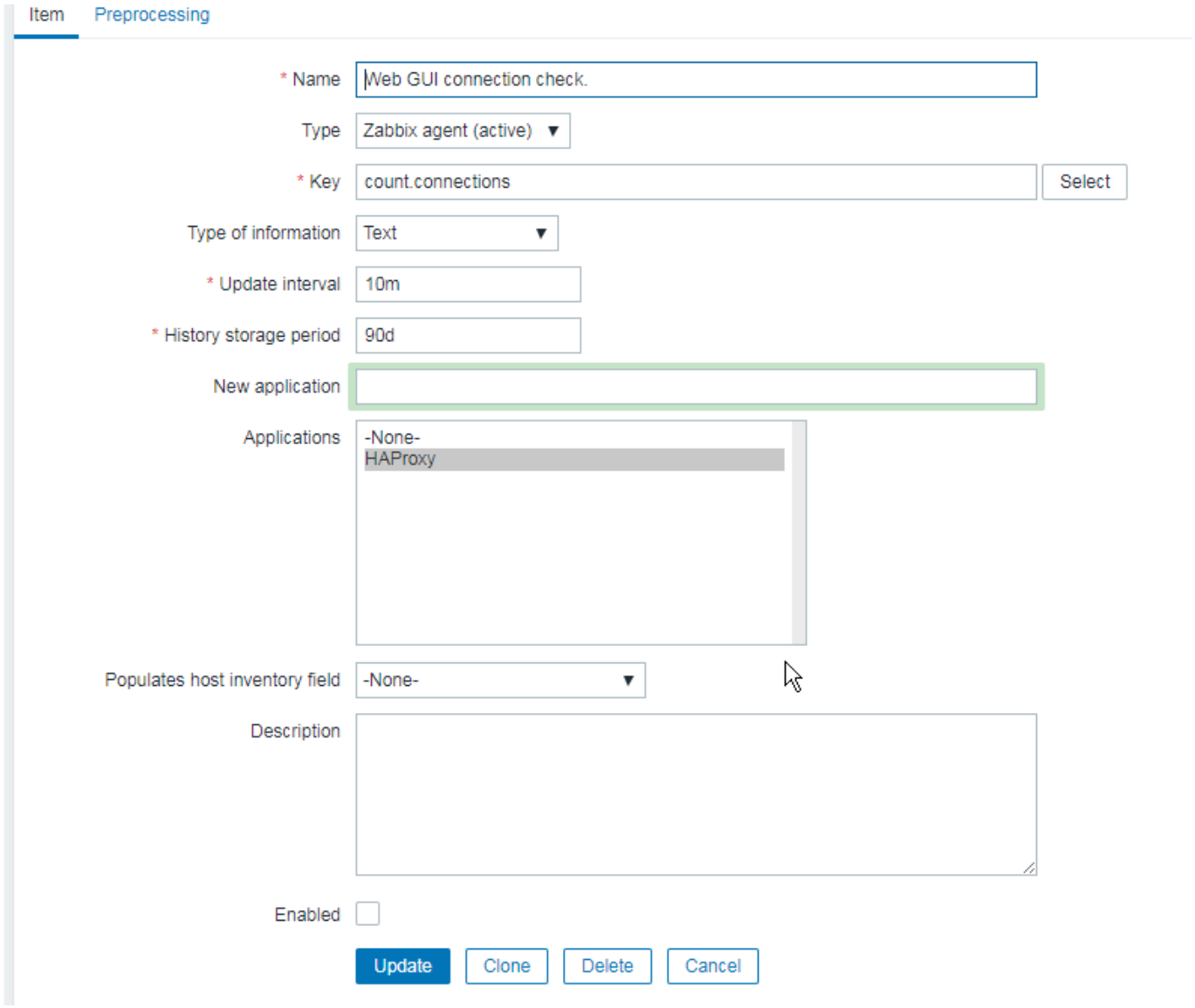
```
root@pcfreak:/bashscripts# ./calc_total_ip_match_zabbix.sh
1 TIME_WAIT 2 ESTABLISHED 3 LISTEN

Total: 6
```

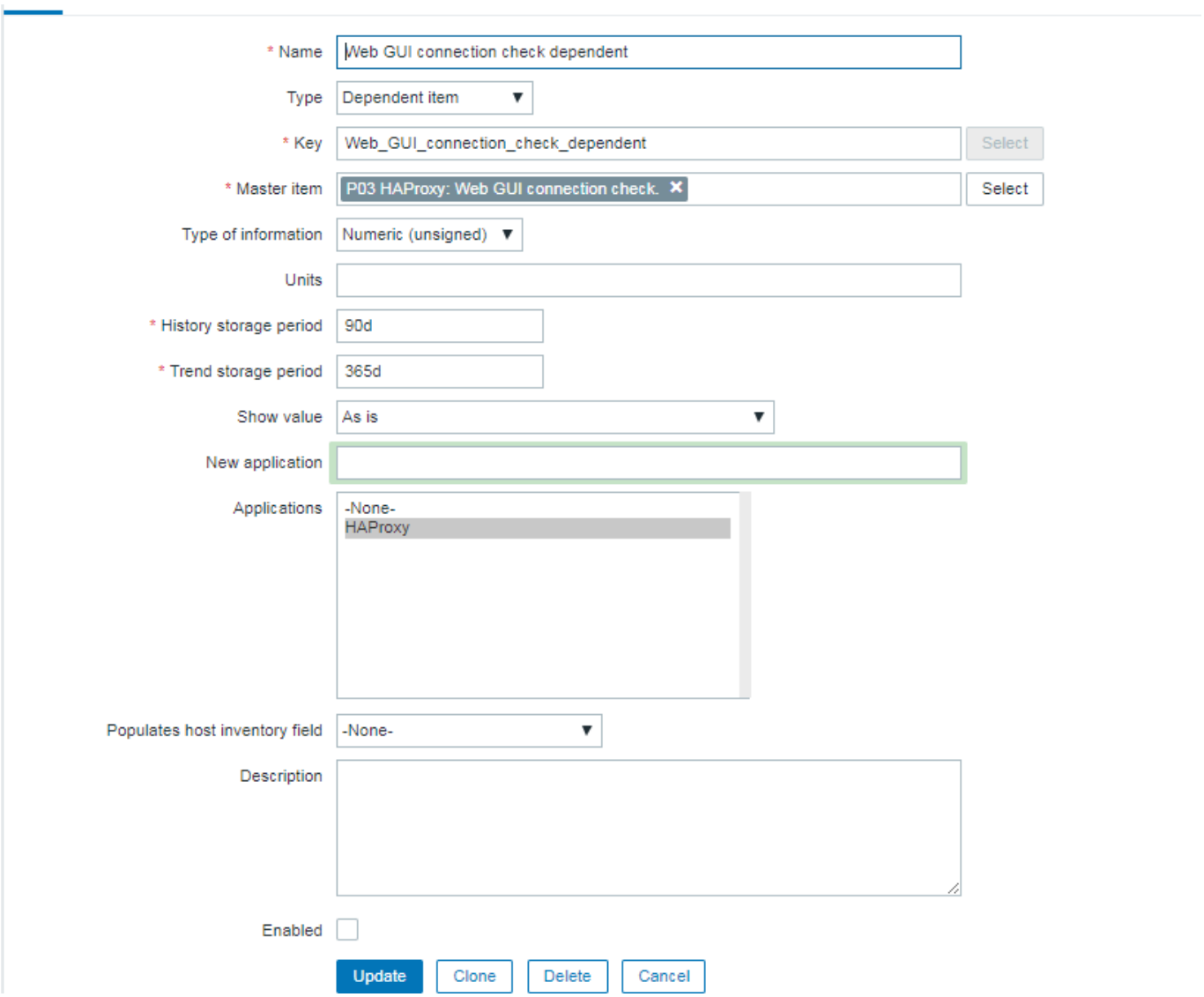
```
root@pcfreak:/bashscripts# ./calc_total_ip_match_zabbix.sh
2 ESTABLISHED 3 LISTEN
Total: 5
```

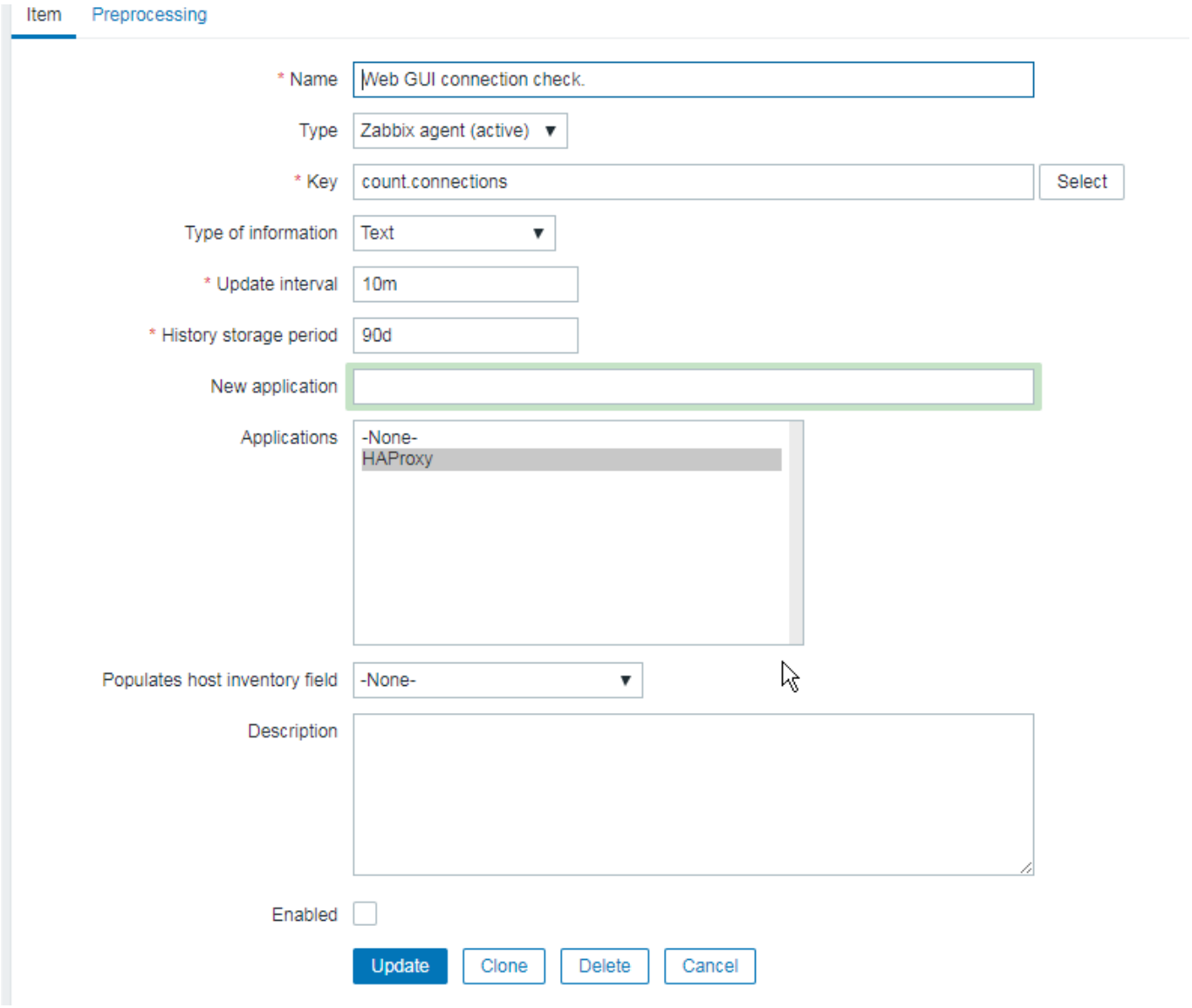
To make process with Zabbix it is necessery to have an Item created and a Depedent Item.



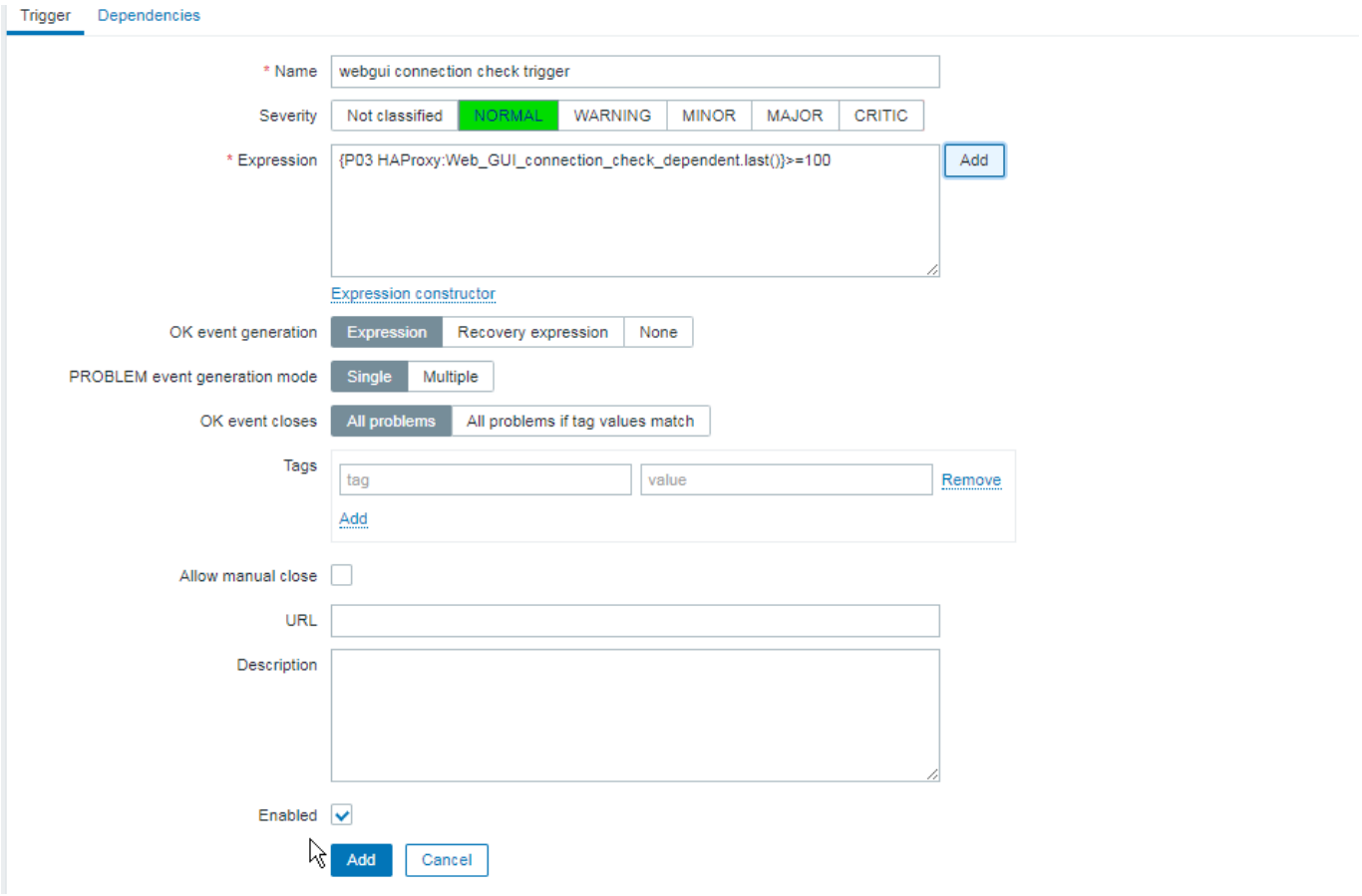

Item
Preprocessing
* Name
Web GUI connection check.
Type
Zabbix agent (active)
* Key
count.connections
Select
Type of information
Text
* Update interval
10m
* History storage period
90d
New application
Applications
-None-
HAProxy
Populates host inventory field
-None-
Description
Enabled
Update
Clone
Delete
Cancel


Item
Preprocessing
* Name
Web GUI connection check.
Type
Zabbix agent (active)
* Key
count.connections
Select
Type of information
Text
* Update interval
10m
* History storage period
90d
New application
Applications
-None-
HAProxy
Populates host inventory field
-None-
Description
Enabled
Update
Clone
Delete
Cancel


* Name
Web GUI connection check dependent
Type
Dependent item
* Key
Web_GUI_connection_check_dependent
Select
* Master item
P03 HAProxy: Web GUI connection check.
Select
Type of information
Numeric (unsigned)
Units
* History storage period
90d
* Trend storage period
365d
Show value
As is
New application
Applications
-None-
HAProxy
Populates host inventory field
-None-
Description
Enabled
Update
Clone
Delete
Cancel



Finally create a trigger to trigger alarm if you have more than or eqaul to 100 Total overall connections.



The Zabbix userparameter script should be as this:

cat /etc/zabbix/zabbix_agentd.d/userparameter_webgui_conn.conf
UserParameter=count.connections,(/usr/local/bin/webgui_conn_track.sh)

Some collleagues suggested more efficient shell script solution for suming the overall number of connections, below is less time consuming version of script, that can be used for the calculation.

```
#!/bin/bash -x
# show FIN_WAIT2 / ESTIMATED etc. and calcuate total
count=$(netstat -n | grep "192.168.0.1" | awk ' { print $6 } ' | sort -n | uniq -c | sort -nr)
total=$((${count// /+}))
echo "$count"
echo "Total:" "$total"
```

2 ESTABLISHED
1 TIME_WAIT
Total: 3

Below is the graph built with Zabbix showing all the fluctuations from connections from monitored IP.