Zabbix script to track arp address cache loss (arp incomplete) from Linux server to gateway IP

Author : admin

Some of the Linux servers recently, I'm responsible had a very annoying issue recently. The problem is ARP address to default configured server gateway is being lost, every now and then and it takes up time, fot the remote CISCO router to realize the problem and resolve it. We have debugged with the Network expert colleague, while he was checking the Cisco router and we were checking the arp table on the Linux server with arp command. And we came to conclusion this behavior is due to some network mess because of too many NAT address configurations on the network or due to a Cisco bug. The colleagues asked Cisco but cisco does not have any solution to the issue and the only close work around for the gateway loosing the mac is to set a network rule on the Cisco router to flush its arp record for the server it was loosing the MAC address for.
This does not really solve completely the problem but at least, once we run into the issue, it gets resolved as quick as 5 minutes time. }

As we run a cluster environment it is useful to Monitor and know immediately once we hit into the MAC gateway disappear issue and if the issue persists, exclude the Linux node from the Cluster so we don't loose connection traffic.
For the purpose of Monitoring MAC state from the Linux haproxy machine towards the Network router GW, I have developed a small userparameter script, that is periodically checking the state of the MAC address of the IP address of remote gateway host and log to a external file for any problems with incomplete MAC address of the Remote configured default router.

In case if you happen to need the same MAC address state monitoring for your servers, I though that might be of a help to anyone out there.
To monitor MAC address incomplete state with Zabbix, do the following:

1. Create userparamater_arp_gw_check.conf Zabbix script

```
# cat userparameter_arp_gw_check.conf
UserParameter=arp.check,/usr/local/bin/check_gw_arp.sh
```

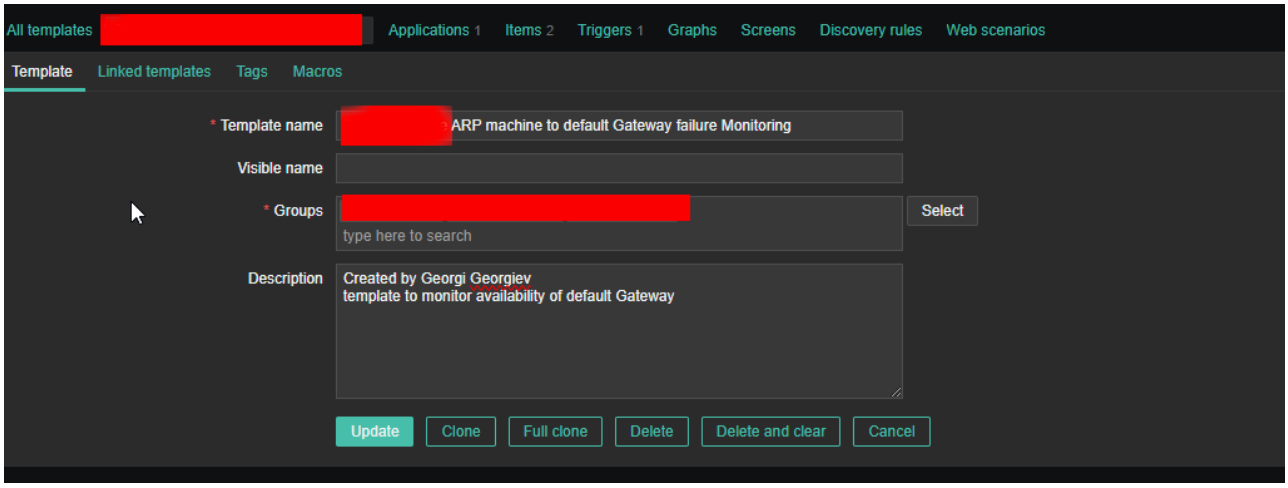
2. Create the following shell script /usr/local/bin/check_gw_arp.sh

```
#!/bin/bash
# simple script to run on cron peridically or via zabbix userparameter
# to track arp loss issues to gateway IP
#gw_ip='192.168.0.55';
gw_ip=$(ip route show|grep -i default|awk '{ print $3 }');
log_f='/var/log/arp_incomplete.log';
grep_word='incomplete';
inactive_status=$(arp -n "$gw_ip" |grep -i $grep_word);
# if GW incomplete record empty all is ok
if [[ $inactive_status == '' ]]; then
echo $gw_ip OK 1;
else
# log inactive MAC to gw_ip
echo "$(date '+%Y-%m-%d %H:%M:%S')" "ARP_ERROR $inactive_status 0" | tee -a $log_f
2>&1 >/dev/null;
# printout to zabbix
echo "1 ARP FAILED: $inactive_status";
fi
```

You can download the check_gw_arp.sh here.

The script is supposed to automatically grep for the Default Gateway router IP, however before setting it up. Run it and make sure this corresponds correctly to the default Gateway IP MAC you would like to monitor.

3. Create New Zabbix Template for ARP incomplete monitoring

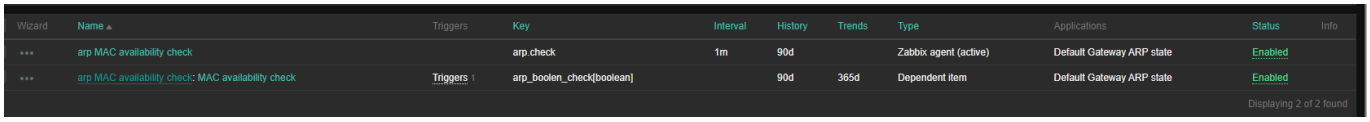


Create Application

**Name*
Default Gateway ARP state

4. Create Item and Dependent Item

Create Zabbix Item and Dependent Item like this



Wizard	Name	Triggers	Key	Interval	History	Trends	Type	Applications	Status	Info
•••	arp MAC availability check		arp.check	1m	90d		Zabbix agent (active)	Default Gateway ARP state	Enabled	
•••	arp MAC availability check: MAC availability check	Triggers 1	arp_boolen_check[boolean]		90d	365d	Dependent item	Default Gateway ARP state	Enabled	

Displaying 2 of 2 found

Item | Preprocessing

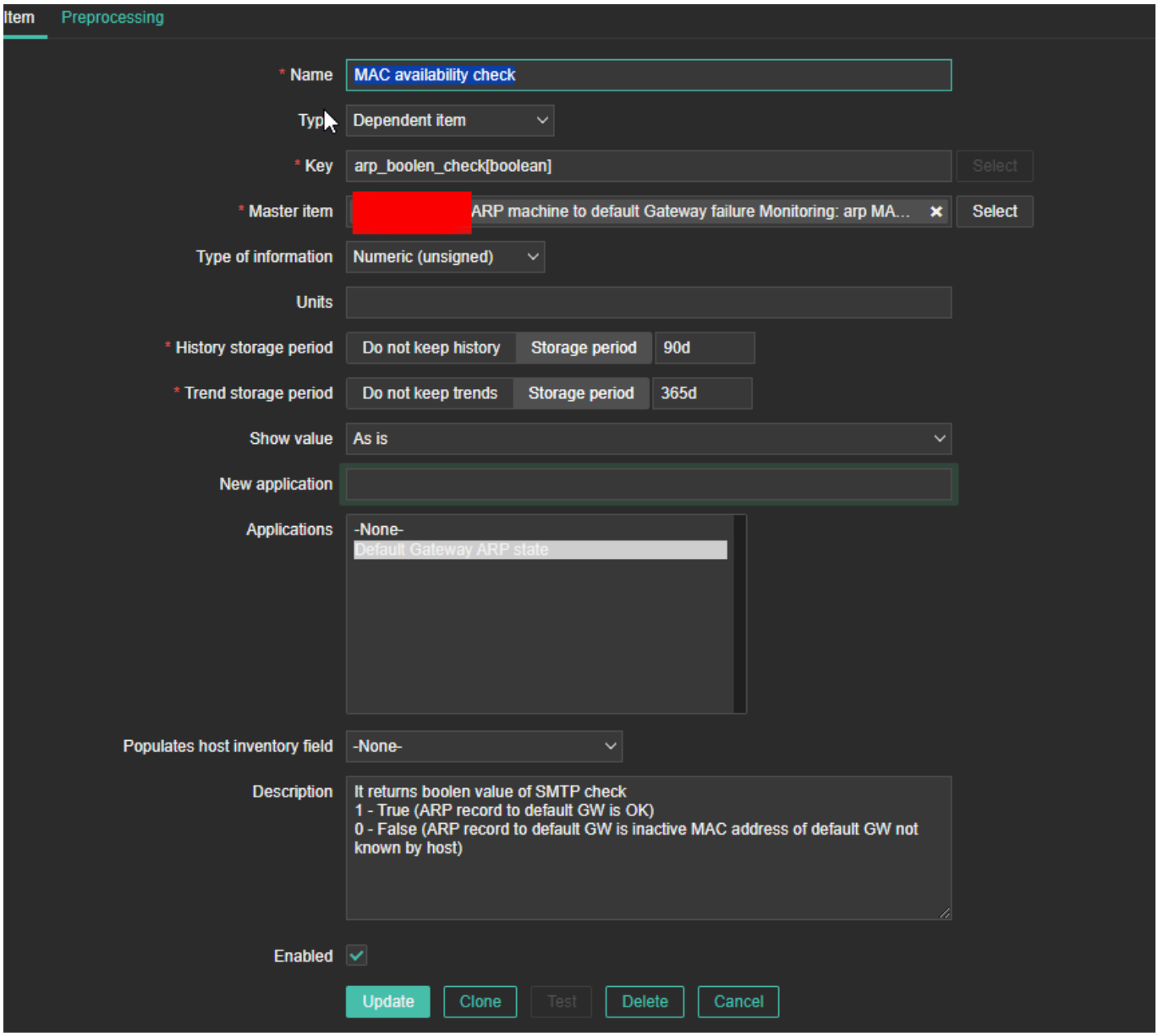
* Name: arp MAC availability check
Type: Zabbix agent (active)
* Key: arp.check [Select]
Type of information: Text
* Update interval: 1m
Custom intervals:

Type	Interval	Period	Action
Flexible / Scheduling	50s	1-7,00:00-24:00	Remove

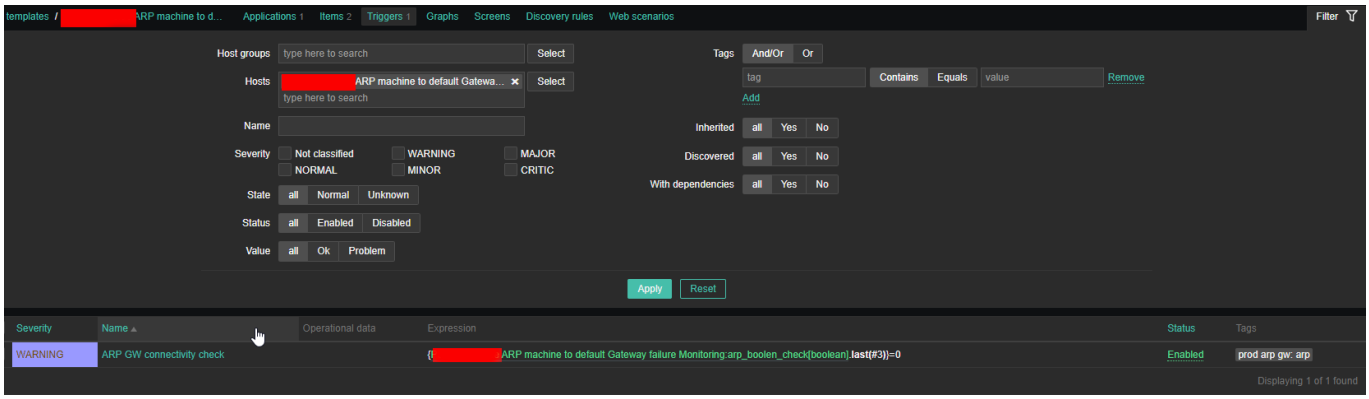
Add

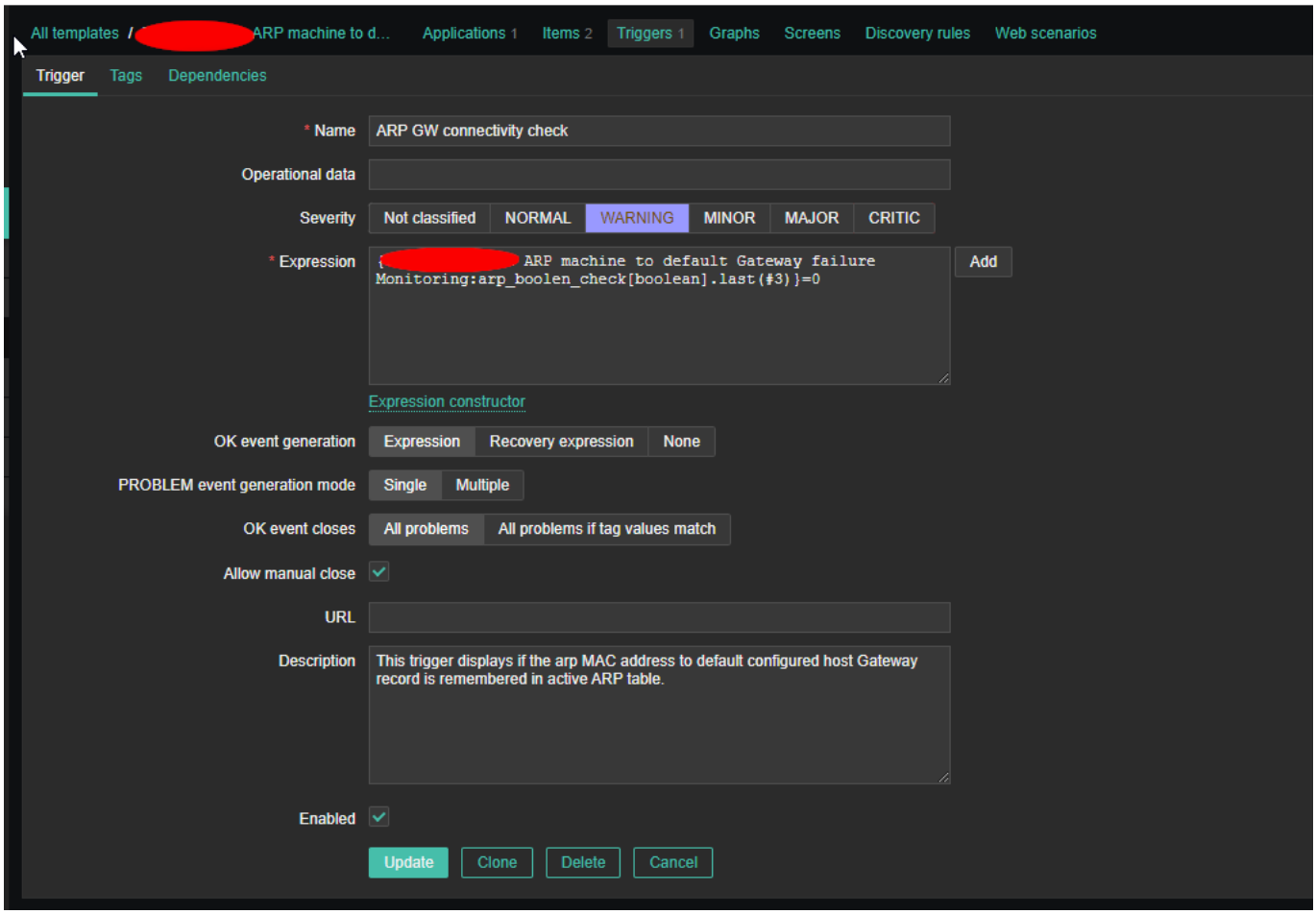
* History storage period: Do not keep history | Storage period | 90d
New application:
Applications: -None- / Default Gateway ARP state
Populates host inventory field: -None-
Description: This check is testing if the arp MAC address of default Gateway is reachable.
Enabled: ✓

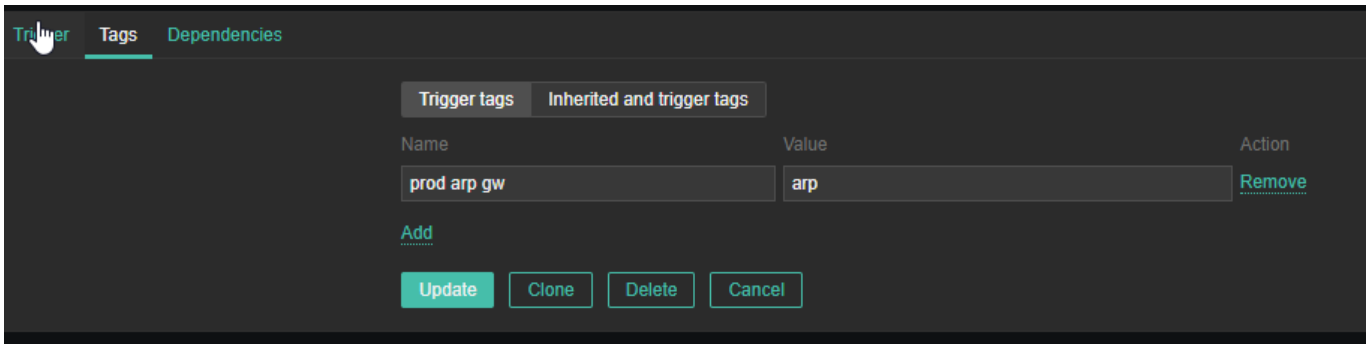
Update | Clone | Test | Delete | Cancel



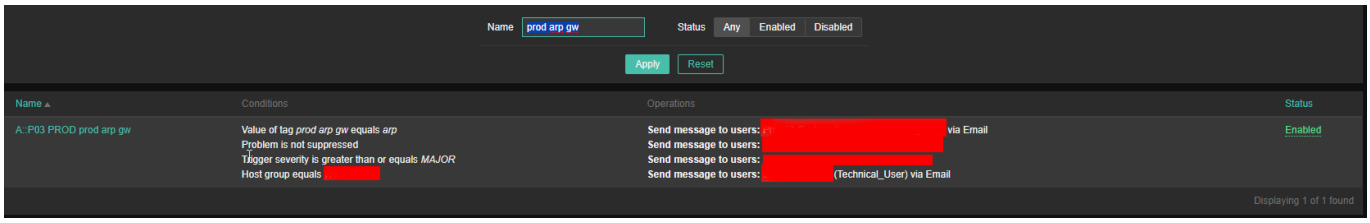
5. Create Trigger to trigger WARNING or whatever you like

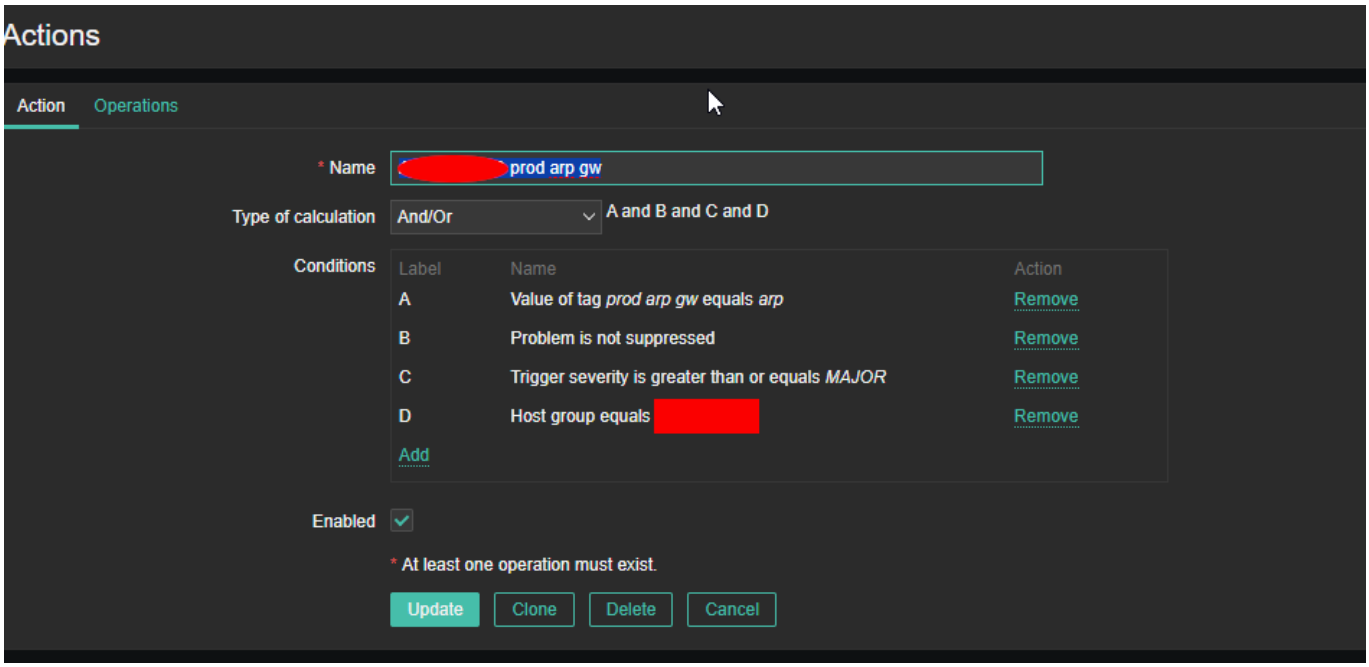

templates / [redacted] ARP machine to d...
Applications 1
Items 2
Triggers 1
Graphs
Screens
Discovery rules
Web scenarios
Filter
Host groups
type here to search
Select
Hosts
[redacted] ARP machine to default Gatewa...
Select
type here to search
Name
Severity
Not classified
WARNING
MAJOR
NORMAL
MINOR
CRITIC
State
all
Normal
Unknown
Status
all
Enabled
Disabled
Value
all
Ok
Problem
Tags
And/Or
Or
tag
Contains
Equals
value
Remove
Add
Inherited
all
Yes
No
Discovered
all
Yes
No
With dependencies
all
Yes
No
Apply
Reset
Severity
Name
Operational data
Expression
Status
Tags
WARNING
ARP GW connectivity check
{[redacted] ARP machine to default Gateway failure Monitoring:arp_boolen_check[boolean].last(#3)}=0
Enabled
prod arp gw: arp
Displaying 1 of 1 found


All templates / [redacted] ARP machine to d...
Applications 1
Items 2
Triggers 1
Graphs
Screens
Discovery rules
Web scenarios
Trigger
Tags
Dependencies
* Name
ARP GW connectivity check
Operational data
Severity
Not classified
NORMAL
WARNING
MINOR
MAJOR
CRITIC
* Expression
{[redacted] ARP machine to default Gateway failure Monitoring:arp_boolen_check[boolean].last(#3)}=0
Add
Expression constructor
OK event generation
Expression
Recovery expression
None
PROBLEM event generation mode
Single
Multiple
OK event closes
All problems
All problems if tag values match
Allow manual close
URL
Description
This trigger displays if the arp MAC address to default configured host Gateway record is remembered in active ARP table.
Enabled
Update
Clone
Delete
Cancel



6. Create Zabbix Action to notify via Email etc.





That's all. Once you set up this few little things, you can enjoy having monitoring Alerts for your ARP state incomplete on your Linux / Unix servers.
Enjoy !