SYSLOG-NG & SNMP

PRACTICAL WORK 2

TIZIANO NARDONE

UNIVERSITY OF REIMS | FRANCE

Table of Contents

I. Syslog-ng

1. Installation SYSLOG-NG

1. Installation on Debian

➔ *sudo apt install syslog-ng*

1. Installation on Alpine

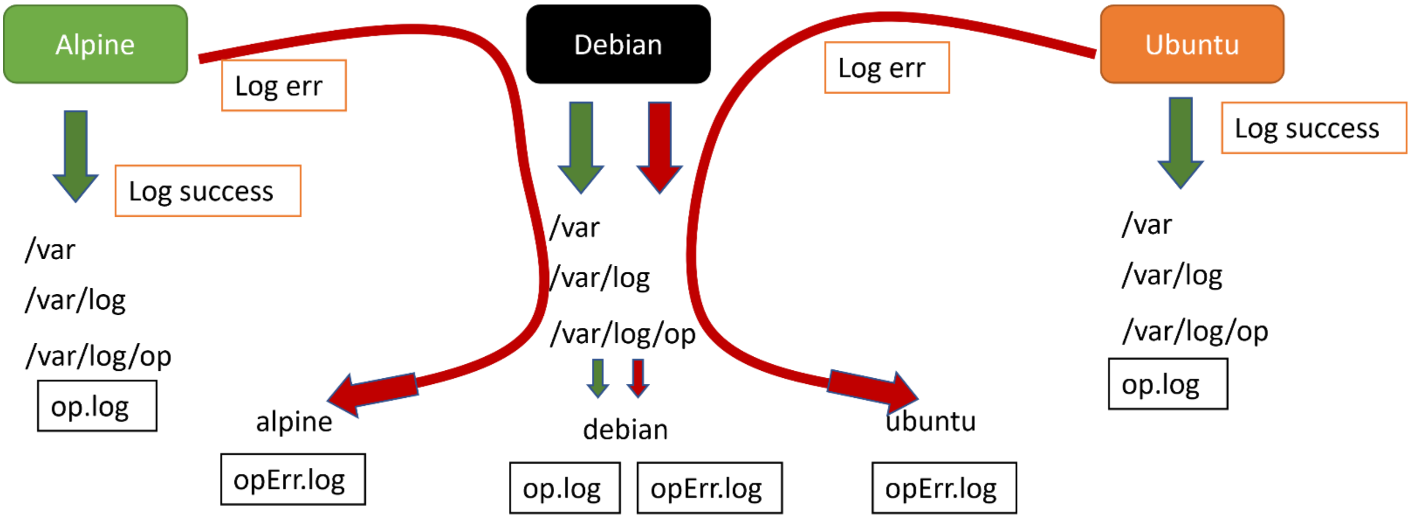
➔ *sudo apk add syslog-ng*

1. Installation on Ubuntu

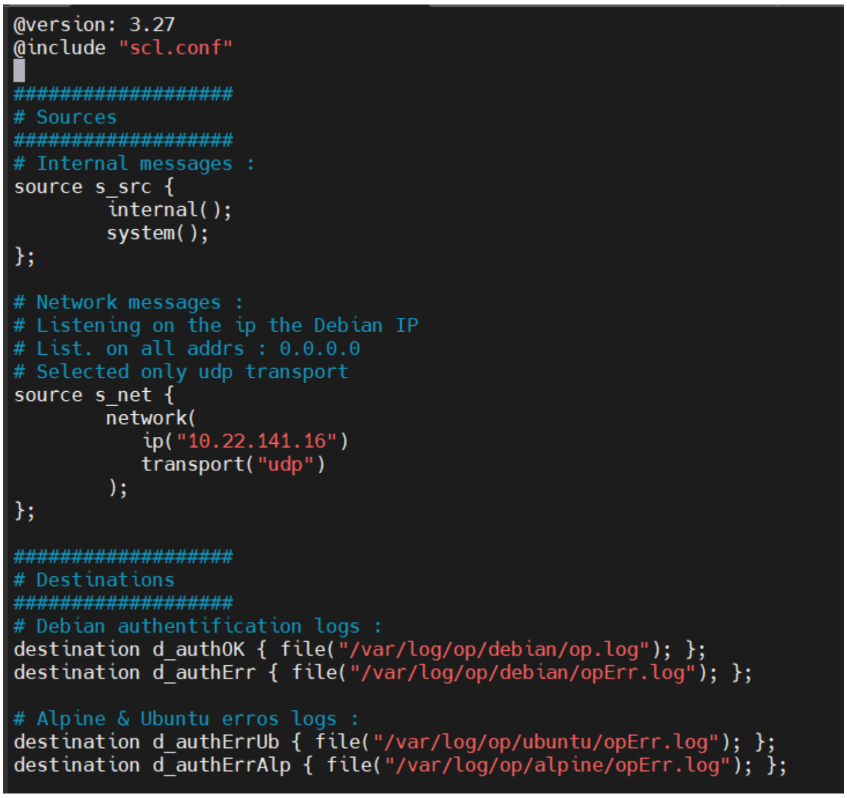
➔ *sudo apt install syslog-ng*

2. Logs management – Edit config files (/etc/syslog-ng/syslog-ng.conf)

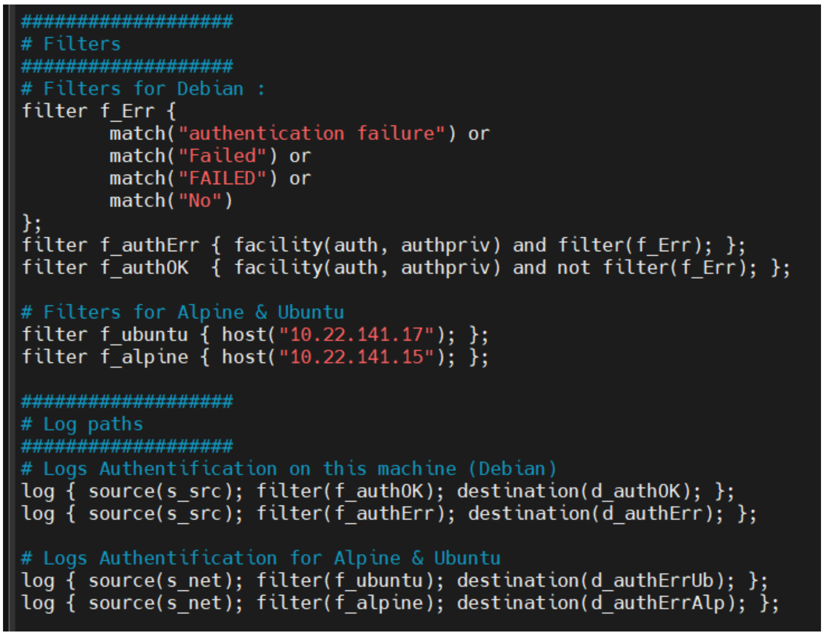
- Debian : log authentication (local, sudo, ssh, su) for success and errors & logs authentication errors from alpine and ubuntu machines
- Ubuntu : log authentication (local, sudo, ssh, su) for success only
- Alpine : log authentication (local, sudo, ssh, su) for success only



2. Syslog-ng config file on Debian

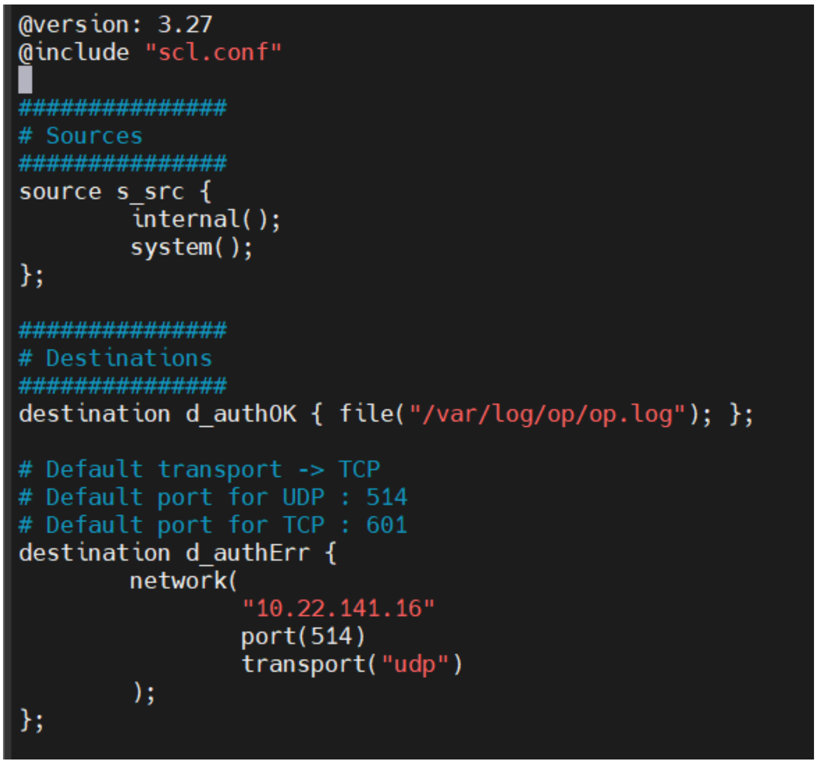


```
@version: 3.27
@include "scl.conf"

###################
# Sources
###################
# Internal messages :
source s_src {
        internal();
        system();
};

# Network messages :
# Listening on the ip the Debian IP
# List. on all addrs : 0.0.0.0
# Selected only udp transport
source s_net {
        network(
           ip("10.22.141.16")
           transport("udp")
        );
};

###################
# Destinations
###################
# Debian authentification logs :
destination d_authOK { file("/var/log/op/debian/op.log"); };
destination d_authErr { file("/var/log/op/debian/opErr.log"); };

# Alpine & Ubuntu erros logs :
destination d_authErrUb { file("/var/log/op/ubuntu/opErr.log"); };
destination d_authErrAlp { file("/var/log/op/alpine/opErr.log"); };
```

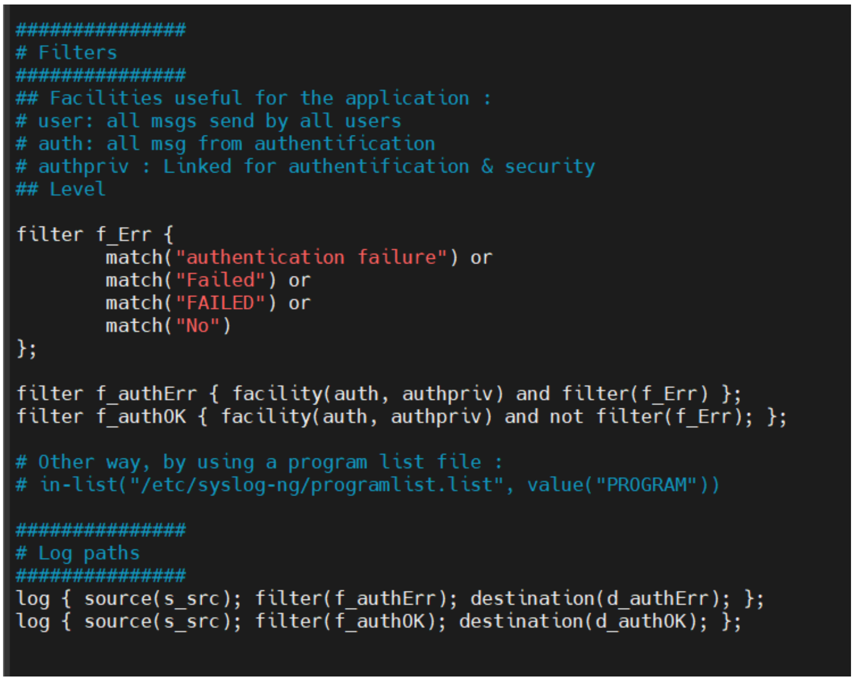


```
###################
# Filters
###################
# Filters for Debian :
filter f_Err {
        match("authentication failure") or
        match("Failed") or
        match("FAILED") or
        match("No")
};
filter f_authErr { facility(auth, authpriv) and filter(f_Err); };
filter f_authOK  { facility(auth, authpriv) and not filter(f_Err); };

# Filters for Alpine & Ubuntu
filter f_ubuntu { host("10.22.141.17"); };
filter f_alpine { host("10.22.141.15"); };

###################
# Log paths
###################
# Logs Authentification on this machine (Debian)
log { source(s_src); filter(f_authOK); destination(d_authOK); };
log { source(s_src); filter(f_authErr); destination(d_authErr); };

# Logs Authentification for Alpine & Ubuntu
log { source(s_net); filter(f_ubuntu); destination(d_authErrUb); };
log { source(s_net); filter(f_alpine); destination(d_authErrAlp); };
```

2. Syslog-ng config file on Ubuntu

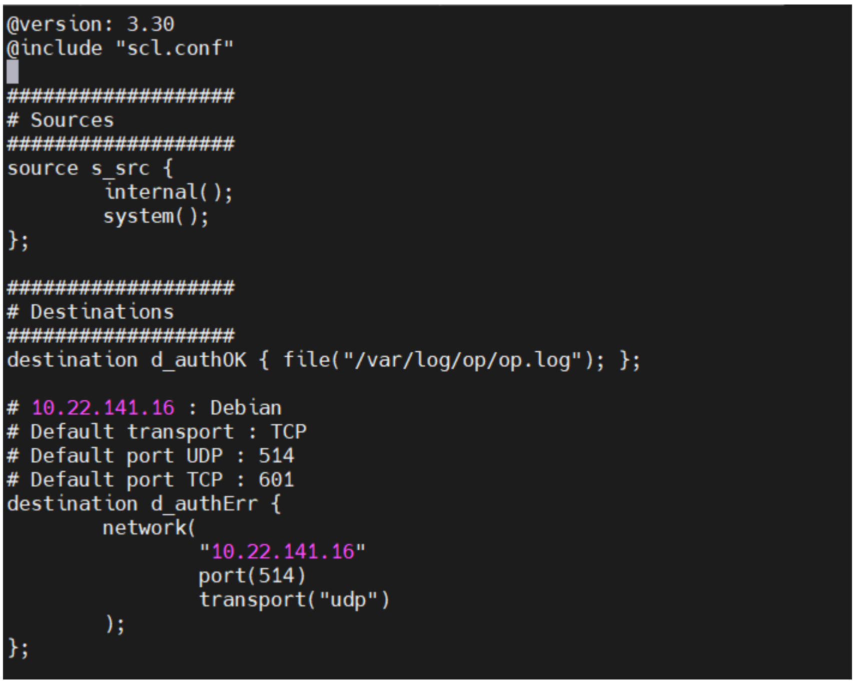


```
@version: 3.27
@include "scl.conf"

###############
# Sources
###############
source s_src {
        internal();
        system();
};

###############
# Destinations
###############
destination d_authOK { file("/var/log/op/op.log"); };

# Default transport -> TCP
# Default port for UDP : 514
# Default port for TCP : 601
destination d_authErr {
        network(
                "10.22.141.16"
                port(514)
                transport("udp")
        );
};
```

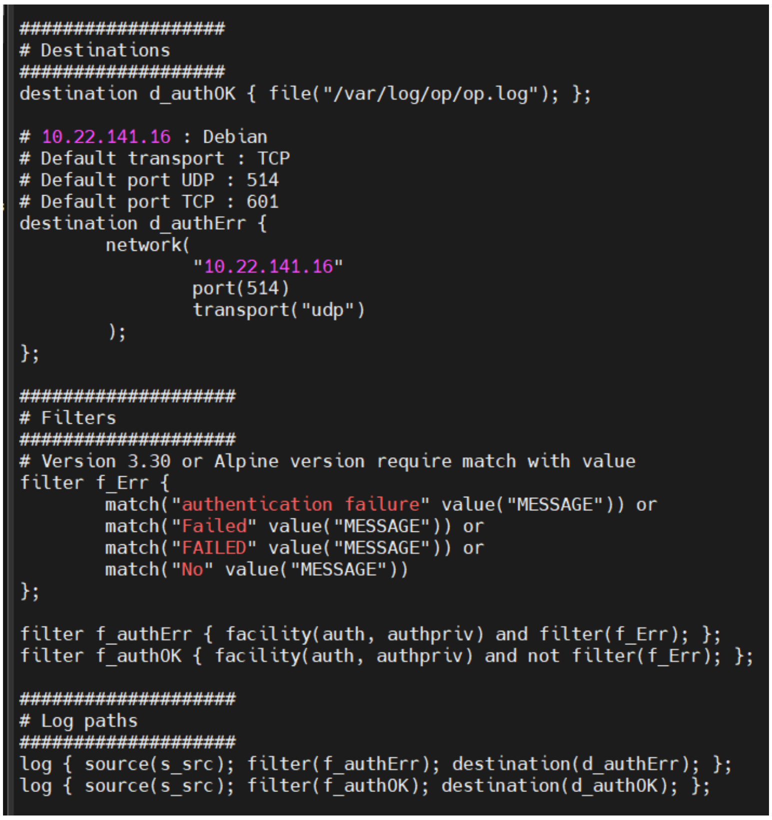


```
###############
# Filters
###############
## Facilities useful for the application :
# user: all msgs send by all users
# auth: all msg from authentification
# authpriv : Linked for authentification & security
## Level

filter f_Err {
        match("authentication failure") or
        match("Failed") or
        match("FAILED") or
        match("No")
};

filter f_authErr { facility(auth, authpriv) and filter(f_Err) };
filter f_authOK { facility(auth, authpriv) and not filter(f_Err); };

# Other way, by using a program list file :
# in-list("/etc/syslog-ng/programlist.list", value("PROGRAM"))

###############
# Log paths
###############
log { source(s_src); filter(f_authErr); destination(d_authErr); };
log { source(s_src); filter(f_authOK); destination(d_authOK); };
```

2. Syslog-ng config file on Alpine



```
@version: 3.30
@include "scl.conf"

###################
# Sources
###################
source s_src {
        internal();
        system();
};

###################
# Destinations
###################
destination d_authOK { file("/var/log/op/op.log"); };

# 10.22.141.16 : Debian
# Default transport : TCP
# Default port UDP : 514
# Default port TCP : 601
destination d_authErr {
        network(
                "10.22.141.16"
                port(514)
                transport("udp")
        );
};
```



```
###################
# Destinations
###################
destination d_authOK { file("/var/log/op/op.log"); };

# 10.22.141.16 : Debian
# Default transport : TCP
# Default port UDP : 514
# Default port TCP : 601
destination d_authErr {
        network(
                "10.22.141.16"
                port(514)
                transport("udp")
        );
};

####################
# Filters
####################
# Version 3.30 or Alpine version require match with value
filter f_Err {
        match("authentication failure" value("MESSAGE")) or
        match("Failed" value("MESSAGE")) or
        match("FAILED" value("MESSAGE")) or
        match("No" value("MESSAGE"))
};

filter f_authErr { facility(auth, authpriv) and filter(f_Err); };
filter f_authOK { facility(auth, authpriv) and not filter(f_Err); };

####################
# Log paths
####################
log { source(s_src); filter(f_authErr); destination(d_authErr); };
log { source(s_src); filter(f_authOK); destination(d_authOK); };
```

3. Update services

3. Update service on Debian

➔ *sudo systemctl restart syslog-ng.service*

3. Update service on Ubuntu

➔ *sudo systemctl restart syslog-ng.service*

3. Update service on Alpine

➔ *sudo service syslog-ng restart*

II. SNMP

4. Installation SNMP

4. NMS installation on Ubuntu

➔ *sudo apt-get install snmp*

The snmp package provides a collection of command line tools for issuing SNMP requests to agents.

➔ *sudo apt-get install snmp snmp-mibs-downloader*

The snmp-mibs-downloader package will help to install and manage Management Information Base (MIB) files, which keep track of network objects.

➔ *sudo download-mibs*

5. Agent installation on Ubuntu

➔ *sudo apt-get install snmpd*

4. Agent installation on the MD Debian

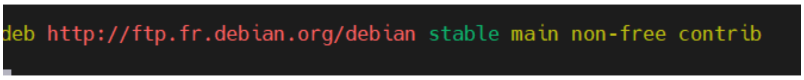
➔ *sudo apt-get install snmpd*

Note that you do not need the snmp-mibs-downloader package, since the agent server will not be managing MIB files.

5. NMS installation on Debian

➔ *sudo apt-get install snmp*

➔ *Add the non-free repository in /etc/apt/sources.list*



```
deb http://ftp.fr.debian.org/debian stable main non-free contrib
```

➔ *sudo apt update*

➔ *sudo apt-get install snmp-mibs-downloader*

➔ *sudo download-mibs*

4. Agent installation on Alpine

- ➔ *sudo apk add net-snmp*
- ➔ *sudo apk add net-snmp-agent-libs*

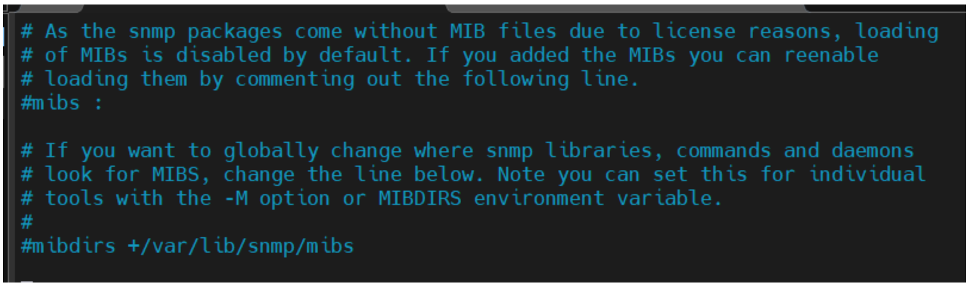
5. Configuration SNMP

6. NMS configuration

Most of the bulk of the work happens in the agent server, so the configuration on the manager server will be less involved. We just need to modify one file to make sure that SNMP tools can use the extra MIB data we installed.

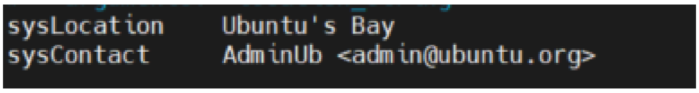
On ubuntu : /etc/snmp/snmp.conf

In this file, there are a few comments and a single un-commented line. To allow the manager to import the MIB files, comment out the mibs : line

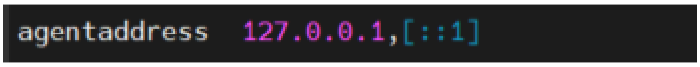


```
# As the snmp packages come without MIB files due to license reasons, loading
# of MIBs is disabled by default. If you added the MIBs you can reenable
# loading them by commenting out the following line.
#mibs :

# If you want to globally change where snmp libraries, commands and daemons
# look for MIBS, change the line below. Note you can set this for individual
# tools with the -M option or MIBDIRS environment variable.
#
#mibdirs +/var/lib/snmp/mibs
```

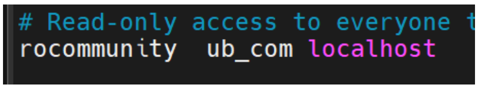
7. Agent configuration (local monitoring)



```
sysLocation    Ubuntu's Bay
sysContact     AdminUb <admin@ubuntu.org>
```



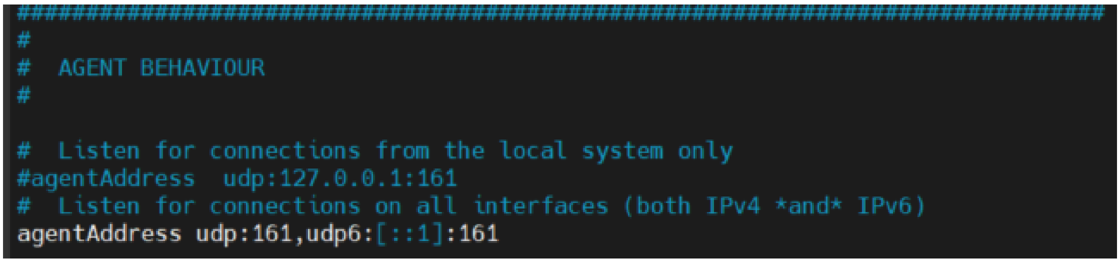
```
agentaddress  127.0.0.1,[::1]
```



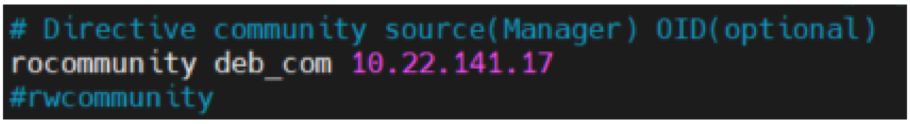
```
# Read-only access to everyone t
rocommunity  ub_com localhost
```

6. Agent configuration

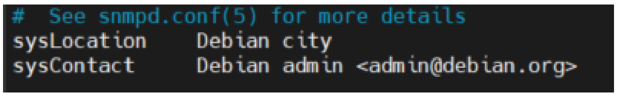
➔ comment in the agent address used for local system & comment out the last line



```
###############################################################################
#
#  AGENT BEHAVIOUR
#

#  Listen for connections from the local system only
#agentAddress  udp:127.0.0.1:161
#  Listen for connections on all interfaces (both IPv4 *and* IPv6)
agentAddress udp:161,udp6:[::1]:161
```



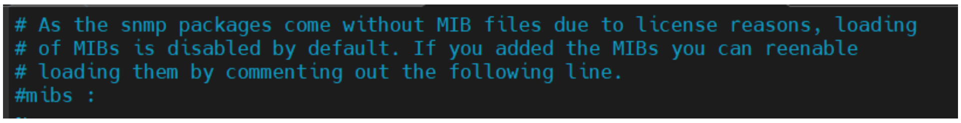
```
# Directive community source(Manager) OID(optional)
rocommunity deb_com 10.22.141.17
#rwcommunity
```



```
#  See snmpd.conf(5) for more details
sysLocation    Debian city
sysContact     Debian admin <admin@debian.org>
```

7. NMS configuration on Debian

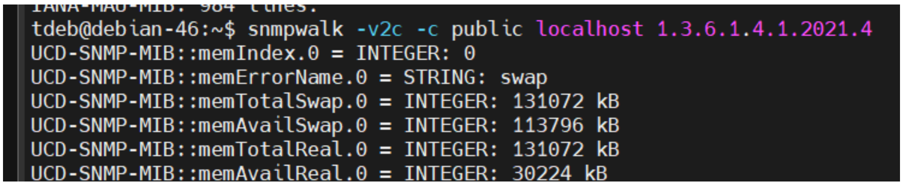
➔ *Comment out the last line of the file /etc/snmp/snmp.conf*



```
# As the snmp packages come without MIB files due to license reasons, loading
# of MIBs is disabled by default. If you added the MIBs you can reenable
# loading them by commenting out the following line.
#mibs :
```

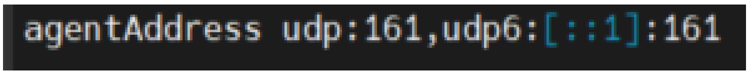
➔ *sudo systemctl restart snmpd.service*

➔ *(For testing) snmpwalk -v2c -c public localhost 1.3.6.1.4.1.2021.4*

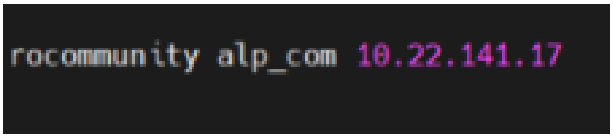


```
IANA-MAU-MIB: 984 lines.
tdeb@debian-46:~$ snmpwalk -v2c -c public localhost 1.3.6.1.4.1.2021.4
UCD-SNMP-MIB::memIndex.0 = INTEGER: 0
UCD-SNMP-MIB::memErrorName.0 = STRING: swap
UCD-SNMP-MIB::memTotalSwap.0 = INTEGER: 131072 kB
UCD-SNMP-MIB::memAvailSwap.0 = INTEGER: 113796 kB
UCD-SNMP-MIB::memTotalReal.0 = INTEGER: 131072 kB
UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 30224 kB
```

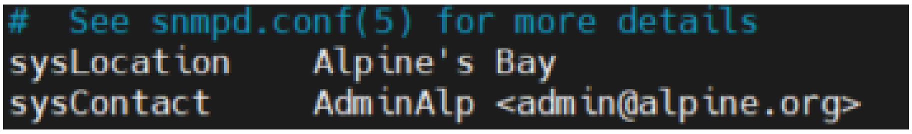
5. Agent configuration



```
agentAddress udp:161,udp6:[::1]:161
```



```
rocommunity alp_com 10.22.141.17
```



```
#  See snmpd.conf(5) for more details
sysLocation    Alpine's Bay
sysContact     AdminAlp <admin@alpine.org>
```

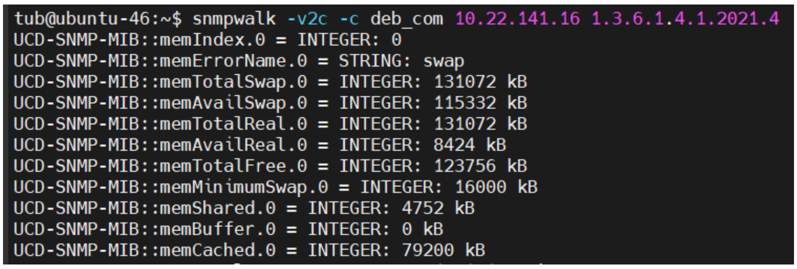
6. Get memory and CPU's charge & percentage disk used

8. NMS get information from Debian

- *Example memory information :*

```
$ snmpwalk -v 2c -c xxxxxxxxxx localhost Memory
UCD-SNMP-MIB::memIndex.0 = INTEGER: 0
UCD-SNMP-MIB::memErrorName.0 = STRING: swap
UCD-SNMP-MIB::memTotalSwap.0 = INTEGER: 8388600
UCD-SNMP-MIB::memAvailSwap.0 = INTEGER: 8388600
UCD-SNMP-MIB::memTotalReal.0 = INTEGER: 8174656
UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 6446020
UCD-SNMP-MIB::memTotalFree.0 = INTEGER: 14834620
UCD-SNMP-MIB::memMinimumSwap.0 = INTEGER: 16000
UCD-SNMP-MIB::memShared.0 = INTEGER: 0
UCD-SNMP-MIB::memBuffer.0 = INTEGER: 42552
UCD-SNMP-MIB::memCached.0 = INTEGER: 285616
UCD-SNMP-MIB::memSwapError.0 = INTEGER: 0
UCD-SNMP-MIB::memSwapErrorMsg.0 = STRING:
```

- *Memory information :*

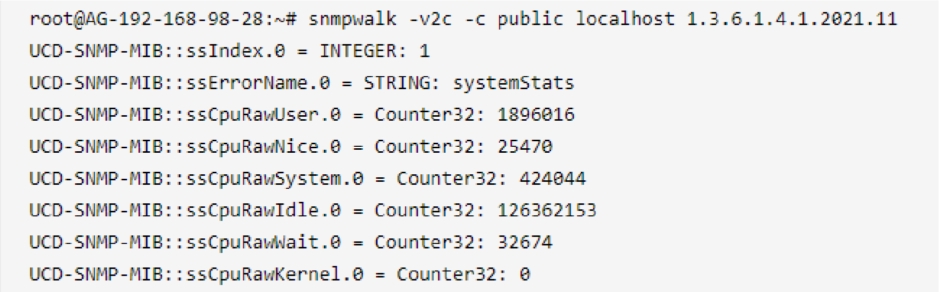


```
tub@ubuntu-46:~$ snmpwalk -v2c -c deb_com 10.22.141.16 1.3.6.1.4.1.2021.4
UCD-SNMP-MIB::memIndex.0 = INTEGER: 0
UCD-SNMP-MIB::memErrorName.0 = STRING: swap
UCD-SNMP-MIB::memTotalSwap.0 = INTEGER: 131072 kB
UCD-SNMP-MIB::memAvailSwap.0 = INTEGER: 115332 kB
UCD-SNMP-MIB::memTotalReal.0 = INTEGER: 131072 kB
UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 8424 kB
UCD-SNMP-MIB::memTotalFree.0 = INTEGER: 123756 kB
UCD-SNMP-MIB::memMinimumSwap.0 = INTEGER: 16000 kB
UCD-SNMP-MIB::memShared.0 = INTEGER: 4752 kB
UCD-SNMP-MIB::memBuffer.0 = INTEGER: 0 kB
UCD-SNMP-MIB::memCached.0 = INTEGER: 79200 kB
```

➔ *Memory load :*

- *memTotal = memTotalReal*
  - *131072 -> 128.00 MiB*
- *memTotalFree = memAvailReal + memBuffer + memCached*
  - *8424 + 0 + 79200 = 87624 -> 85.57 MiB*
- *memUsed = memTotal - memTotalFree*
  - *128 – 85.57 = 42.43 MiB*
- *memLoad = (memUsed / memTotal) x 100*
  - *(42.43 / 128) x 100 = 33.15 %*

- *Example CPU information*
  - *CPU times :*

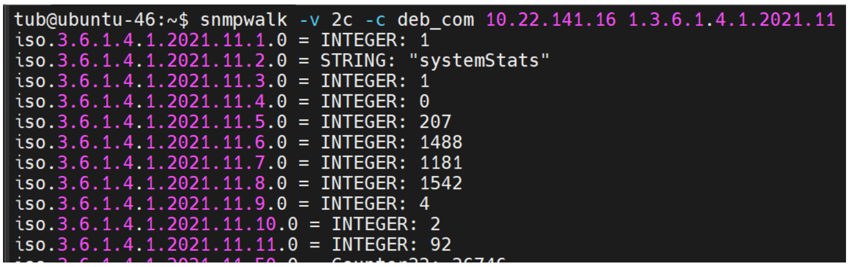


```
root@AG-192-168-98-28:~# snmpwalk -v2c -c public localhost 1.3.6.1.4.1.2021.11
UCD-SNMP-MIB::ssIndex.0 = INTEGER: 1
UCD-SNMP-MIB::ssErrorName.0 = STRING: systemStats
UCD-SNMP-MIB::ssCpuRawUser.0 = Counter32: 1896016
UCD-SNMP-MIB::ssCpuRawNice.0 = Counter32: 25470
UCD-SNMP-MIB::ssCpuRawSystem.0 = Counter32: 424044
UCD-SNMP-MIB::ssCpuRawIdle.0 = Counter32: 126362153
UCD-SNMP-MIB::ssCpuRawWait.0 = Counter32: 32674
UCD-SNMP-MIB::ssCpuRawKernel.0 = Counter32: 0
```

- *CPU loads*

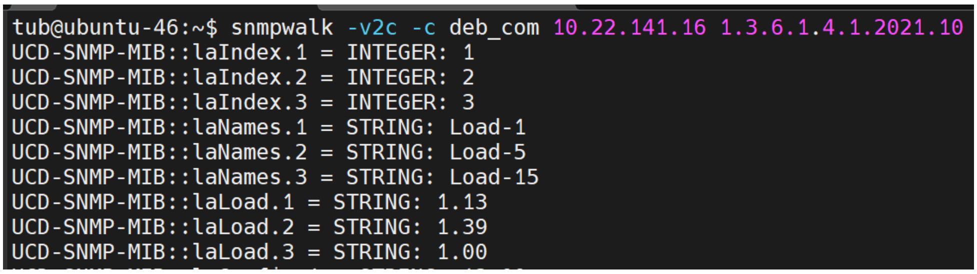
Load
1 minute Load: .1.3.6.1.4.1.2021.10.1.3.1
5 minute Load: .1.3.6.1.4.1.2021.10.1.3.2
15 minute Load: .1.3.6.1.4.1.2021.10.1.3.3

- *CPU information*
  - *CPU times*



```
tub@ubuntu-46:~$ snmpwalk -v 2c -c deb_com 10.22.141.16 1.3.6.1.4.1.2021.11
iso.3.6.1.4.1.2021.11.1.0 = INTEGER: 1
iso.3.6.1.4.1.2021.11.2.0 = STRING: "systemStats"
iso.3.6.1.4.1.2021.11.3.0 = INTEGER: 1
iso.3.6.1.4.1.2021.11.4.0 = INTEGER: 0
iso.3.6.1.4.1.2021.11.5.0 = INTEGER: 207
iso.3.6.1.4.1.2021.11.6.0 = INTEGER: 1488
iso.3.6.1.4.1.2021.11.7.0 = INTEGER: 1181
iso.3.6.1.4.1.2021.11.8.0 = INTEGER: 1542
iso.3.6.1.4.1.2021.11.9.0 = INTEGER: 4
iso.3.6.1.4.1.2021.11.10.0 = INTEGER: 2
iso.3.6.1.4.1.2021.11.11.0 = INTEGER: 92
iso.3.6.1.4.1.2021.11.50.0 = Counter32: 26746
```

  - *CPU Loads*

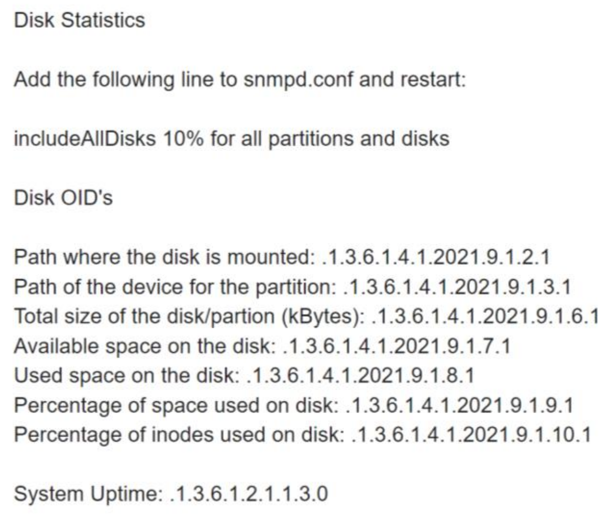


```
tub@ubuntu-46:~$ snmpwalk -v2c -c deb_com 10.22.141.16 1.3.6.1.4.1.2021.10
UCD-SNMP-MIB::laIndex.1 = INTEGER: 1
UCD-SNMP-MIB::laIndex.2 = INTEGER: 2
UCD-SNMP-MIB::laIndex.3 = INTEGER: 3
UCD-SNMP-MIB::laNames.1 = STRING: Load-1
UCD-SNMP-MIB::laNames.2 = STRING: Load-5
UCD-SNMP-MIB::laNames.3 = STRING: Load-15
UCD-SNMP-MIB::laLoad.1 = STRING: 1.13
UCD-SNMP-MIB::laLoad.2 = STRING: 1.39
UCD-SNMP-MIB::laLoad.3 = STRING: 1.00
```

➔ *CPU Loads (1 CPU on Proxmox):*

  - *1 min : During the last minute, the CPU was overloaded by 13 % (1 CPU with 1.13 runnable processes, so that 0.13 processes had to wait for a turn)*
  - *5 min : During the last 5 minutes, the CPU was overloaded by 39 % (1 CPU with 1.39 runnable processes, so that 0.39 processes had to wait for a turn)*
  - *15 min : During the last 15 minutes, the CPU was loaded by 0 % (1 CPU with 1.00 runnable processes, so that 0 processes had to wait for a turn)*

- *Example Disk used*



Disk Statistics

Add the following line to snmpd.conf and restart:

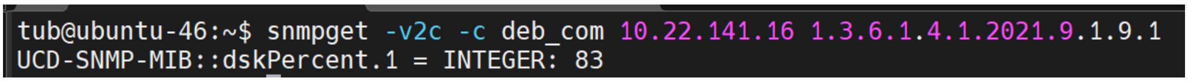
includeAllDisks 10% for all partitions and disks

Disk OID's

Path where the disk is mounted: .1.3.6.1.4.1.2021.9.1.2.1
Path of the device for the partition: .1.3.6.1.4.1.2021.9.1.3.1
Total size of the disk/partion (kBytes): .1.3.6.1.4.1.2021.9.1.6.1
Available space on the disk: .1.3.6.1.4.1.2021.9.1.7.1
Used space on the disk: .1.3.6.1.4.1.2021.9.1.8.1
Percentage of space used on disk: .1.3.6.1.4.1.2021.9.1.9.1
Percentage of inodes used on disk: .1.3.6.1.4.1.2021.9.1.10.1

System Uptime: .1.3.6.1.2.1.1.3.0

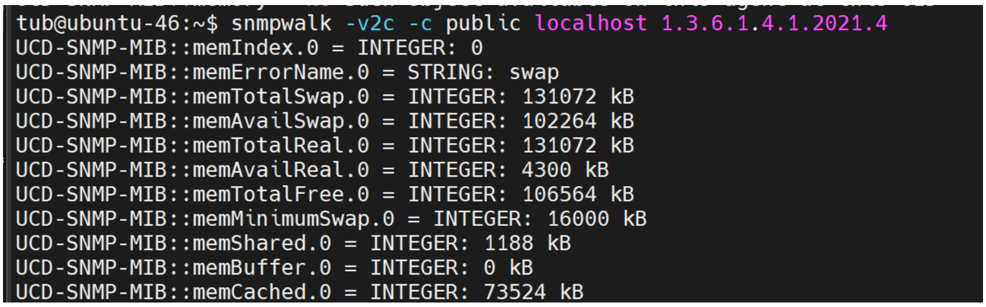
- *Disk used*



```
tub@ubuntu-46:~$ snmpget -v2c -c deb_com 10.22.141.16 1.3.6.1.4.1.2021.9.1.9.1
UCD-SNMP-MIB::dskPercent.1 = INTEGER: 83
```

➔ *disk used : 83 %*

9. NMS get information from Ubuntu

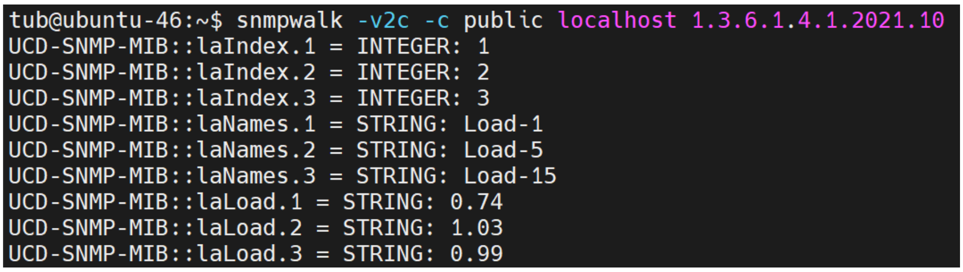


```
tub@ubuntu-46:~$ snmpwalk -v2c -c public localhost 1.3.6.1.4.1.2021.4
UCD-SNMP-MIB::memIndex.0 = INTEGER: 0
UCD-SNMP-MIB::memErrorName.0 = STRING: swap
UCD-SNMP-MIB::memTotalSwap.0 = INTEGER: 131072 kB
UCD-SNMP-MIB::memAvailSwap.0 = INTEGER: 102264 kB
UCD-SNMP-MIB::memTotalReal.0 = INTEGER: 131072 kB
UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 4300 kB
UCD-SNMP-MIB::memTotalFree.0 = INTEGER: 106564 kB
UCD-SNMP-MIB::memMinimumSwap.0 = INTEGER: 16000 kB
UCD-SNMP-MIB::memShared.0 = INTEGER: 1188 kB
UCD-SNMP-MIB::memBuffer.0 = INTEGER: 0 kB
UCD-SNMP-MIB::memCached.0 = INTEGER: 73524 kB
```

➔ *Memory load :*

- *memTotal = memTotalReal*
  - *131072 -> 128.00 MiB*
- *memTotalFree = memAvailReal + memBuffer + memCached*
  - *4300 + 0 + 73524 = 77824 -> 76 MiB*
- *memUsed = memTotal - memTotalFree*
  - *128 – 76 = 52 MiB*
- *memLoad = (memUsed / memTotal) x 100*
  - *(52 / 128) x 100 = 40.62 %*

➔ *CPU Loads (1 CPU on Proxmox):*



```
tub@ubuntu-46:~$ snmpwalk -v2c -c public localhost 1.3.6.1.4.1.2021.10
UCD-SNMP-MIB::laIndex.1 = INTEGER: 1
UCD-SNMP-MIB::laIndex.2 = INTEGER: 2
UCD-SNMP-MIB::laIndex.3 = INTEGER: 3
UCD-SNMP-MIB::laNames.1 = STRING: Load-1
UCD-SNMP-MIB::laNames.2 = STRING: Load-5
UCD-SNMP-MIB::laNames.3 = STRING: Load-15
UCD-SNMP-MIB::laLoad.1 = STRING: 0.74
UCD-SNMP-MIB::laLoad.2 = STRING: 1.03
UCD-SNMP-MIB::laLoad.3 = STRING: 0.99
```

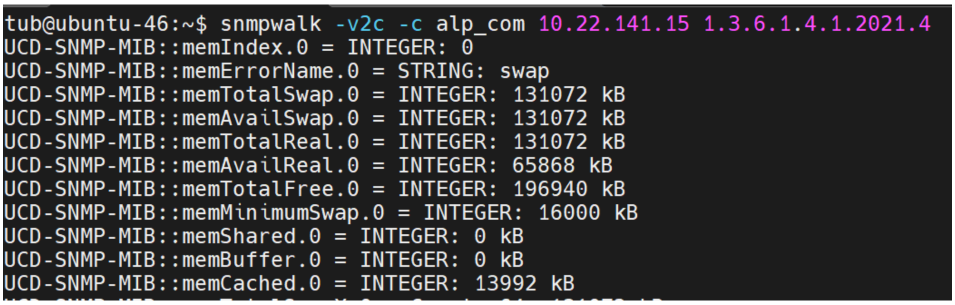
- *1 min : During the last minute, the CPU was underloaded 74% (no processes had to wait for a turn)*
- *5 min : During the last 5 minutes, the CPU was overloaded by 3 % (1 CPU with 1.03 runnable processes, so that 0.3 processes had to wait for a turn)*
- *15 min : During the last 15 minutes, the CPU was underloaded by 99 % (no processes had to wait for a turn)*

➔ *Disk used*

…

10. NMS get information from Alpine

- *Memory information :*

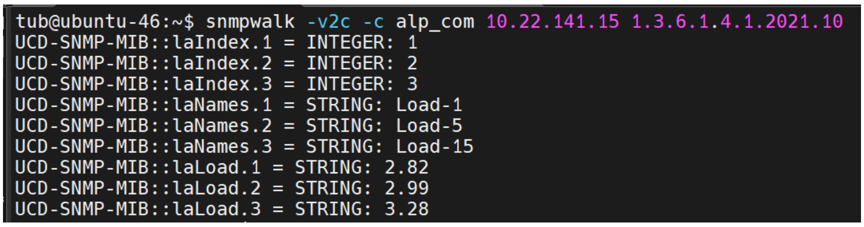


```
tub@ubuntu-46:~$ snmpwalk -v2c -c alp_com 10.22.141.15 1.3.6.1.4.1.2021.4
UCD-SNMP-MIB::memIndex.0 = INTEGER: 0
UCD-SNMP-MIB::memErrorName.0 = STRING: swap
UCD-SNMP-MIB::memTotalSwap.0 = INTEGER: 131072 kB
UCD-SNMP-MIB::memAvailSwap.0 = INTEGER: 131072 kB
UCD-SNMP-MIB::memTotalReal.0 = INTEGER: 131072 kB
UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 65868 kB
UCD-SNMP-MIB::memTotalFree.0 = INTEGER: 196940 kB
UCD-SNMP-MIB::memMinimumSwap.0 = INTEGER: 16000 kB
UCD-SNMP-MIB::memShared.0 = INTEGER: 0 kB
UCD-SNMP-MIB::memBuffer.0 = INTEGER: 0 kB
UCD-SNMP-MIB::memCached.0 = INTEGER: 13992 kB
```

➔ *Memory load :*

- *memTotal = memTotalReal*
  - *131072 -> 128.00 MiB*
- *memTotalFree = memAvailReal + memBuffer + memCached*
  - *65868 + 0 + 13992 = 79860 -> 76.16 MiB*
- *memUsed = memTotal - memTotalFree*
  - *128 – 76.16 = 51.84 MiB*
- *memLoad = (memUsed / memTotal) x 100*
  - *(51.84 / 128) x 100 = 40.50 %*

➔ *CPU Loads (1 CPU on Proxmox):*



```
tub@ubuntu-46:~$ snmpwalk -v2c -c alp_com 10.22.141.15 1.3.6.1.4.1.2021.10
UCD-SNMP-MIB::laIndex.1 = INTEGER: 1
UCD-SNMP-MIB::laIndex.2 = INTEGER: 2
UCD-SNMP-MIB::laIndex.3 = INTEGER: 3
UCD-SNMP-MIB::laNames.1 = STRING: Load-1
UCD-SNMP-MIB::laNames.2 = STRING: Load-5
UCD-SNMP-MIB::laNames.3 = STRING: Load-15
UCD-SNMP-MIB::laLoad.1 = STRING: 2.82
UCD-SNMP-MIB::laLoad.2 = STRING: 2.99
UCD-SNMP-MIB::laLoad.3 = STRING: 3.28
```

- *1 min : During the last minute, the CPU was overloaded 182% (1 CPU with 2.82 runnable processes, so that 2.82 processes had to wait for a turn)*
- *5 min : During the last 5 minutes, the CPU was overloaded 199% (1 CPU with 2.99 runnable processes, so that 2.99 processes had to wait for a turn)*
- *15 min : During the last 15 minutes, the CPU was overloaded 228% (1 CPU with 3.28 runnable processes, so that 2.28 processes had to wait for a turn)*

➔ *Disk used ?*

7. Get list of packets installed and users currently connected