

# Tutorial

En este tutorial se configurará las herramientas de SNMP que nos facilitará la comunicación con un determinado agente configurado de manera local. Nuestro agente cumplirá las órdenes del servidor mediante la ejecución de comandos que nos permitirán la visualización del estado y su rendimiento.

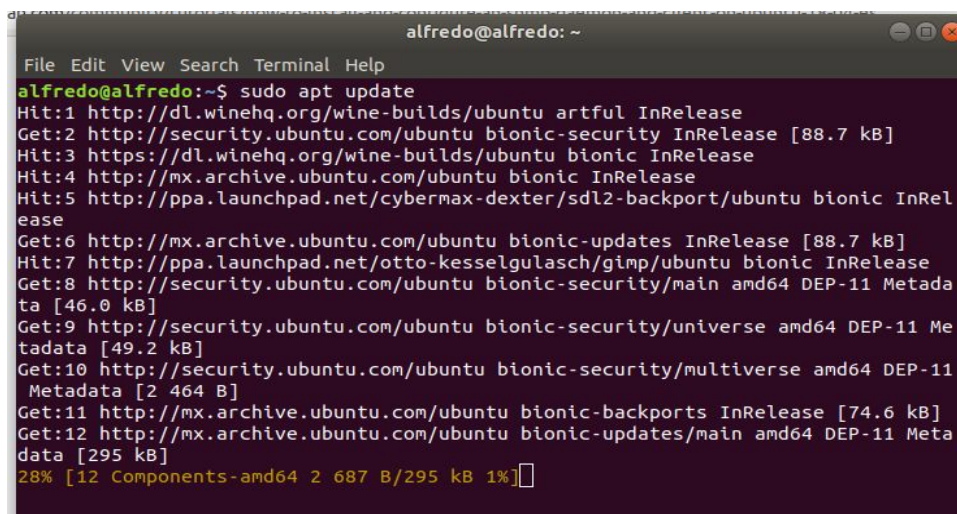
## Requisitos previos

Para este tutorial, necesitará lo siguiente:

- Un servidor Ubuntu 18.04 instalado de manera local.
- Puertos de firewall ufw desactivados.
- Conocimiento de la MIB
- Conocimientos acerca del uso de SNMP

## Configuración de SNMP y MIB

1. Actualice el contenido de los paquetes del administrador apt: `sudo apt update`



```
alfredo@alfredo: ~  
File Edit View Search Terminal Help  
alfredo@alfredo:~$ sudo apt update  
Hit:1 http://dl.winehq.org/wine-builds/ubuntu artful InRelease  
Get:2 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]  
Hit:3 https://dl.winehq.org/wine-builds/ubuntu bionic InRelease  
Hit:4 http://mx.archive.ubuntu.com/ubuntu bionic InRelease  
Hit:5 http://ppa.launchpad.net/cybermax-dexter/sdl2-backport/ubuntu bionic InRelease  
Get:6 http://mx.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]  
Hit:7 http://ppa.launchpad.net/otto-kesselgulasch/gimp/ubuntu bionic InRelease  
Get:8 http://security.ubuntu.com/ubuntu bionic-security/main amd64 DEP-11 Metadata [46.0 kB]  
Get:9 http://security.ubuntu.com/ubuntu bionic-security/universe amd64 DEP-11 Metadata [49.2 kB]  
Get:10 http://security.ubuntu.com/ubuntu bionic-security/multiverse amd64 DEP-11 Metadata [2 464 B]  
Get:11 http://mx.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]  
Get:12 http://mx.archive.ubuntu.com/ubuntu bionic-updates/main amd64 DEP-11 Metadata [295 kB]  
28% [12 Components-amd64 2 687 B/295 kB 1%]
```

*Imagen 1. Actualización.*

2. Escribiremos en nuestra línea de comandos las siguientes instrucciones: `sudo apt install snmp snmp-mibs-downloader`. Que nos podrá permitir trabajar con los objetos de la MIB devueltas por nuestras consultas del sistema.

```
alfredo@alfredo: ~  
File Edit View Search Terminal Help  
nvm is not compatible with the npm config "prefix" option: currently set to "/home/alfredo/.npm-global"  
Run 'npm config delete prefix' or 'nvm use --delete-prefix v13.7.0 --silent' to unset it.  
alfredo@alfredo:~$ sudo apt install snmp snmp-mibs-downloader  
[sudo] password for alfredo:  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  linux-headers-5.3.0-53 linux-headers-5.3.0-53-generic  
  linux-image-5.3.0-53-generic linux-modules-5.3.0-53-generic  
  linux-modules-extra-5.3.0-53-generic  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
  smstrip  
The following NEW packages will be installed:  
  smstrip snmp snmp-mibs-downloader  
0 upgraded, 3 newly installed, 0 to remove and 31 not upgraded.  
Need to get 5 330 kB of archives.  
After this operation, 5 914 kB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

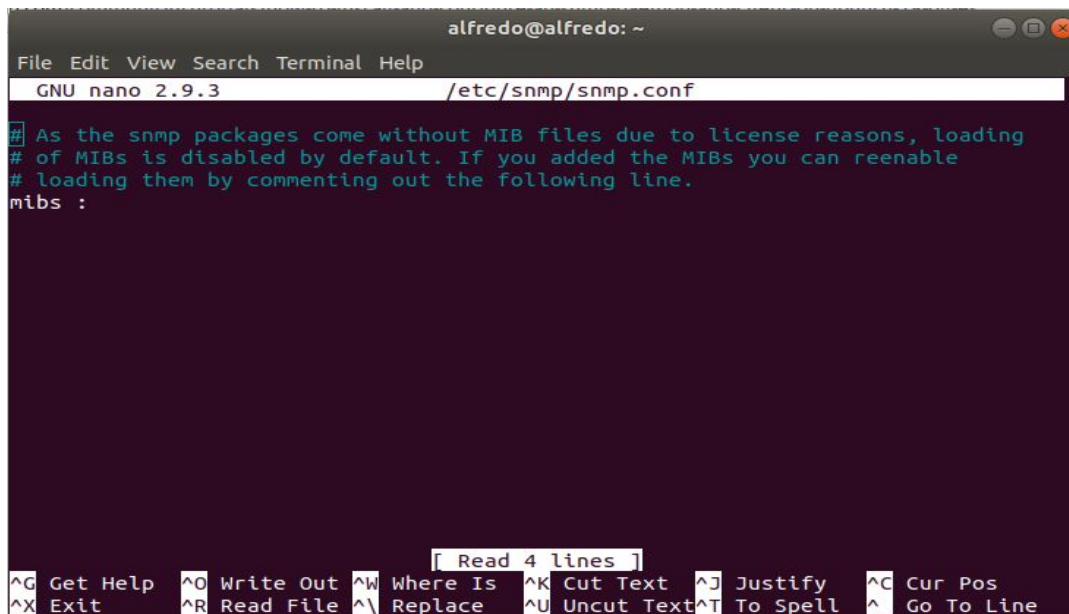
*Imagen 2. Descarga de la MIB.*

3. A continuación instalaremos el paquete snmp, el cual aporta un paquete de comandos para emitir solicitudes tipo snmp a los agentes del sistema. La instrucción snmp-mibs-downloader nos permitirá la administración de los archivos de la MIB, que realizan un seguimiento de los objetos que se hayan en nuestra red.

```
alfredo@alfredo: ~  
File Edit View Search Terminal Help  
alfredo@alfredo:~$ sudo apt install snmpd  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  linux-headers-5.3.0-53 linux-headers-5.3.0-53-generic  
  linux-image-5.3.0-53-generic linux-modules-5.3.0-53-generic  
  linux-modules-extra-5.3.0-53-generic  
Use 'sudo apt autoremove' to remove them.  
Suggested packages:  
  snmptrapd  
The following NEW packages will be installed:  
  snmpd  
0 upgraded, 1 newly installed, 0 to remove and 31 not upgraded.  
Need to get 57.0 kB of archives.  
After this operation, 144 kB of additional disk space will be used.  
Get:1 http://mx.archive.ubuntu.com/ubuntu bionic-updates/main amd64 snmpd amd64  
5.7.3+dfsg-1.8ubuntu3.3 [57.0 kB]  
Fetched 57.0 kB in 0s (121 kB/s)  
[Y]
```

*Imagen 3. Instalación SNMP.*

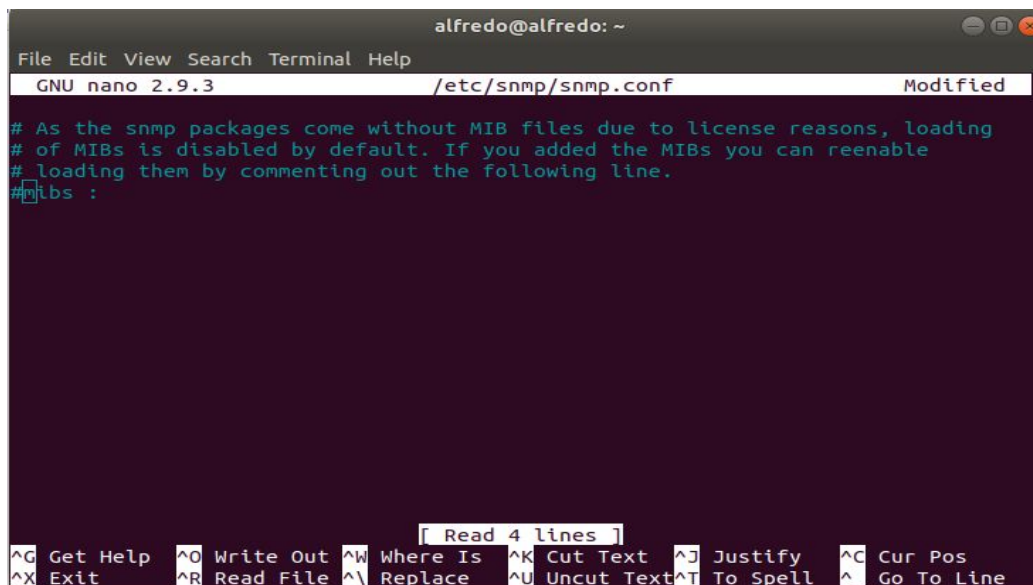
4. Una vez instalada la herramienta procederemos a digitar el siguiente comandos que nos abrirá una ventana como la siguiente. `sudo nano /etc/snmp/snmpd.conf`  
En esta parte usaremos nano para editar el archivo.



```
alfredo@alfredo: ~  
File Edit View Search Terminal Help  
GNU nano 2.9.3 /etc/snmp/snmpd.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 reenale  
# loading them by commenting out the following line.  
mibs :  
  
[ Read 4 lines ]  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos  
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

*Imagen 4. Edición archivo snmpd.conf*

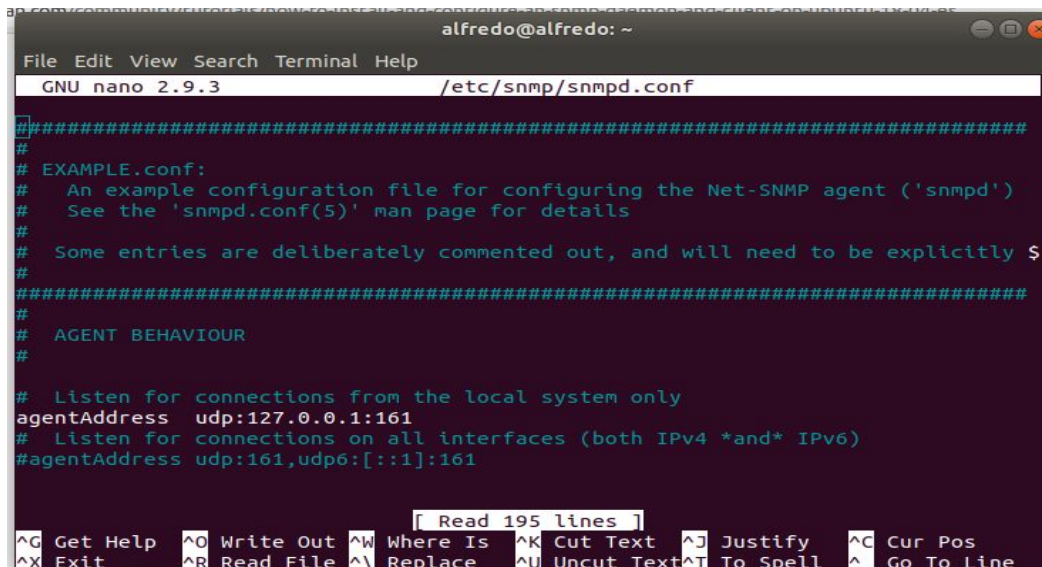
5. Comentamos la línea mibs con el fin de que SNMP reconozca el paquete de MIB que instalamos en el paso número 2.



```
alfredo@alfredo: ~  
File Edit View Search Terminal Help  
GNU nano 2.9.3 /etc/snmp/snmpd.conf Modified  
# 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 reenale  
# loading them by commenting out the following line.  
#mibs :  
  
[ Read 4 lines ]  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos  
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

*Imagen 5. Edición archivo snmpd.conf*

6. Ahora configuraremos el archivo para escuchar tanto en un host local como en una IP de interfaz. De manera predeterminada, el agente SNMP activado está configurado para permitir conexiones que se originan sólo desde el host local. agentAddress udp: 127.0.0.1: 161.



```
alfredo@alfredo: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/snmp/snmpd.conf

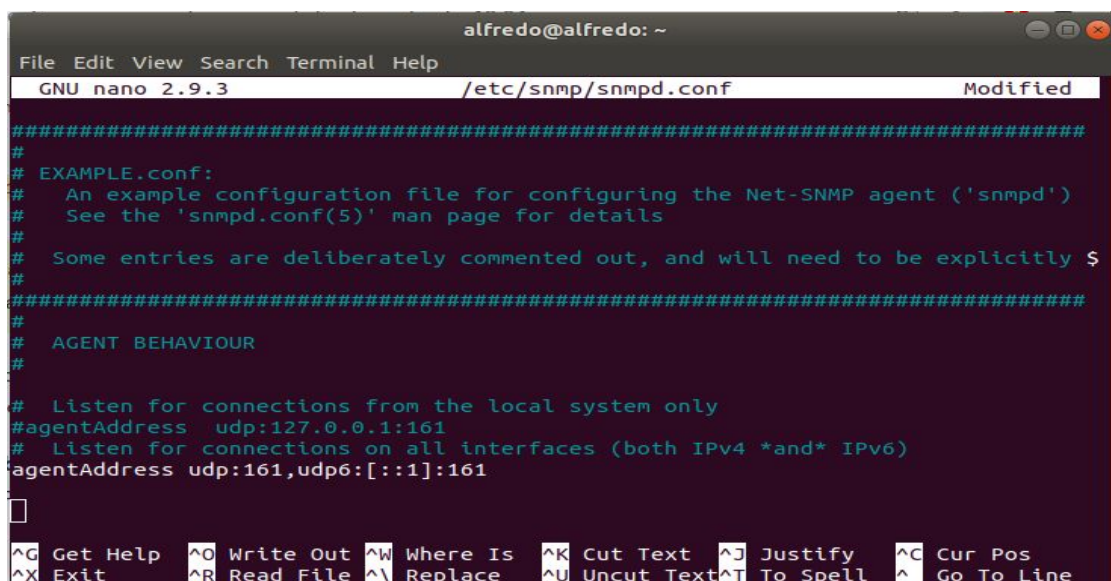
#####
#
# EXAMPLE.conf:
#   An example configuration file for configuring the Net-SNMP agent ('snmpd')
#   See the 'snmpd.conf(5)' man page for details
#
#   Some entries are deliberately commented out, and will need to be explicitly $
#
#####
#
# AGENT BEHAVIOUR
#
# Listen for connections from the local 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

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line

Read 195 lines
```

*Imagen 6. Edición archivo snmpd.conf*

- Comentamos la línea: agentAddress udp: 127.0.0.1: 161. y descomentamos agentAddress udp: 127.0.0.1: 161, udp6:[::1]:161. Las modificaciones se aprecian a continuación.



```
alfredo@alfredo: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/snmp/snmpd.conf Modified

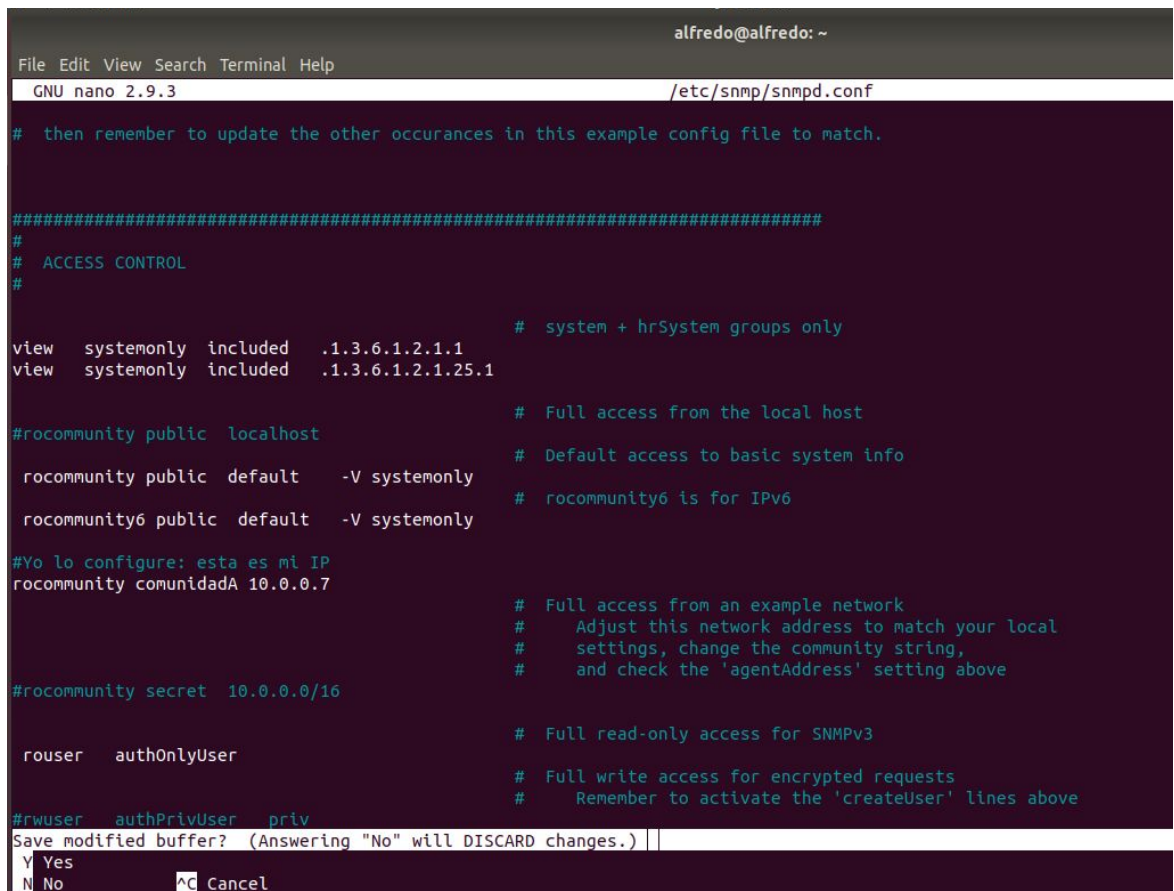
#####
#
# EXAMPLE.conf:
#   An example configuration file for configuring the Net-SNMP agent ('snmpd')
#   See the 'snmpd.conf(5)' man page for details
#
#   Some entries are deliberately commented out, and will need to be explicitly $
#
#####
#
# AGENT BEHAVIOUR
#
# Listen for connections from the local 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

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

*Imagen 7. Edición archivo snmpd.conf*

- Posteriormente, configuraremos el agente que permitirá la detección de solicitudes SNMP. La cadena usada en esta práctica es: comunidadA. Pero puede configurarse con la de su agrado. Es necesario también escribir el puerto desde el cual obtendrá la información nuestro agente. Como lo estamos configurando de manera local escribiremos nuestra IP a continuación del nombre de la comunidad quedando de esta forma: rocommunity [nombre\_de\_la\_comunidad] [direccion\_IP]. Habiendo realizado esto guardamos.





```
alfredo@alfredo: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 /etc/snmp/snmpd.conf

# then remember to update the other occurrences in this example config file to match.

#####
#
# ACCESS CONTROL
#
# system + hrSystem groups only
view systemonly included .1.3.6.1.2.1.1
view systemonly included .1.3.6.1.2.1.25.1

#rocommunity public localhost
# Default access to basic system info
rocommunity public default -V systemonly
# rocommunity6 is for IPv6
rocommunity6 public default -V systemonly

#Yo lo configure: esta es mi IP
rocommunity comunidadA 10.0.0.7

# Full access from an example network
# Adjust this network address to match your local
# settings, change the community string,
# and check the 'agentAddress' setting above
#rocommunity secret 10.0.0.0/16

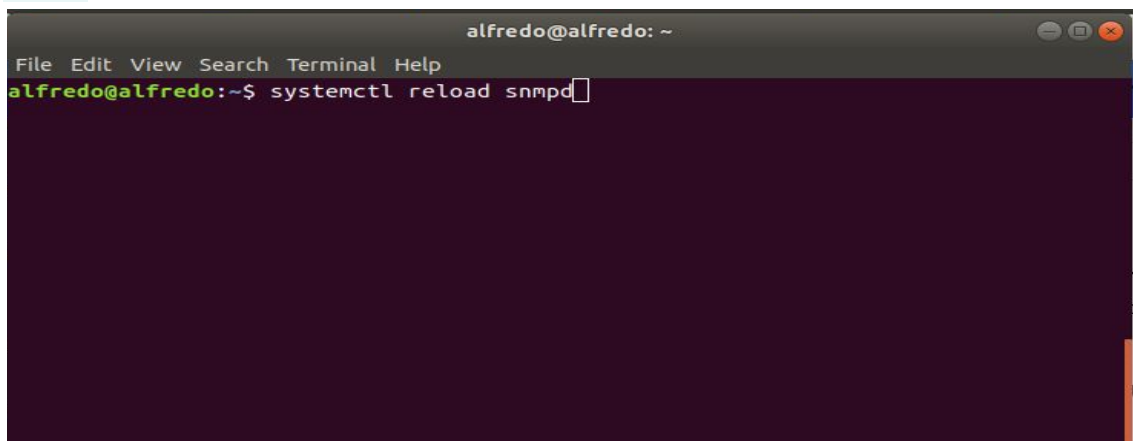
# Full read-only access for SNMPv3
rouser authOnlyUser

# Full write access for encrypted requests
# Remember to activate the 'createUser' lines above
#rwuser authPrivUser priv

Save modified buffer? (Answering "No" will DISCARD changes.)
Y Yes
N No ^C Cancel
```

*Imagen 8. Edición archivo snmpd.conf*

9. Para que los cambios en nuestro sistema se vean reflejados a continuación reiniciaremos el servicio de SNMP con el siguiente comando: `systemctl reload snmpd`



```
alfredo@alfredo: ~
File Edit View Search Terminal Help
alfredo@alfredo:~$ systemctl reload snmpd
```

*Imagen 9. Reinicio del servicio SNMP.*

10. Una vez hecho esto comprobaremos que SNMP esté trabajando en conjunto mediante las MIB's.

**Funcionamiento:**

- Probaremos la MIB: `1.3.6.1.2.1.1.7.0` la cual indica la cantidad de servicios que tiene nuestro sistema operativo.

- Probaremos la MIB: 1.3.6.1.2.1.1.1 mediante un snmpwalk que indica el sistema operativo en el que reside el agente.

A continuación las respuestas:

```
alfredo@alfredo: ~
File Edit View Search Terminal Help
nvm is not compatible with the npm config "prefix" option: currently set to "/home/alfredo/.npm-global"
Run `npm config delete prefix` or `npm use --delete-prefix v13.7.0 --silent` to unset it.
alfredo@alfredo:~$ snmpget -v2c -c comunidadA 10.0.0.7 1.3.6.1.2.1.1.7.0
SNMPv2-MIB::sysServices.0 = INTEGER: 72
alfredo@alfredo:~$ snmpwalk -v1 -c comunidadA 10.0.0.7 1.3.6.1.2.1.1.1
Command 'snmpwalk' not found, did you mean:
  command 'snmpwalk' from deb snmp
Try: sudo apt install <deb name>
alfredo@alfredo:~$ snmpwalk -v1 -c comunidadA 10.0.0.7 1.3.6.1.2.1.1.1
SNMPv2-MIB::sysDescr.0 = STRING: Linux alfredo 5.3.0-61-generic #55~18.04.1-Ubuntu SMP Mon Jun 22 16:40:20 UTC 2020 x86_64
alfredo@alfredo:~$
```

Imagen 10. Respuestas de la MIB.

## Script de monitorización de MIB's

Programa: *getSNMP.py*

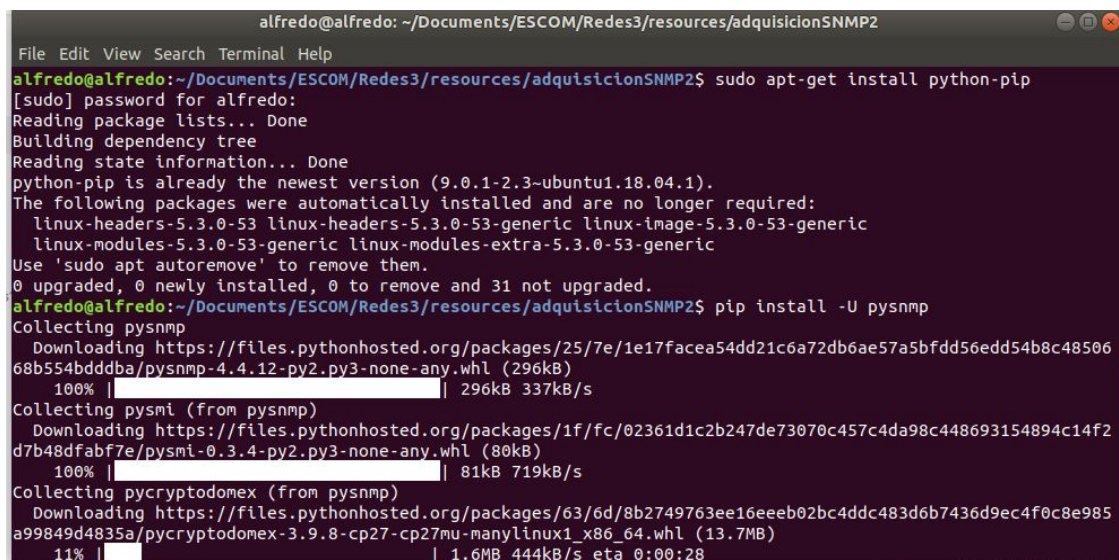
```
1. from pysnmp.hlapi import *
2.
3. def consultaSNMP(comunidad,host,oid):
4.     errorIndication, errorStatus, errorIndex, varBinds = next(
5.         getCmd(SnmpEngine(),
6.                 CommunityData(comunidad),
7.                 UdpTransportTarget((host, 161)),
8.                 ContextData(),
9.                 ObjectType(ObjectIdentity(oid))))
10.
11.     if errorIndication:
12.         print(errorIndication)
13.     elif errorStatus:
14.         print('%s at %s' % (errorStatus.prettyPrint(),errorIndex and
15.                               varBinds[int(errorIndex) - 1][0] or '?'))
16.     else:
17.         for varBind in varBinds:
18.             varB=(' = '.join([x.prettyPrint() for x in varBind]))
19.             resultado = varB.split()[2]
20.     return resultado
```

```

21.
22. def consultaSNMP2(comunidad,host,oid):
23.     errorIndication, errorStatus, errorIndex, varBinds = next(
24.         getCmd(SnmpEngine(),
25.             CommunityData(comunidad),
26.             UdpTransportTarget((host, 161)),
27.             ContextData(),
28.             ObjectType(ObjectIdentity(oid))))
29.
30.     if errorIndication:
31.         print(errorIndication)
32.     elif errorStatus:
33.         print('%s at %s' % (errorStatus.prettyPrint(),errorIndex and
varBinds[int(errorIndex) - 1][0] or '?'))
34.     else:
35.         for varBind in varBinds:
36.             varB=(' = '.join([x.prettyPrint() for x in varBind]))
37.     return varB
38.
39. cadena = consultaSNMP("comunidadA","10.0.0.7","1.3.6.1.2.1.1.1.0")
40. print cadena
41.

```

Importamos la biblioteca *pysnmp.hlapi*

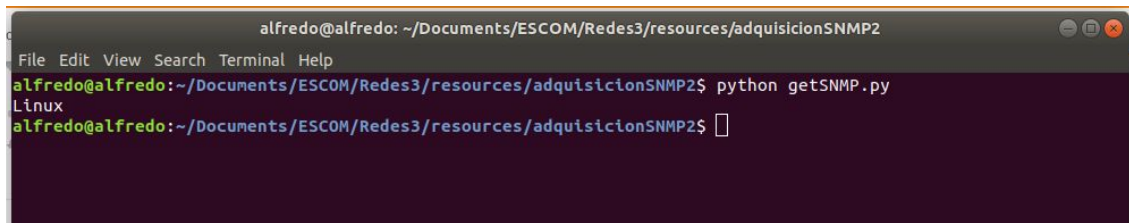


```

alfredo@alfredo: ~/Documents/ESCOM/Redes3/resources/adquisicionSNMP2
File Edit View Search Terminal Help
alfredo@alfredo:~/Documents/ESCOM/Redes3/resources/adquisicionSNMP2$ sudo apt-get install python-pip
[sudo] password for alfredo:
Reading package lists... Done
Building dependency tree
Reading state information... Done
python-pip is already the newest version (9.0.1-2.3-ubuntu1.18.04.1).
The following packages were automatically installed and are no longer required:
  linux-headers-5.3.0-53 linux-headers-5.3.0-53-generic linux-image-5.3.0-53-generic
  linux-modules-5.3.0-53-generic linux-modules-extra-5.3.0-53-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 31 not upgraded.
alfredo@alfredo:~/Documents/ESCOM/Redes3/resources/adquisicionSNMP2$ pip install -U pysnmp
Collecting pysnmp
  Downloading https://files.pythonhosted.org/packages/25/7e/1e17facea54dd21c6a72db6ae57a5bfd56edd54b8c4850668b554bddbba/pysnmp-4.4.12-py2.py3-none-any.whl (296kB)
    100% |#####| 296kB 337kB/s
Collecting pysmi (from pysnmp)
  Downloading https://files.pythonhosted.org/packages/1f/fc/02361d1c2b247de73070c457c4da98c448693154894c14f2d7b48dfabf7e/pysmi-0.3.4-py2.py3-none-any.whl (80kB)
    100% |#####| 81kB 719kB/s
Collecting pycryptodomex (from pysnmp)
  Downloading https://files.pythonhosted.org/packages/63/6d/8b2749763ee16eeeb02bc4ddc483d6b7436d9ec4f0c8e985a99849d4835a/pycryptodomex-3.9.8-cp27-cp27mu-manylinux1_x86_64.whl (13.7MB)
    11% |#####| 1.6MB 444kB/s eta 0:00:28

```

Imagen 11. Instalación de la librería.

A terminal window with a dark background and light text. The title bar at the top reads 'alfredo@alfredo: ~/Documents/ESCOM/Redes3/resources/adquisicionSNMP2'. Below the title bar is a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal content shows a prompt 'alfredo@alfredo:~/Documents/ESCOM/Redes3/resources/adquisicionSNMP2\$' followed by the command 'python getSNMP.py'. The output of the command is 'Linux'. The prompt is followed by a cursor.

```
alfredo@alfredo: ~/Documents/ESCOM/Redes3/resources/adquisicionSNMP2
File Edit View Search Terminal Help
alfredo@alfredo:~/Documents/ESCOM/Redes3/resources/adquisicionSNMP2$ python getSNMP.py
Linux
alfredo@alfredo:~/Documents/ESCOM/Redes3/resources/adquisicionSNMP2$
```

*Imagen 12. Ejecución del programa.*