

Instituto Politécnico Nacional  
Escuela Superior de Cómputo



## **PSA3. Servidor de monitorización SNMP**

**Grupo: 7CV1**

**Alumnos:**

- **Díaz Ortiz Brandon Aldair**
- **García Cárdenas Ángel Alberto**
- **Gutiérrez Pérez Lizbeth Alejandra**
  - **Nava Izquierdo César**

**Unidad de Aprendizaje:**

- **ADMINISTRACIÓN DE SERVICIOS EN RED**

**Profesor:**

- **MANUEL ALEJANDRO SOTO RAMOS**

**Fecha:28/11/2024**

<b>Introducción</b>	<b>3</b>
<b>Desarrollo</b>	<b>4</b>
<b>1. Fundamentos de SNMP</b>	<b>4</b>
1.1. Principios básicos del Protocolo Simple de Gestión de Red (SNMP) y su importancia en la monitorización de redes.	4
1.2. Arquitectura de SNMP	4
<b>2. Instalación y Configuración de un Servidor SNMP en Debian</b>	<b>4</b>
2.1. Instalación y configuración del servidor SNMP en una máquina con alguna distribución basada en Linux	4
Paso 1	5
Paso 2	5
Paso 3	5
Paso 4	5
2.2. Configuración del archivo de configuración del servidor SNMP para definir las comunidades, permisos y parámetros de red	6
Paso 1	6
Paso 2	6
Paso 3	7
Paso 4	7
Paso 5	7
Paso 6	7
Paso 7	8
<b>3. Configuración de Agentes SNMP en Clientes Debian y Windows</b>	<b>9</b>
3.1. Instalación y configuración de agentes SNMP en sistemas clientes con Debian y Windows	9
Linux Debian 12	9
Instalación	9
Paso 1	9
Paso 2	9
Paso 3	9
Paso 4	10
Configuración	10
Paso 1	10
Paso 2	11
Paso 3	11
Paso 4	12
Paso 5	12
Paso 6	12
Paso 7	13
Windows	14
Instalación	14
Paso 1	14
Paso 1	14
Paso 2	15
<b>4. Monitorización y Recolección de Datos de Red</b>	<b>16</b>

Cacti	16
4.1. Configuración de la recolección de datos en el servidor SNMP para monitorizar diversos parámetros de rendimiento de los sistemas clientes	16
Instalación	16
Paso 1	16
Paso 2	17
Paso 3	17
Paso 4	17
Paso 5	17
Paso 6	18
Paso 7	18
4.2. Utilización de herramientas de monitorización para visualizar y analizar los datos recolectados (al menos 20 por cada equipo)	19
Paso 1	19
Paso 3	20
Paso 4	22
<b>Conclusiones</b>	<b>24</b>

# Introducción

La monitorización de redes es una parte fundamental en la administración de infraestructuras tecnológicas, ya que permite asegurar el buen funcionamiento de los sistemas, detectar problemas antes de que se conviertan en fallas graves y optimizar los recursos disponibles. Una de las herramientas más utilizadas para esta tarea es el **Protocolo Simple de Gestión de Red** (SNMP, por sus siglas en inglés), que facilita la supervisión de dispositivos en una red, como servidores, routers, switches y otros equipos de red.

Esta práctica tiene como objetivo comprender los principios fundamentales de SNMP y su importancia en la gestión de redes. A través de la instalación y configuración de un servidor SNMP en un sistema operativo basado en Debian, así como la implementación de agentes SNMP en clientes Debian y Windows, se busca realizar una monitorización integral de parámetros clave del sistema, como el uso de CPU, memoria, almacenamiento y tarjeta de red. Además, se configurarán alertas para asegurar una respuesta proactiva ante posibles fallos de rendimiento. Al final, se evaluará la eficiencia del sistema de monitorización para mejorar la precisión de los datos recolectados.

# Desarrollo

## 1. Fundamentos de SNMP

El Protocolo Simple de Gestión de Red (SNMP) es un estándar de Internet para la gestión de dispositivos en redes IP. SNMP es ampliamente utilizado para monitorizar y gestionar routers, switches, servidores, estaciones de trabajo, impresoras y más.

### 1.1. Principios básicos del Protocolo Simple de Gestión de Red (SNMP) y su importancia en la monitorización de redes.

SNMP permite a los administradores de red:

- **Monitorizar** el rendimiento de la red.
- **Detectar y resolver** problemas de red.
- **Planificar** el crecimiento de la red.

Se basa en una arquitectura cliente-servidor donde el administrador (manager) recopila información de los agentes instalados en los dispositivos.

### 1.2. Arquitectura de SNMP

- **Administrador (Manager):** Software que solicita información a los agentes y recibe notificaciones.
- **Agente (Agent):** Programa que se ejecuta en el dispositivo gestionado y envía información al manager.
- **Base de Información de Gestión (MIB):** Esquema que define las variables que pueden ser gestionadas y monitorizadas.

## 2. Instalación y Configuración de un Servidor SNMP en Debian

### 2.1. Instalación y configuración del servidor SNMP en una máquina con alguna distribución basada en Linux

Para su instalación es necesario tener permisos de superusuario (root/administrador) y realizar los siguientes pasos:

## Paso 1

Realizaremos la copia del archivo `/etc/apt/source.list` al mismo directorio con nombre `source.list.original` como se muestra a continuación:

```
cp /etc/apt/sources.list /etc/apt/sources.list.original
```

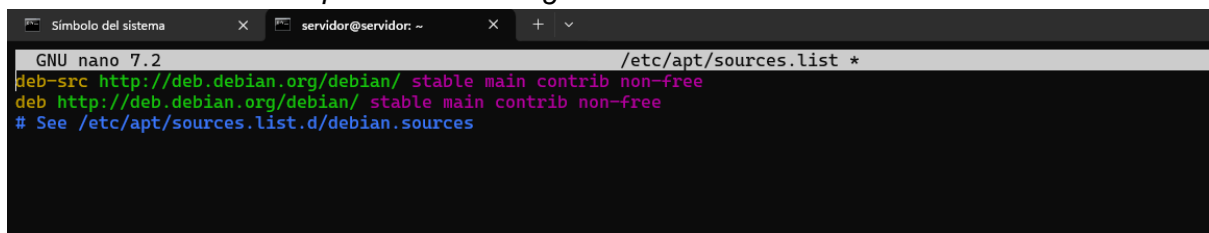
Con el fin de tener respaldo de las configuraciones de fábrica del servidor

```
servidor@servidor:~$ sudo cp /etc/apt/sources.list /etc/apt/sources.list.original
servidor@servidor:~$ |
```

## Paso 2

Comenzaremos a modificar el archivo `/etc/apt/source.list` agregando al final del archivo, las siguientes líneas:

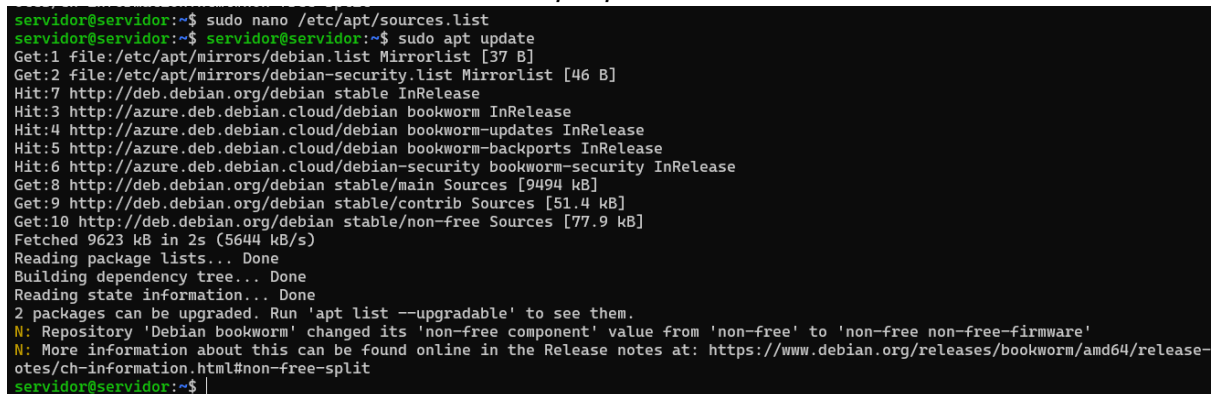
```
deb http://deb.debian.org/debian/ stable main contrib non-free
deb-src http://deb.debian.org/debian/ stable main contrib non-free
```



## Paso 3

Realizar una actualización con el siguiente comando:

```
apt update
```



## Paso 4

Instalar los paquetes `snmp`, `snmpd` y `snmp-mibs-downloader`

```
apt install snmp snmpd snmp-mibs-downloader
```

```

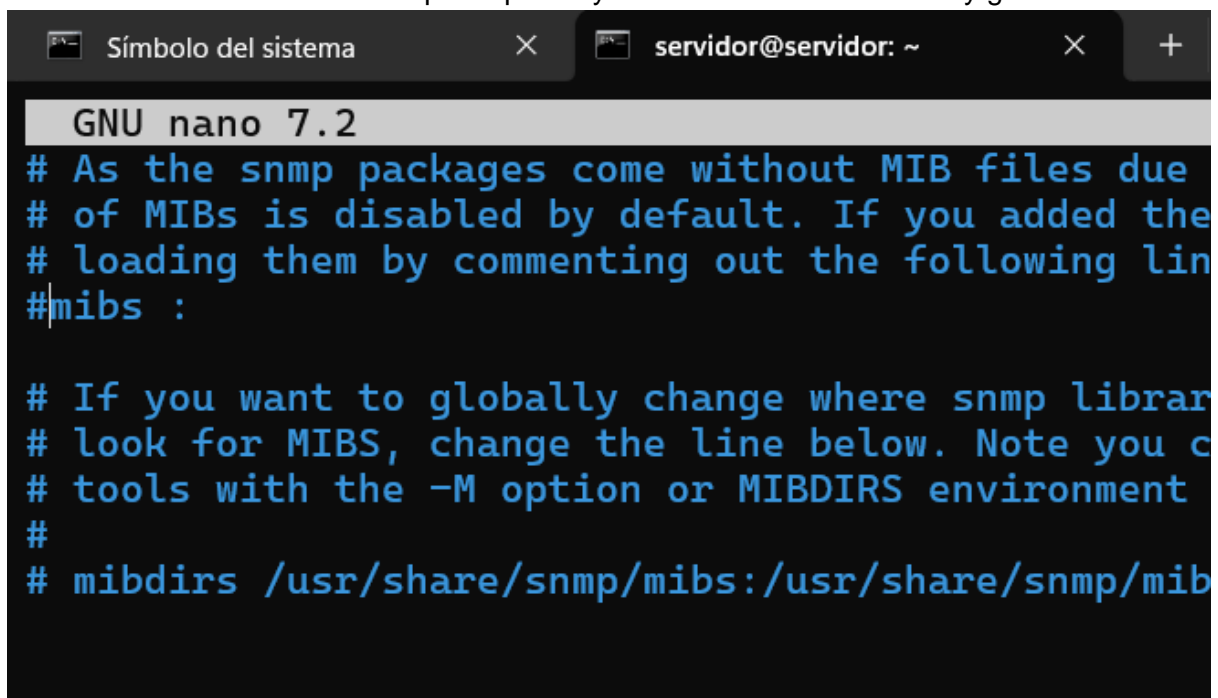
servidor@servidor:~$ sudo apt install snmp snmpd snmp-mibs-downloader
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libgdbm-compat4 libperl5.36 libsensors-config libsensors5 libsnmp-base libsnmp40 patch perl perl-modules-5.36 smstrip
Suggested packages:
  lm-sensors ed diffutils-doc perl-doc libterm-readline-gnu-perl | libterm-readline-perl-perl make libtap-harness-archive-perl
  unzip snmptrapd
The following NEW packages will be installed:
  libgdbm-compat4 libperl5.36 libsensors-config libsensors5 libsnmp-base libsnmp40 patch perl perl-modules-5.36 smstrip snmp
  snmp-mibs-downloader snmpd
0 upgraded, 13 newly installed, 0 to remove and 2 not upgraded.
Need to get 17.2 MB of archives.
After this operation, 63.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian stable/main amd64 perl-modules-5.36 all 5.36.0-7+deb12u1 [2815 kB]
Get:2 http://deb.debian.org/debian stable/main amd64 libgdbm-compat4 amd64 1.23-3 [48.2 kB]
Get:3 http://deb.debian.org/debian stable/main amd64 libperl5.36 amd64 5.36.0-7+deb12u1 [4218 kB]
Get:4 http://deb.debian.org/debian stable/main amd64 perl amd64 5.36.0-7+deb12u1 [239 kB]
Get:5 http://deb.debian.org/debian stable/main amd64 libsensors-config all 1:3.6.0-7.1 [14.3 kB]
Get:6 http://deb.debian.org/debian stable/main amd64 libsensors5 amd64 1:3.6.0-7.1 [34.2 kB]
Get:7 http://deb.debian.org/debian stable/main amd64 libsnmp-base all 5.9.3+dfsg-2 [1753 kB]
Get:8 http://deb.debian.org/debian stable/main amd64 libsnmp40 amd64 5.9.3+dfsg-2 [2556 kB]
Get:9 http://deb.debian.org/debian stable/main amd64 snmpd amd64 5.9.3+dfsg-2 [57.5 kB]
Get:10 http://deb.debian.org/debian stable/main amd64 patch amd64 2.7.6-7 [128 kB]
Get:11 http://deb.debian.org/debian stable/main amd64 smstrip all 0.4.8+dfsg2-16 [29.4 kB]

```

## 2.2. Configuración del archivo de configuración del servidor SNMP para definir las comunidades, permisos y parámetros de red

### Paso 1

Modificamos el archivo `/etc/snmp/snmp.conf` y se comenta la línea `mibs :` y guardar.



```

GNU nano 7.2
# As the snmp packages come without MIB files due
# of MIBs is disabled by default. If you added the
# loading them by commenting out the following line
#mibs :

# If you want to globally change where snmp libraries
# look for MIBS, change the line below. Note you can use
# tools with the -M option or MIBDIRS environment variable
#
# mibdirs /usr/share/snmp/mibs:/usr/share/snmp/mibs

```

### Paso 2

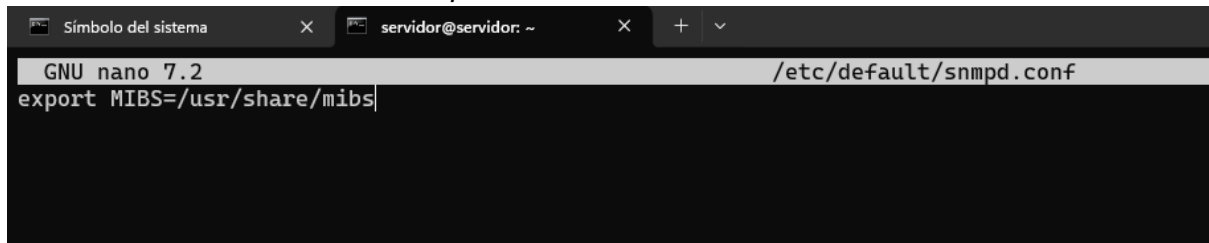
Una vez modificado el archivo anterior, tendrás que descargar los MIBS para tener una buena comunicación entre equipos, colocando el siguiente comando:

`download-mibs`

### Paso 3

Para poder leer humanamente los OID's, debemos modificar el archivo `/etc/default/snmpd` y agregar la siguiente línea:

*export MIBS=/usr/share/mibs*

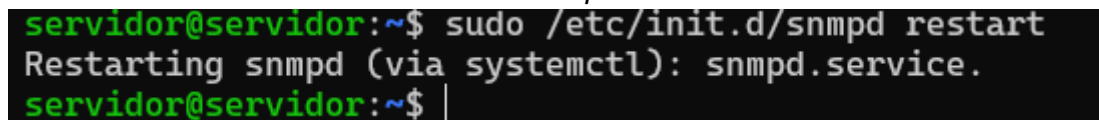


```
GNU nano 7.2 /etc/default/snmpd.conf
export MIBS=/usr/share/mibs
```

### Paso 4

Reiniciamos el servicio de snmp para efectuar las configuraciones con el siguiente comando:

*/etc/init.d/snmpd restart*

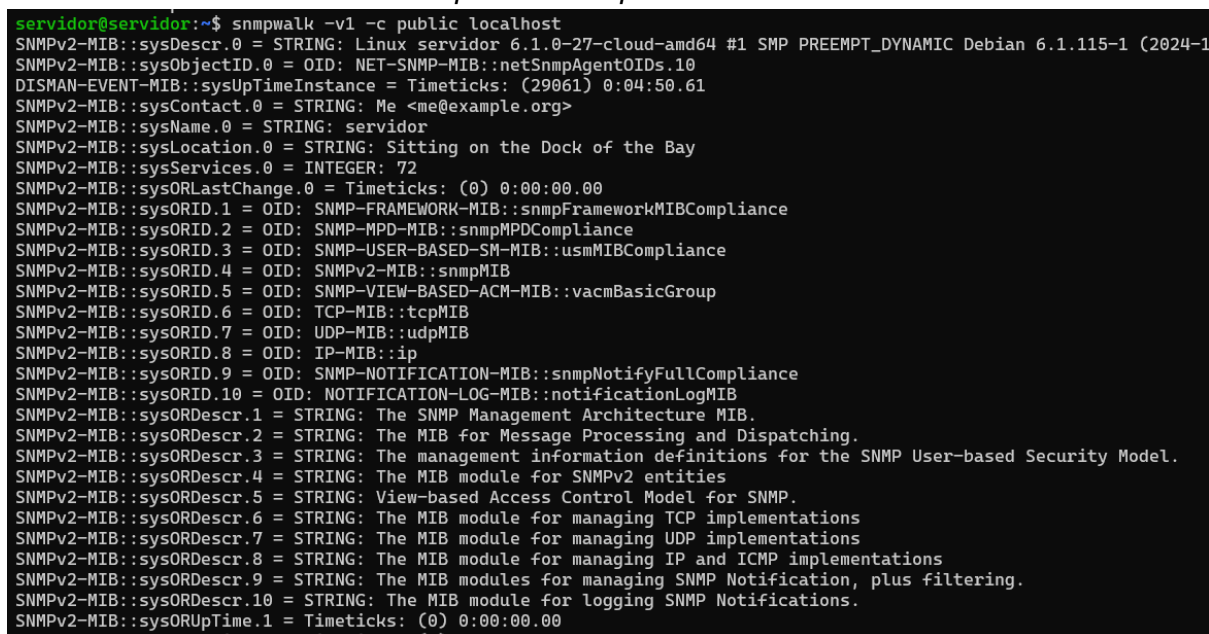


```
servidor@servidor:~$ sudo /etc/init.d/snmpd restart
Restarting snmpd (via systemctl): snmpd.service.
servidor@servidor:~$
```

### Paso 5

Realizamos las pruebas con nosotros mismos para ver que todo está correcto con el siguiente comando:

*snmpwalk -v1 -c public localhost*



```
servidor@servidor:~$ snmpwalk -v1 -c public localhost
SNMPv2-MIB::sysDescr.0 = STRING: Linux servidor 6.1.0-27-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.115-1 (2024-1
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (29061) 0:04:50.61
SNMPv2-MIB::sysContact.0 = STRING: Me <me@example.org>
SNMPv2-MIB::sysName.0 = STRING: servidor
SNMPv2-MIB::sysLocation.0 = STRING: Sitting on the Dock of the Bay
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.6 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance
SNMPv2-MIB::sysORID.10 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB
SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.3 = STRING: The management information definitions for the SNMP User-based Security Model.
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.5 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing TCP implementations
SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing UDP implementations
SNMPv2-MIB::sysORDescr.8 = STRING: The MIB module for managing IP and ICMP implementations
SNMPv2-MIB::sysORDescr.9 = STRING: The MIB modules for managing SNMP Notification, plus filtering.
SNMPv2-MIB::sysORDescr.10 = STRING: The MIB module for logging SNMP Notifications.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (0) 0:00:00.00
```

### Paso 6

Aquí solo debemos realizar pruebas de comunicación con los clientes para ver que todo está correcto y llevar la integración de manera correcta, esto se logra colocando el siguiente comando:

*snmpwalk -v2c -c publica <IP-CLIENTE>*

De esta forma podemos realizar la prueba de comunicación, donde la respuesta es



algo extensa

```
SNMPv2-MIB::sysDescr.0 = STRING: Linux debian 6.1.0-22-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.94-1 (2024-06-21) x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (358298) 0:59:42.98
SNMPv2-MIB::sysContact.0 = STRING: ssh ssh@example.org
SNMPv2-MIB::sysName.0 = STRING: debian
SNMPv2-MIB::sysLocation.0 = STRING: Servidor SSH
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.6 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance
SNMPv2-MIB::sysORID.10 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB
SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.3 = STRING: The management information definitions for the SNMP User-based Security Model.
```

## Paso 7

Finalmente realizamos la última consulta donde obtenemos datos del sistema del cliente para poder realizar un monitoreo adecuado del equipo, se realiza con el siguiente comando:

*snmpwalk -v2c -c publica <IP-CLIENTE> system*

```
SNMPv2-MIB::sysDescr.0 = STRING: Linux debian 6.1.0-22-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.94-1 (2024-06-21) x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (383190) 1:03:51.90
SNMPv2-MIB::sysContact.0 = STRING: ssh ssh@example.org
SNMPv2-MIB::sysName.0 = STRING: debian
SNMPv2-MIB::sysLocation.0 = STRING: Servidor SSH
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.6 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance
SNMPv2-MIB::sysORID.10 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB
SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.3 = STRING: The management information definitions for the SNMP User-based Security Model.
```

## 3. Configuración de Agentes SNMP en Clientes Debian y Windows

### 3.1. Instalación y configuración de agentes SNMP en sistemas clientes con Debian y Windows

#### Linux Debian 12

##### Instalación

Para su instalación es necesario tener permisos de superusuario (root/administrador) y realizar los siguientes pasos:

##### Paso 1

Realizaremos la copia del archivo `/etc/apt/sources.list` al mismo directorio con nombre `sources.list.original` como se muestra a continuación:

```
cp /etc/apt/sources.list /etc/apt/sources.list.original
```

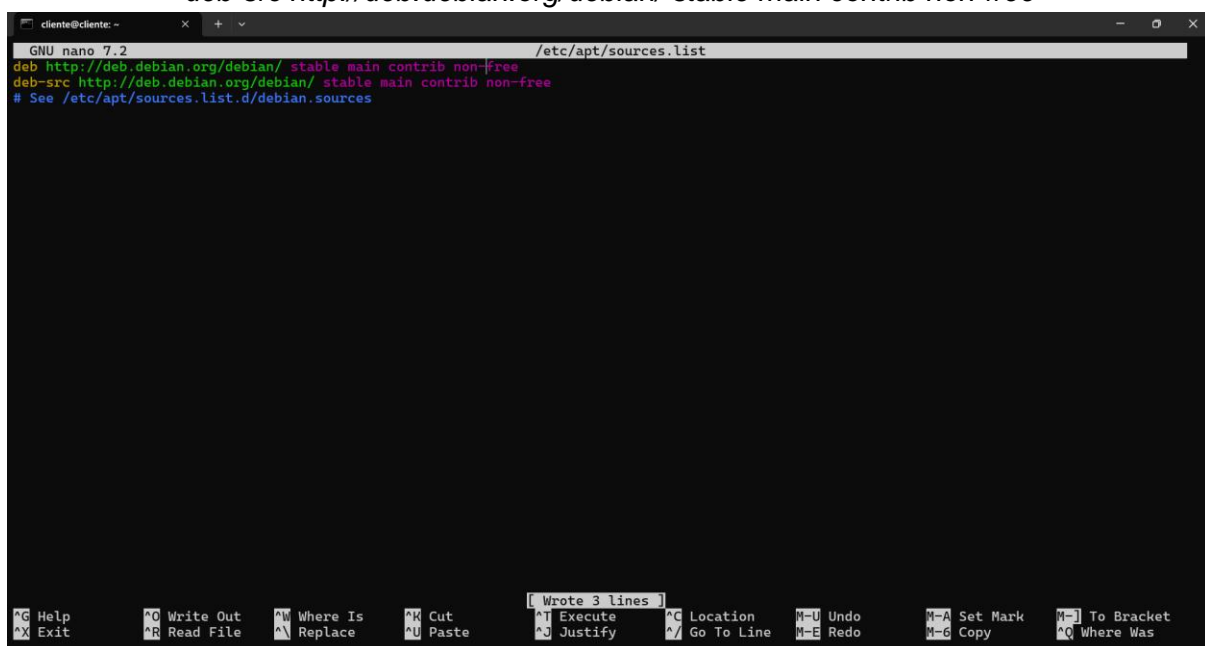
Con el fin de tener respaldo de las configuraciones de fábrica del servidor

```
cliente@cliente:~$ sudo cp /etc/apt/sources.list /etc/apt/sources.list.original
cliente@cliente:~$ deb http://deb.debian.org/debian/ stable main contrib non-free
```

##### Paso 2

Comenzaremos a modificar el archivo `/etc/apt/sources.list` agregando al final del archivo, las siguientes líneas:

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



```
cliente@cliente: ~
GNU nano 7.2 /etc/apt/sources.list
deb http://deb.debian.org/debian/ stable main contrib non-free
deb-src http://deb.debian.org/debian/ stable main contrib non-free
# See /etc/apt/sources.list.d/debian.sources

[ Wrote 3 lines ]
Help      Write Out  Where Is   Cut        Execute    Location  N-U Undo   M-A Set Mark  M-] To Bracket
Exit      Read File  Replace    Paste      Justify    Go To Line N-E Redo   M-C Copy   M-Q Where Was
```

##### Paso 3

Realizar una actualización con el siguiente comando:

## apt update

```
cliente@cliente:~$ sudo apt update
Get:1 file:/etc/apt/mirrors/debian.list Mirrorlist [37 B]
Get:2 file:/etc/apt/mirrors/debian-security.list Mirrorlist [46 B]
Get:7 http://deb.debian.org/debian stable InRelease [151 kB]
Hit:3 http://azure.deb.debian.cloud/debian bookworm InRelease
Get:4 http://azure.deb.debian.cloud/debian bookworm-updates InRelease [55.4 kB]
Get:5 http://azure.deb.debian.cloud/debian bookworm-backports InRelease [59.0 kB]
Get:6 http://azure.deb.debian.cloud/debian-security bookworm-security InRelease [48.0 kB]
Get:8 http://deb.debian.org/debian stable/main amd64 Packages [8789 kB]
Get:9 http://deb.debian.org/debian stable/main Translation-en [6109 kB]
Get:10 http://deb.debian.org/debian stable/contrib amd64 Packages [54.1 kB]
Get:11 http://deb.debian.org/debian stable/contrib Translation-en [48.8 kB]
Get:12 http://deb.debian.org/debian stable/non-free amd64 Packages [97.3 kB]
Get:13 http://deb.debian.org/debian stable/non-free Translation-en [67.0 kB]
Get:14 http://azure.deb.debian.cloud/debian bookworm-backports/main Sources.diff/Index [63.3 kB]
Get:15 http://azure.deb.debian.cloud/debian bookworm-backports/main amd64 Packages.diff/Index [63.3 kB]
Get:16 http://azure.deb.debian.cloud/debian bookworm-backports/main Sources T-2024-11-24-1410.30-F-2024-11-24-0804.56.pdiff [1567 B]
Get:16 http://azure.deb.debian.cloud/debian bookworm-backports/main Sources T-2024-11-24-1410.30-F-2024-11-24-0804.56.pdiff [1567 B]
```

## Paso 4

Instalar los paquetes snmp, snmpd y snmp-mibs-downloader

*apt install snmp snmpd snmp-mibs-downloader*

```
cliente@cliente:~$ sudo apt install snmp snmpd snmp-mibs-downloader
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libsnmp-base libsnmp40 patch smstrip
Suggested packages:
  ed diffutils-doc unzip snmpttrapd
The following NEW packages will be installed:
  libsnmp-base libsnmp40 patch smstrip snmp snmp-mibs-downloader snmpd
0 upgraded, 7 newly installed, 0 to remove and 2 not upgraded.
Need to get 9858 kB of archives.
After this operation, 14.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian stable/main amd64 libsnmp-base all 5.9.3+dfsg-2 [1753 kB]
Get:2 http://deb.debian.org/debian stable/main amd64 libsnmp40 amd64 5.9.3+dfsg-2 [2556 kB]
Get:3 http://deb.debian.org/debian stable/main amd64 snmpd amd64 5.9.3+dfsg-2 [57.5 kB]
Get:4 http://deb.debian.org/debian stable/main amd64 patch amd64 2.7.6-7 [128 kB]
Get:5 http://deb.debian.org/debian stable/main amd64 smstrip all 0.4.8+dfsg2-16 [29.4 kB]
Get:6 http://deb.debian.org/debian stable/main amd64 snmp amd64 5.9.3+dfsg-2 [172 kB]
Get:7 http://deb.debian.org/debian stable/non-free amd64 snmp-mibs-downloader all 1.5 [5163 kB]
Fetched 9858 kB in 0s (22.9 MB/s)
Preconfiguring packages ...
Selecting previously unselected package libsnmp-base.
(Reading database ... 35760 files and directories currently installed.)
Preparing to unpack .../0-libsnmp-base_5.9.3+dfsg-2_all.deb ...
Unpacking libsnmp-base (5.9.3+dfsg-2) ...
Selecting previously unselected package libsnmp40:amd64.
Preparing to unpack .../1-libsnmp40_5.9.3+dfsg-2_amd64.deb ...
Unpacking libsnmp40:amd64 (5.9.3+dfsg-2) ...
Selecting previously unselected package snmpd.
Preparing to unpack .../2-snmpd_5.9.3+dfsg-2_amd64.deb ...
Unpacking snmpd (5.9.3+dfsg-2) ...
```

## Configuración

### Paso 1

Modificamos el archivo `/etc/snmp/snmp.conf` y se comenta la línea `mibs` : y guardar.

```
cliente@cliente: ~  
GNU nano 7.2 /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 reenale  
# 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 /usr/share/snmp/mibs:/usr/share/snmp/mibs/iana:/usr/share/snmp/mibs/ietf  
  
[ Read 10 lines ]  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark  
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo      M-G Copy
```

## Paso 2

Una vez modificado el archivo anterior, descargamos los MIBS para tener una buena comunicación entre equipos, colocando el siguiente comando:

*download-mibs*

```
cliente@cliente:~$ sudo download-mibs  
  
Downloading documents and extracting MIB files.  
This will take some minutes.  
  
In case this process fails, it can always be repeated later by executing  
/usr/bin/download-mibs again.  
  
RFC1155-SMI: 119 lines.  
RFC1213-MIB: 2613 lines.  
NOTE: SMUX: ignored.  
SMUX-MIB: 158 lines.  
CLNS-MIB: 1294 lines.  
RFC1381-MIB: 1007 lines.  
RFC1382-MIB: 2627 lines.  
RFC1414-MIB: 131 lines.  
SNMPv2-PARTY-MIB: 1410 lines.  
SNMPv2-M2M-MIB: 807 lines.  
MIOX25-MIB: 708 lines.  
PPP-LCP-MIB: 764 lines.  
PPP-SEC-MIB: 289 lines.  
PPP-IP-MCP-MIB: 203 lines.  
PPP-BRIDGE-MCP-MIB: 429 lines.  
FDDI-SMT73-MIB: 2126 lines.  
TOKEN-RING-RMON-MIB: 2302 lines.  
SOURCE-ROUTING-MIB: 450 lines.  
DECNET-PHIV-MIB: 3030 lines.  
DSA-MIB: 642 lines.  
DPI20-MIB: 47 lines.  
IBM-6611-APPN-MIB: 5112 lines.  
DNS-SERVER-MIB: 1078 lines.  
DNS-RESOLVER-MIB: 1196 lines.  
UPS-MIB: 1899 lines.
```

## Paso 3

Verificamos que todas las configuraciones hayan sido correctas ejecutando el siguiente comando:

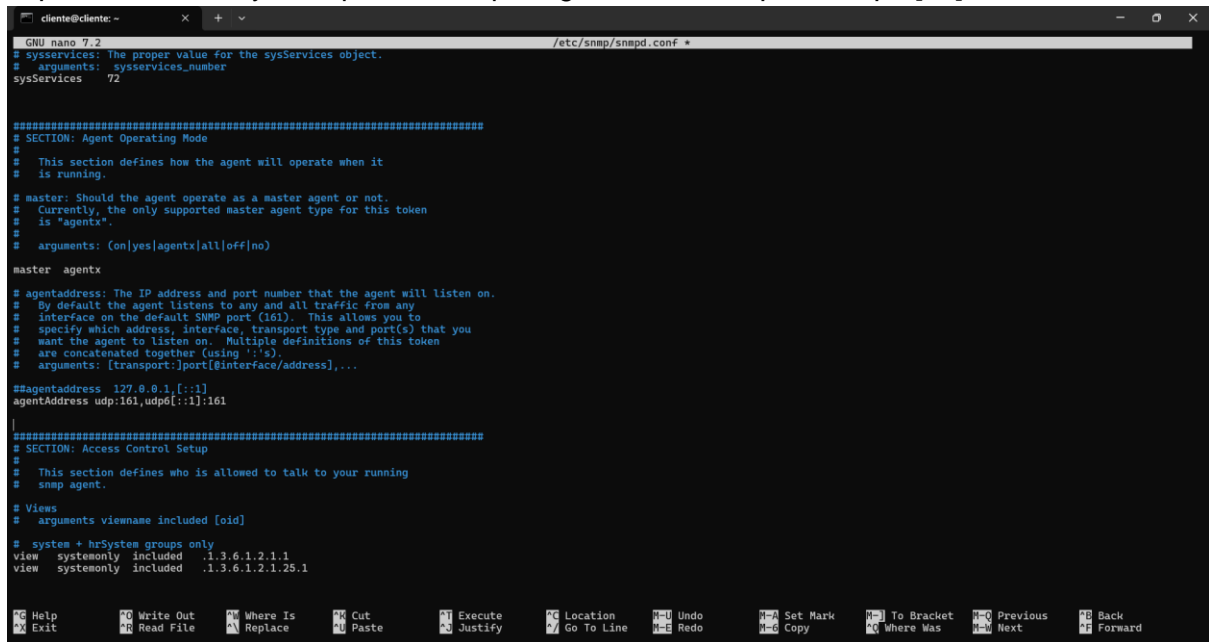
*snmpstatus -v2c -c public localhost*

Obteniendo algo como lo siguiente:

```
cliente@cliente:~$ sudo snmpstatus -v2c -c public localhost  
[UDP: [127.0.0.1]:161->[0.0.0.0]:47815]=>[Linux cliente 6.1.0-26-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.112-1 (2024-09-30) x86_64] Up: 0:04:48.77  
Interfaces: 0, Recv/Trans packets: 0/0 | IP: 0/0
```

## Paso 4

Modificar el archivo `/etc/snmp/snmpd.conf`, comentando la línea `agentAddress udp:127.0.0.1:161` y reemplazandola por `agentaddress udp:161,udp6:[::1]:161`



```
cliente@cliente: ~
GNU nano 2.2 /etc/snmp/snmpd.conf
# sysServices: The proper value for the sysServices object.
# arguments: sysServices_number
sysServices 72

#####
# SECTION: Agent Operating Mode
#
# This section defines how the agent will operate when it
# is running.
#
# master: Should the agent operate as a master agent or not.
# Currently, the only supported master agent type for this token
# is "agentx".
# arguments: (on|yes|agentx|all|off|no)
master agentx

# agentAddress: The IP address and port number that the agent will listen on.
# By default the agent listens to any and all traffic from any
# interface on the default SNMP port (161). This allows you to
# specify which address, interface, transport type and port(s) that you
# want the agent to listen on. Multiple definitions of this token
# are concatenated together (using ':').
# arguments: [transport:]port[@interface/address],...

#agentAddress 127.0.0.1[:1]
agentAddress udp:161,udp6:[::1]:161

#####
# SECTION: Access Control Setup
#
# This section defines who is allowed to talk to your running
# snmp agent.
#
# Views
# arguments viewname included [oid]
#
# 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

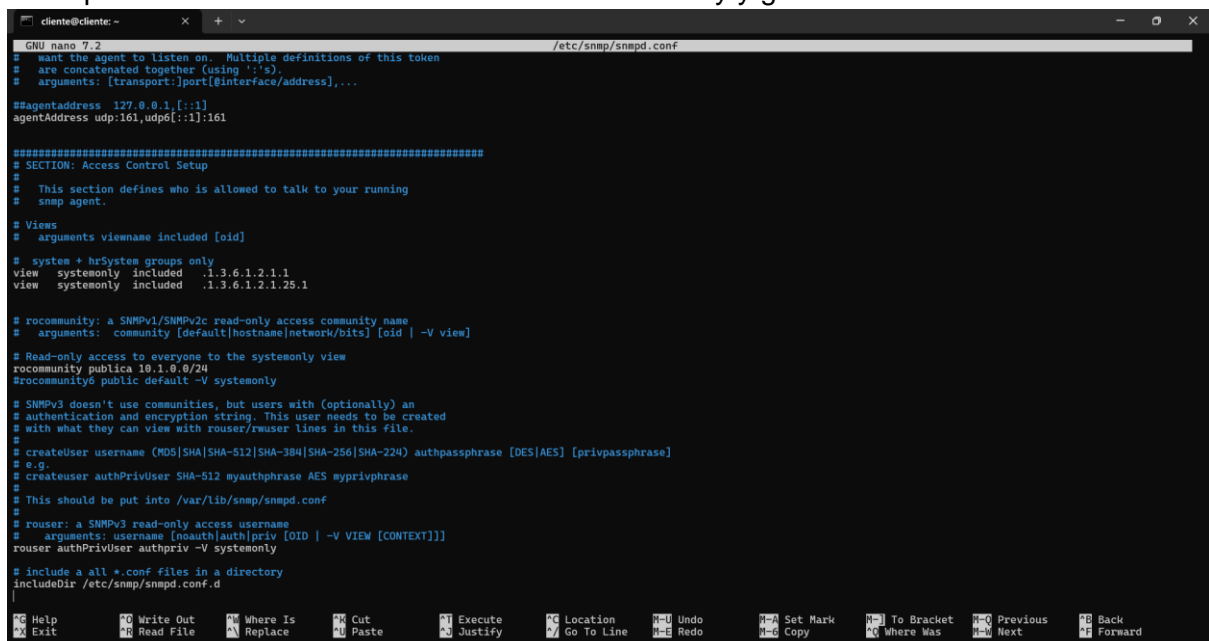
#####
# Help
# Exit
# Write Out
# Read File
# Where Is
# Replace
# Cut
# Paste
# Execute
# Justify
# Location
# Go To Line
# Undo
# Redo
# Set Mark
# Copy
# To Bracket
# Where Was
# Previous
# Next
# Back
# Forward
```

## Paso 5

En el mismo archivo, reemplazar `public` por la palabra `pública` para que sea un entorno distinto y especificamos el servidor snmp con la máscara que la red:

*rocommunity publica 10.1.0.4*

Solo queda comentar las demas lineas de `rocommunity` y guardar el archivo



```
cliente@cliente: ~
GNU nano 2.2 /etc/snmp/snmpd.conf
# want the agent to listen on. Multiple definitions of this token
# are concatenated together (using ':').
# arguments: [transport:]port[@interface/address],...

#agentAddress 127.0.0.1[:1]
agentAddress udp:161,udp6:[::1]:161

#####
# SECTION: Access Control Setup
#
# This section defines who is allowed to talk to your running
# snmp agent.
#
# Views
# arguments viewname included [oid]
#
# 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: a SNMPv1/SNMPv2c read-only access community name
# arguments: community [default|hostname|network/bits] [oid | -V view]

# Read-only access to everyone to the systemonly view
rocommunity publica 10.1.0.0/24
#rocommunity public default -V systemonly

# SNMPv3 doesn't use communities, but users with (optionally) an
# authentication and encryption string. This user needs to be created
# with what they can view with rouser/rwuser lines in this file.
#
# createuser username (MD5|SHA|SHA-512|SHA-384|SHA-256|SHA-224) authpassphrase [DES|AES] [privpassphrase]
# e.g.
# createuser authPrivUser SHA-512 myauthphrase AES myprivphrase
# This should be put into /var/lib/snmp/snmpd.conf
#
# rouser: a SNMPv3 read-only access username
# arguments: username [noauth|auth|priv [OID | -V VIEW [CONTEXT]]]
rouser authPrivUser authpriv -V systemonly

# include a all *.conf files in a directory
includeDir /etc/snmp/snmpd.conf.d

#####
# Help
# Exit
# Write Out
# Read File
# Where Is
# Replace
# Cut
# Paste
# Execute
# Justify
# Location
# Go To Line
# Undo
# Redo
# Set Mark
# Copy
# To Bracket
# Where Was
# Previous
# Next
# Back
# Forward
```

## Paso 6

Reiniciamos el servicio snmp para aplicar todas las configuraciones ya realizadas con el siguiente comando:

*/etc/init.d/snmpd restart*

Ahora simplemente restaría agregar usuarios para utilizar la v3 siempre que sea posible

```
cliente@cliente:~$ sudo nano /etc/snmp/snmpd.conf
cliente@cliente:~$
```

#### Paso 7

Creamos un usuario y contraseña para el uso del monitoreo con un enfoque más seguro, primeramente debemos para el servicio snmpd, el cual se logra con el siguiente comando:

*/etc/init.d/snmpd stop*

```
cliente@cliente:~$ sudo /etc/init.d/snmpd stop
Stopping snmpd (via systemctl): snmpd.service.
cliente@cliente:~$ |
```

Después de pararlo, creamos nuestro usuario y contraseña para realizar el monitoreo con ese tipo de autenticación, con el siguiente comando:

*net-snmp-create-v3-user -ro -a SHA -x AES*

Pidiendonos datos, donde solo debemos llenarlos para que todo se lleve a cabo correctamente, como se muestra a continuación

```
cliente@cliente:~$ sudo net-snmp-create-v3-user -ro -a SHA -x AES
Enter a SNMPv3 user name to create:
cesar
Enter authentication pass-phrase:
123
Enter encryption pass-phrase:
[press return to reuse the authentication pass-phrase]
123
adding the following line to /var/lib/snmp/snmpd.conf:
    createUser cesar SHA "123" AES "123"
adding the following line to /etc/snmp/snmpd.conf:
    rouser cesar
cliente@cliente:~$ |
```

Al final de todo ello, simplemente volvemos a levantar el servicio y realizamos un testeo, con los comandos siguientes:

*systemctl start snmpd*

*snmpwalk -OQne -v 3 -t 10 -l AuthPriv -u <snmpuser> -a SHA1 -A*

*<SNMPbadPASS> -x AES -X <SNMPbadPASS> 127.0.0.1 -Os*

*1.3.6.1.2.1.2.2.1*

Obteniendo algo de la siguiente forma

```
cliente@cliente:~$ sudo systemctl start snmpd
cliente@cliente:~$ snmpwalk -Ons -v 3 -t 10 -l AuthPriv -u angel -a SHA1 -A 123456789 -x AES -X 123456789 127.0.0.1 -Os 1.3.6.1.2.1.2.2.1
ifIndex.1 = 1
ifIndex.2 = 2
ifDescr.1 = lo
ifDescr.2 = eth0
ifType.1 = 24
ifType.2 = 6
ifMtu.1 = 65536
ifMtu.2 = 1500
ifSpeed.1 = 100000000
ifSpeed.2 = 4294967295
ifPhysAddress.1 =
ifPhysAddress.2 = 7c:1e:52:43:bd:31
ifAdminStatus.1 = 1
ifAdminStatus.2 = 1
ifOperStatus.1 = 1
ifOperStatus.2 = 1
ifLastChange.1 = 0:0:00:00.00
ifLastChange.2 = 0:0:00:00.00
ifInOctets.1 = 2490
ifInOctets.2 = 1818402250
ifInUcastPkts.1 = 0
ifInUcastPkts.2 = 0
ifInNUcastPkts.1 = 0
ifInNUcastPkts.2 = 0
ifInDiscards.1 = 0
ifInDiscards.2 = 0
ifInErrors.1 = 0
ifInErrors.2 = 0
ifInUnknownProtos.1 = 0
ifInUnknownProtos.2 = 0
ifOutOctets.1 = 2490
ifOutOctets.2 = 1986302093
ifOutUcastPkts.1 = 20
ifOutUcastPkts.2 = 8382107
ifOutNUcastPkts.1 = 0
ifOutNUcastPkts.2 = 0
ifOutDiscards.1 = 0
ifOutDiscards.2 = 0
ifOutErrors.1 = 0
```

## Windows

Para esta configuración es necesario utilizar la terminal powershell con permisos de administrador

### Instalación

#### Paso 1

Abrir terminal powershell con permisos de administrador y colocar el siguiente comando para realizar la descarga del paquete snmp

*Add-WindowsCapability -Online -Name "SNMP.Client~~~~0.0.1.0"*

Y al colocarlo y ejecutarlo

```
Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Add-WindowsCapability -Online -Name "SNMP.Client~~~~0.0.1.0"

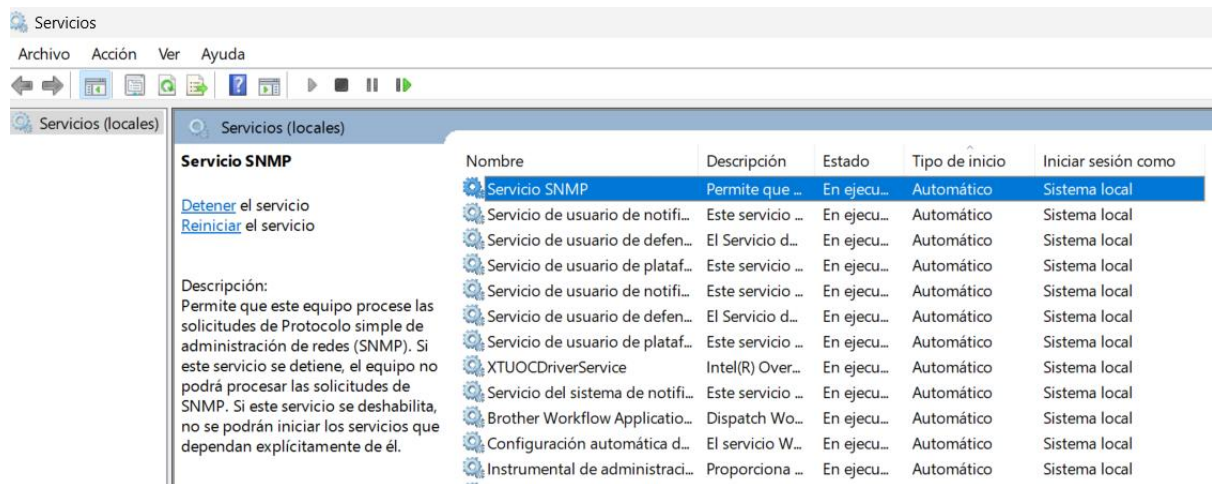
Path          :
Online        : True
RestartNeeded : False

PS C:\WINDOWS\system32>
```

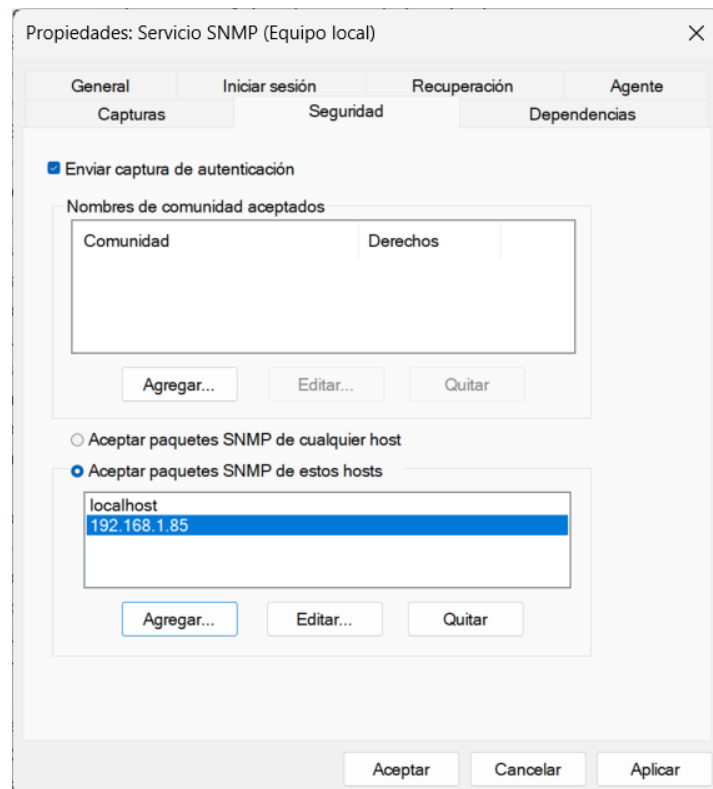
#### Paso 1

Ahora debemos irnos al administrador de servicios, puedes encontrarlo colocando el menú de inicio la palabra servicios o bien services, una vez dentro buscar el servicio SNMP o bien service SNMP.





Ingresa al servicio dándole click, una vez dentro, deberás colocarte en la pestaña de seguridad o bien security y agregar la ip del servidor en cuestión para que reciba los paquetes y se pueda comunicar correctamente.



## Paso 2

Al final solo se aplican los cambios y obtienes tu IP de la máquina windows para poder monitorearla desde el servidor, con el comando:  
ipconfig.



```
Administrador: Símbolo del sistema
C:\Windows\System32>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Dirección IPv6 . . . . . : 2806:106e:23:46af:256c:403b:4812:61c6
    Dirección IPv6 . . . . . : fd0b:175c:34bc:0:fa94:d45f:8c69:dc29
    Dirección IPv6 temporal. . . . . : 2806:106e:23:46af:b92b:a6f:ce72:689f
    Vínculo: dirección IPv6 local. . . : fe80::7f2a:9afe:30f2:ae52%3
    Dirección IPv4. . . . . : 192.168.1.85
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . : fe80::e20e:e4ff:fe5e:1c00%3
                                                192.168.1.254

Adaptador de LAN inalámbrica Conexión de área local* 1:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Conexión de área local* 10:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Wi-Fi:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de Ethernet Conexión de red Bluetooth:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

C:\Windows\System32>
```

## 4. Monitorización y Recolección de Datos de Red

### Cacti

Cacti es una herramienta de código abierto diseñada para la supervisión y el registro gráfico de datos de redes y sistemas. Utiliza SNMP (Simple Network Management Protocol) para recopilar información de dispositivos como routers, switches y servidores. Cacti permite crear gráficos personalizados que muestran el rendimiento y la utilización de recursos a lo largo del tiempo, facilitando así la monitorización y la gestión proactiva de infraestructuras de red y sistemas. Es ampliamente utilizada por administradores de sistemas y redes para mantener un control detallado y eficaz sobre sus entornos informáticos.

### 4.1. Configuración de la recolección de datos en el servidor SNMP para monitorizar diversos parámetros de rendimiento de los sistemas clientes

#### Instalación

Para su instalación es necesario contar con permisos de superusuario (root/administrador) y seguir los siguientes pasos:

#### Paso 1

Antes de instalar Cacti, debemos asegurarnos de que todos nuestros paquetes están en orden y actualizados, con el siguiente comando:

*apt update*

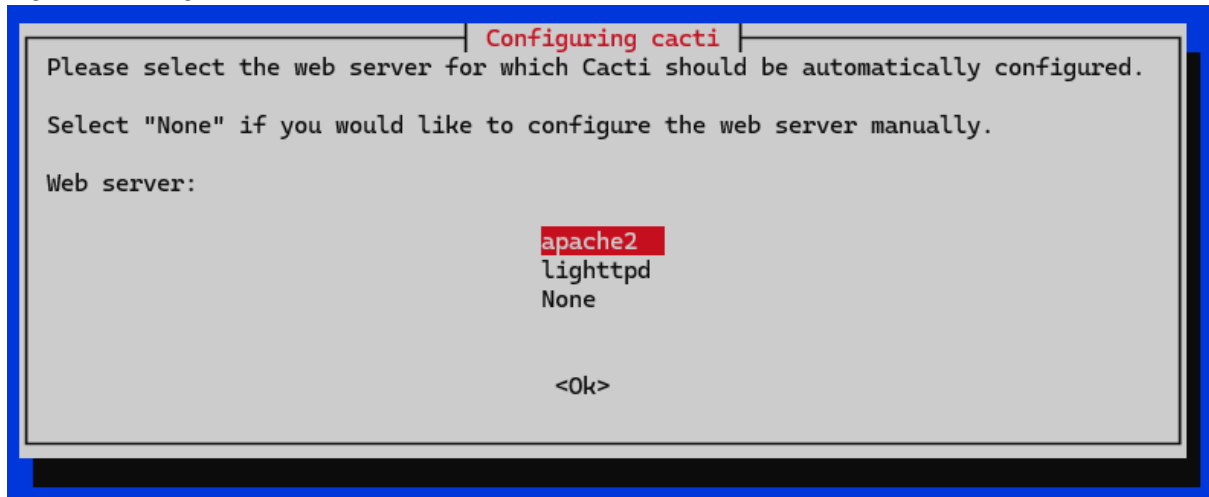
## Paso 2

Instalamos lo que es Cacti, con el siguiente comando:

```
apt-get cacti cacti-spine
```

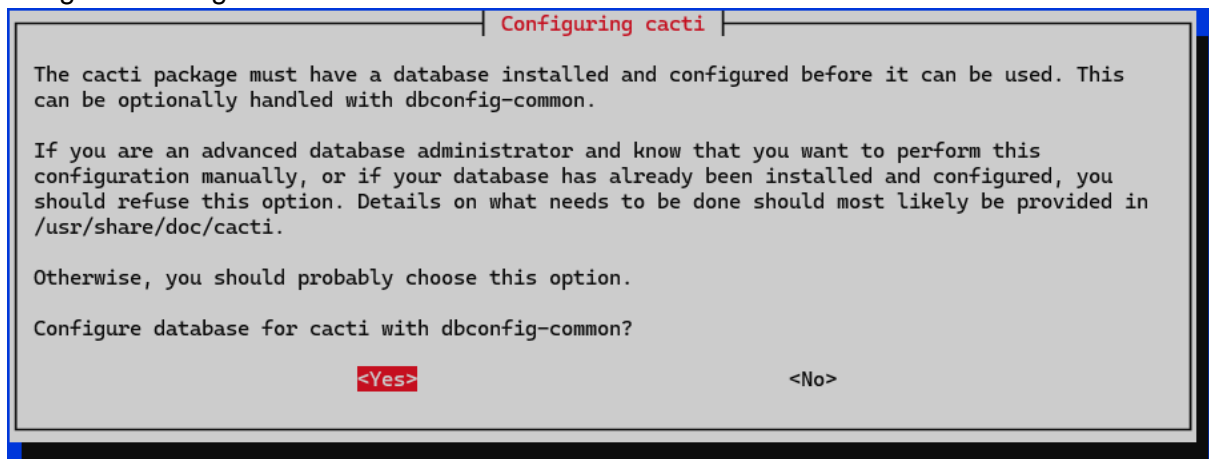
## Paso 3

Seleccionamos el servidor web “apache2” y continuamos, como se muestra en la siguiente imagen:



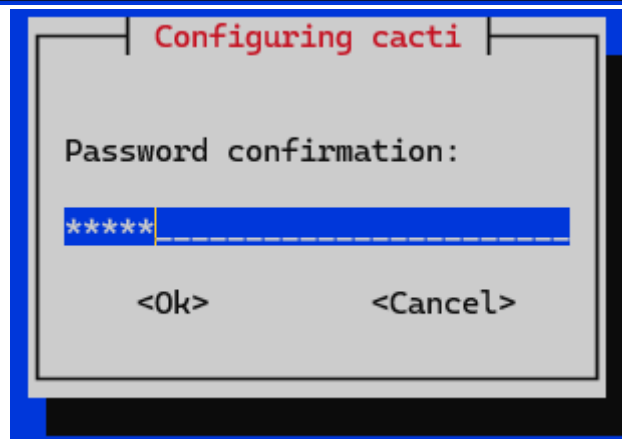
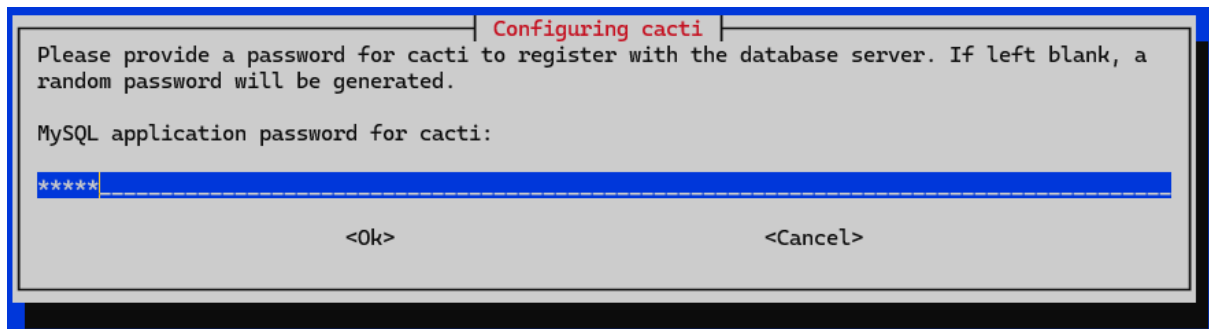
## Paso 4

Una vez seleccionado la opción anterior, nos pedirá la configuración de una base de datos, el cual le daremos que si y continuamos con la configuración, como se ve en la siguiente imagen:



## Paso 5

Nos pedirá una contraseña, el cual también será la contraseña de la aplicación web, trata de colocar una contraseña que recordaras, al finalizar de tipear la contraseña nos pedirá confirmar y simplemente volvemos a ingresar la contraseña, se selecciona la opción, “OK” y continuamos, como se muestra en la siguientes imágenes:



#### Paso 6

Al terminar los pasos anteriores, la instalación de cacti finalizará y podremos acceder a la aplicación web que esta nos proporciona con la siguiente sintaxis en la url, con la siguiente URL, ej. <http://snmp.rgrox.com/cacti>:

*<http://<domain or ip>/cacti>*

#### Paso 7

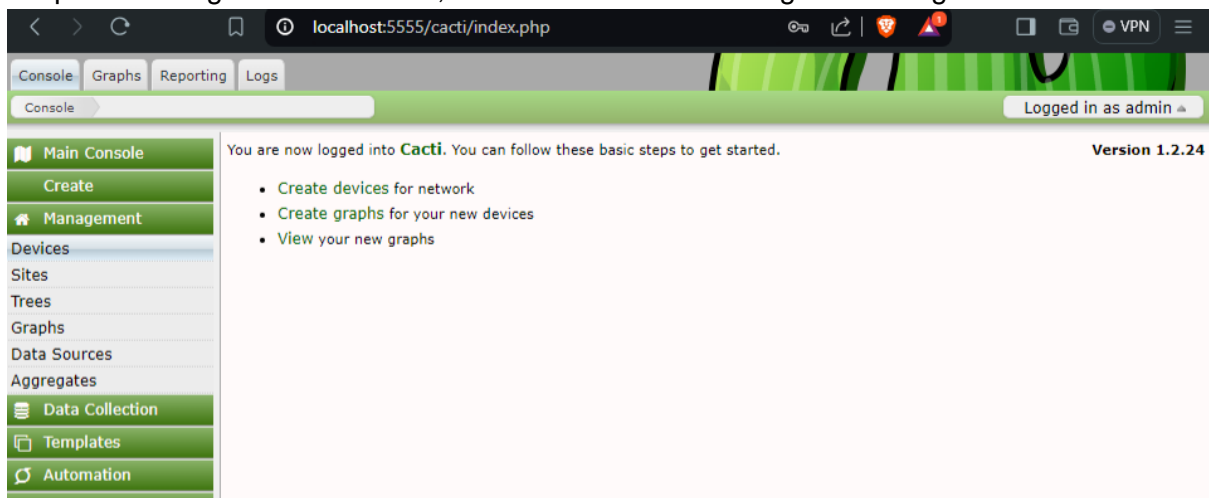
Y podremos ingresar a la aplicación donde el nombre de usuario es admin y el contraseña es la que anteriormente habías ingresado, como se muestra en la imagen siguiente:



## 4.2. Utilización de herramientas de monitorización para visualizar y analizar los datos recolectados (al menos 20 por cada equipo)

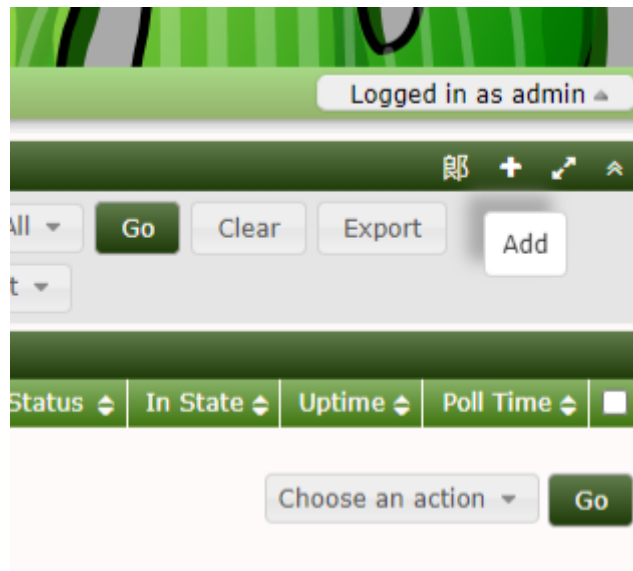
### Paso 1

Una vez se haya ingresado al sistema, podemos realizar el registro de nuestro servidores previamente creados y así monitorearlos de mejor manera, primeramente debemos clickear la opción Management > devices, como se muestra en la siguiente imagen:



### Paso 2

Dentro de esa opción, verás todos los servidores que se registraran conforme a los siguientes pasos, por el momento estara vacio y nosotros procederemos a agregarlos, para hacerlo debemos darle click al boton "+" el cual se encuentra en la esquina superior derecha, como se muestra en la siguiente imagen:



### Paso 3

Dentro de esa vista, tendremos un formulario el cual deberemos llenar con datos del servidor y comunidad para realizar el monitoreo de manera adecuada, el cual debe llevar una descripción (description), un hostname (ip o hostname), una plantilla (device template) el cual debe estar en Net-SNMP para el monitoreo y la configuración de snmp ya sea la versión 2 o la versión 3, como se muestra a continuación:

Ejemplo de la versión 2, la comunidad en este caso es “pública”

localhost:5555/cacti/host.php?action=edit

Console Graphs Reporting Logs

Console Devices (Edit) Logged in as admin

Main Console

Create

Management

Devices

Sites

Trees

Graphs

Data Sources

Aggregates

Data Collection

Templates

Automation

Presets

Import/Export

Configuration

Utilities

Troubleshooting

Device [new]

General Device Options

Description SNMP

Hostname snmp.rgrox.com

Location None

Poller Association Main Poller

Device Site Association Edge

Device Template Net-SNMP Device

Number of Collection Threads 1 Thread

Disable Device

SNMP Options

SNMP Version Version 2

SNMP Community String publica

SNMP Port 161

SNMP Timeout 500

Maximum OIDs Per Get Request 20 OID's

Bulk Walk Maximum Repetitions Auto Detect on Re-Index

Availability/Reachability Options

Downed Device Detection Ping or SNMP Uptime

Ping Method ICMP Ping

Ping Timeout Value 400

Ping Retry Count 1

Additional Options

Notes

External ID

Cancel Create

Ejemplo de la versión 3 de snmp, donde se usa un usuario y contraseña, con su nivel de seguridad y protocolo de autenticación:

Device [edit: SSH] 郎

General Device Options ^

Description ?

SSH

Hostname ?

ssh.rgrox.com

Location ?

None ▾

Poller Association ?

Main Poller ▾

Device Site Association ?

Edge ▾

Device Template ?

Net-SNMP Device ▾

Number of Collection Threads ?

1 Thread ▾

Disable Device ?

☒

SNMP Options

SNMP Version ?

Version 3 ▾

SNMP Security Level ?

authNoPriv ▾

SNMP Auth Protocol (v3) ?

SHA ▾

SNMP Username (v3) ?

pitaro

SNMP Password (v3) ?

\*\*\*\*\*

✔

Passphrases match

\*\*\*\*\*

SNMP Context (v3) ?

SNMP Engine ID (v3) ?

SNMP Port ?

161

SNMP Timeout ?

500

Maximum OIDs Per Get Request ?

20 OID's ▾

Bulk Walk Maximum Repetitions ?

Auto Detect on Re-Index ▾

Availability/Reachability Options ^

Downed Device Detection ?

Ping or SNMP Uptime ▾

Ping Method ?

ICMP Ping ▾

Ping Timeout Value ?

400

Ping Retry Count ?

1

Creamos el dispositivo y confirmamos que se creó correctamente

#### Paso 4

Si todo salió de manera correcta, podremos ver en la misma pestaña los datos del servidor en cuestión o si lo deseas, volver a la pestaña de Management > devices y ver el servidor en cuestión, como se muestra en las siguientes imágenes:

localhost:5555/cacti/host.php?action=edit

g Logs

it)

Logged in as admin

SNMP (snmp.rgrox.com)

SNMP Information

System: Linux snmp 6.1.0-20-amd64 #1 SMP PREEMPT\_DYNAMIC Debian 6.1.85-1 (2024-04-11) x86\_64

Uptime: 210313 (0days, 0hours, 35minutes)

Hostname: snmp

Location: Server ssh

Contact: ssh@example.org

\*Create New Device

\*Create Graphs for this Device

\*Re-Index Device

\*Enable Device Debug

\*Repopulate Poller Cache

\*View Poller Cache

\*Data Source List

\*Graph List

Ping Results

ICMP Ping Success (0.019 ms)

localhost:5555/cacti/host.php

Console Graphs Reporting Logs

Console Devices

Logged in as admin

Main Console

Create

Management

Devices

Sites

Trees

Graphs

Data Sources

Aggregates

Data Collection

Templates

Automation

Devices

郎 + ↗ ⚙

Site Any Data Collector Any Template Any Location All Go Clear Export

Search Enter a search term 🔍 Status Any Devices Default

All 1 Devices

Device Description	Hostname	ID	Graphs	Data Sources	Status	In State	Uptime	Poll Time	
SNMP	snmp.rgrox.com	1	11	18	Unknown	N/A	N/A	0	<input type="checkbox"/>

All 1 Devices

↳ Choose an action Go



# Conclusiones

Al finalizar esta práctica, se logró configurar correctamente un servidor SNMP en un entorno Debian, así como los agentes SNMP en clientes Debian y Windows, permitiendo la monitorización de una variedad de parámetros de rendimiento del sistema. La recolección de datos fue efectiva y se lograron visualizar diversos recursos, tales como el uso de CPU, memoria y almacenamiento de los sistemas, lo que proporciona una visión clara sobre el estado de los equipos monitorizados.

La implementación de alertas y notificaciones basadas en umbrales de rendimiento demostró ser crucial para la monitorización proactiva, permitiendo recibir notificaciones inmediatas ante eventos críticos. Además, la configuración de umbrales de operación y la correcta visualización de las notificaciones contribuyó a una respuesta rápida y eficiente frente a posibles incidentes.

Por último, el análisis de los datos recolectados permitió evaluar el rendimiento general del sistema de monitorización, identificando áreas de mejora y optimización. La práctica no solo proporcionó un entendimiento profundo de los fundamentos de SNMP, sino que también permitió aplicar estos conocimientos en un entorno real, mejorando la eficiencia y fiabilidad de la infraestructura de red gestionada.