

Configuración y funcionamiento de SNMP en Linux

Por: John A. Pérez B. ~ 20186748

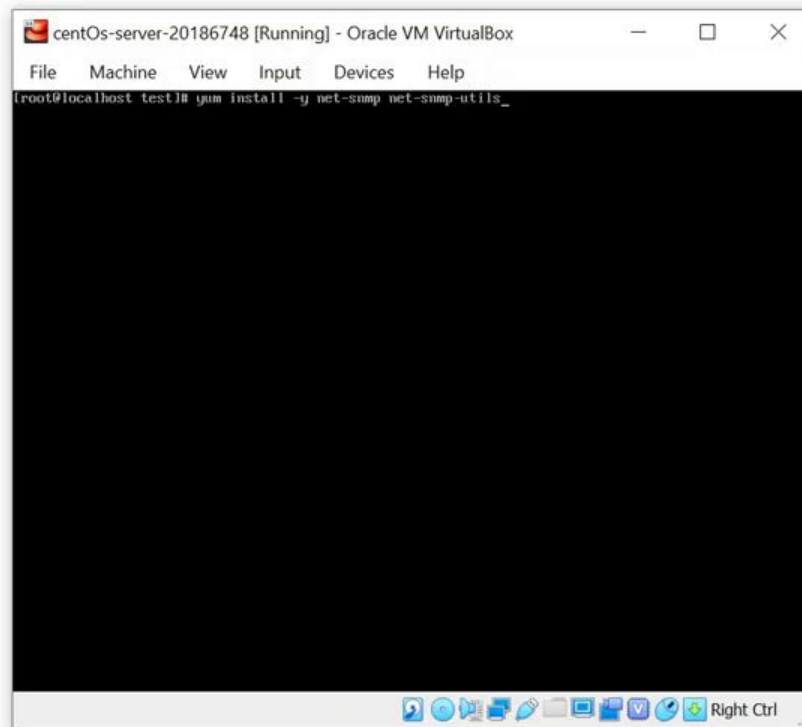
Este tutorial es un extracto del siguiente
video:

<https://youtu.be/u9Zt-UV E-1s>

Configuración del servidor

Paso 1

Instalamos los paquetes **net-snmp** y **net-snmp-utils** en nuestro servidor, y nuestro cliente de Linux para luego mostrar el funcionamiento de snmp



```
centOs-server-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@localhost test]# yum install -y net-snmp net-snmp-utils_
```

```
[centos20186748@localhost ~]$ sudo yum install net-snmp net-snmp-utils
```

```
[sudo] password for centos20186748:
```

```
Loaded plugins: fastestmirror, langpacks
```

```
Loading mirror speeds from cached hostfile
```

I

Paso 2

En nuestro servidor iniciamos la configuración de snmp, con el comando **snmpconf -g basic_setup**

```
[centos20186748@localhost ~]$ sudo yum install net-snmp net-snmp-utils
```

```
[sudo] password for centos20186748:
```

```
Loaded plugins: fastestmirror, langpacks
```

```
Loading mirror speeds from cached hostfile
```

```
* base: centos.brisanet.com.br
```

```
* extras: centos.brisanet.com.br
```

```
* rpmforge: mirror.teklinks.com
```

```
* updates: centos.brisanet.com.br
```

```
http://mirrors.uprm.edu/centos/7.6.1810/extras/x86_64/repodata
```

```
Trying other mirror.
```

```
To address this issue please refer to the below wiki article
```

```
https://wiki.centos.org/yum-errors
```

```
If above article doesn't help to resolve this issue please
```

```
http://centos.brisanet.com.br/7.6.1810/extras/x86_64/repodata
```

```
Trying other mirror.
```

```
http://ftp.unicamp.br/pub/centos/7.6.1810/extras/x86_64/repodata
```

```
Trying other mirror.
```

```
http://centos.brnet.net.br/centos/7.6.1810/extras/x86_64/repodata
```

```
Trying other mirror.
```

```
http://mirror.globo.com/centos/7.6.1810/extras/x86_64/repodata
```

```
Trying other mirror.
```

```
http://mirror.ufscar.br/centos/7.6.1810/extras/x86_64/repodata
```

```
Trying other mirror.
```

```
http://centos.usetelecom.com.br/centos/7.6.1810/extras/x86_64/repodata
```

```
Trying other mirror.
```

```
http://mirror.ufam.edu.br/centos/7.6.1810/extras/x86_64/repodata
```

```
Trying other mirror.
```

```
http://mirror.facom.ufms.br/centos/7.6.1810/extras/x86_64/repodata
```

```
Trying other mirror.
```

```
http://linorg.usp.br/CentOS/7.6.1810/extras/x86_64/repodata
```

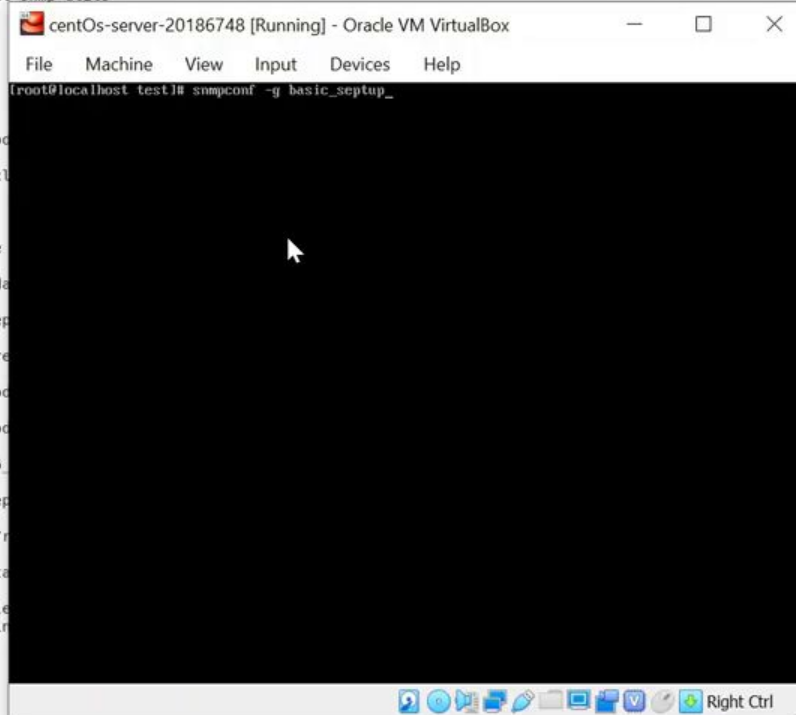
```
Trying other mirror.
```

```
Package 1:net-snmp-5.7.2-38.el7_6.2.x86_64 already installed
```

```
Package 1:net-snmp-utils-5.7.2-38.el7_6.2.x86_64 already installed
```

```
Nothing to do
```

```
[centos20186748@localhost ~]$
```



Paso 3

En este caso simplemente configuraremos el snmp v3, sin agregar ningún usuario debido a que lo agregaremos más tarde, por lo que simplemente damos que si a las opciones iniciales, y no a las relacionadas con la creación de usuario y autenticación.

```
centOs-server-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Read in which (default = all):
=====
*** Beginning basic system information setup ***
=====
Do you want to configure the information returned in the system MIB group (contact info, etc)? (default = y): no
=====
*** BEGINNING ACCESS CONTROL SETUP ***
=====
Do you want to configure the agent's access control? (default = y):
Do you want to allow SNMPv3 read-write user based access (default = y):

Configuring: rwuser
Description:
  a SNMPv3 read-write user
  arguments: user [noauth|authpriv] [restriction_oid]

The SNMPv3 user that should have read-write access:
The minimum security level required for that user [noauth|authpriv, default = auth]:
The OID that this community should be restricted to [if appropriate]:

Finished Output: rwuser
Do another rwuser line? (default = y): no
Do you want to allow SNMPv3 read-only user based access (default = y): no
Do you want to allow SNMPv1/v2c read-write community access (default = y):

Configuring: rwcommunity
Description:
  a SNMPv1/SNMPv2c read-write access community name
  arguments: community [default|hostname:network/bits] [oid]

Enter the community name to add read-write access for:
The hostname or network address to accept this community name from [RETURN for all]:
The OID that this community should be restricted to [RETURN for no-restriction]:

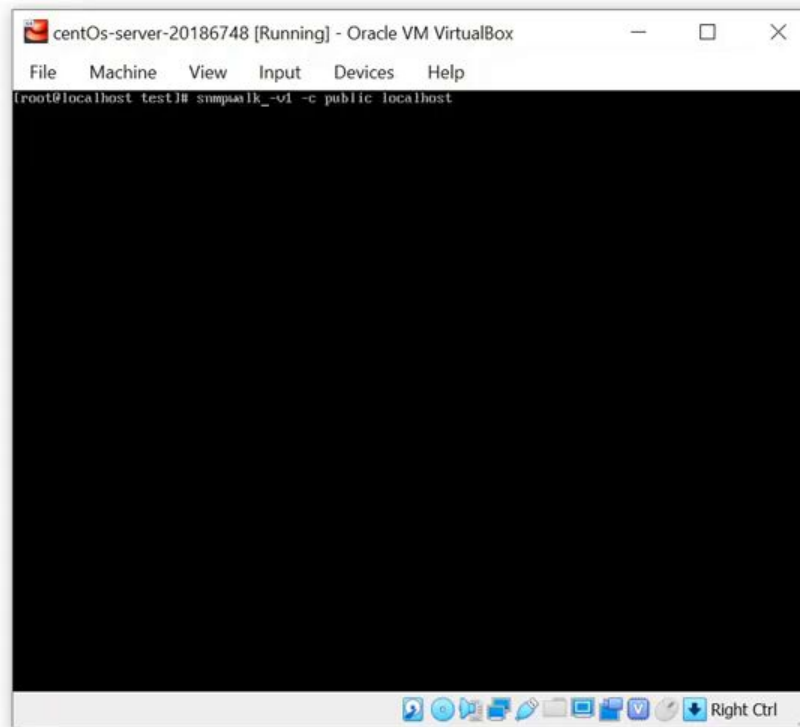
Finished Output: rwcommunity
Do another rwcommunity line? (default = y): no
```



Paso 4

Para probar si snmp está correctamente configurado ejecutamos un walk de versión 1* directamente desde el servidor, con el comando `snmpwalk -v1 -c public localhost`.

*la diferencia entre las versiones de snmp varía en el tipo de seguridad que ofrecen o autenticación que requieren para obtener acceso a la información



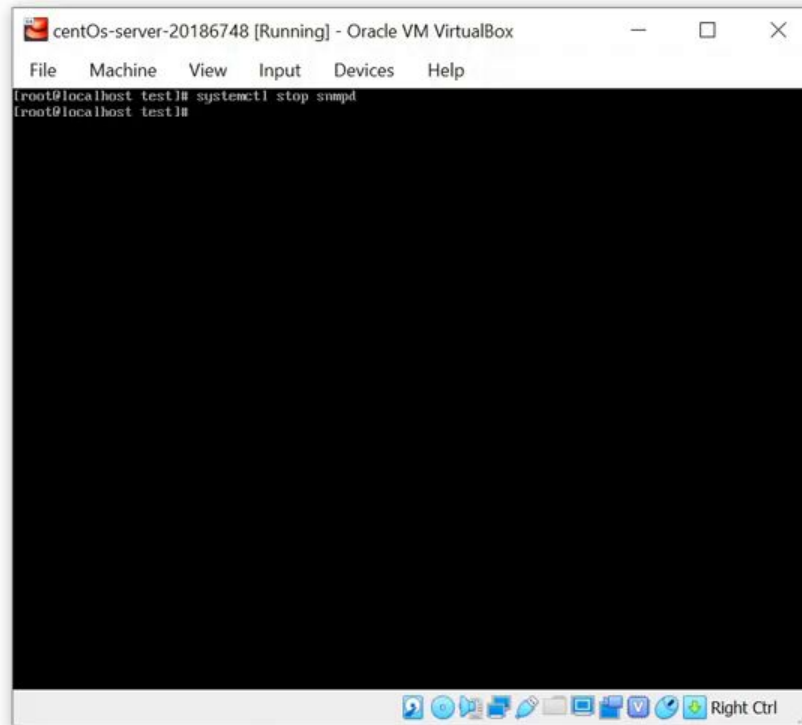
```
centOs-server-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@localhost test]# snmpwalk -v1 -c public localhost
```

El resultado debería ser el siguiente, indicando que snmp está configurado correctamente. Mostrándonos alguna de las variables que snmp utiliza para guardar la información del sistema.

```
centOs-server-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
SNMPv2-MIB::sysName.0 = STRING: localhost.localdomain
SNMPv2-MIB::sysLocation.0 = STRING: Unknown (edit /etc/snmp/snmpd.conf)
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::sysORID.1 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.6 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: SNMP-USER-BASED-ACM-MIB::ucmBasicGroup
SNMPv2-MIB::sysORID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance
SNMPv2-MIB::sysORID.10 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB
SNMPv2-MIB::sysORDescr.1 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.2 = STRING: The management information definitions for the SNMP User-based Security Model.
SNMPv2-MIB::sysORDescr.3 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing TCP implementations
SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing IP and ICMP implementations
SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing UDP implementations
SNMPv2-MIB::sysORDescr.8 = STRING: View-based Access Control Model for SNMP.
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: (3) 0:00:00.03
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::sysORUpTime.4 = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::sysORUpTime.5 = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::sysORUpTime.6 = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::sysORUpTime.7 = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::sysORUpTime.9 = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::sysORUpTime.10 = Timeticks: (3) 0:00:00.03
HOST-RESOURCES-MIB::hrSystemUpTime.0 = Timeticks: (891119) 2:28:31.19
End of MIB
(root@localhost test)ll
```

Paso 5

Para comenzar con la creación del usuario con el que accederemos remotamente detenemos el snmp, con el comando **systemctl stop snmpd**



```
centOs-server-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@localhost test]# systemctl stop snmpd
[root@localhost test]#
```


Paso 6

Para comenzar con la creación del usuario con el que accederemos remotamente utilizamos el comando **net-snmp-create-v3-user**. Luego colocamos el nombre del usuario y la frase de autenticación, debido a que estamos utilizando la versión 3 de snmp.

```
centOs-server-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@localhost test]# systemctl stop snmpd
[root@localhost test]# net-snmp-create-v3-user
Enter a SNMPv3 user name to create:
centos20186748
Enter authentication pass-phrase:
20186748
Enter encryption pass-phrase:
[press return to reuse the authentication pass-phrase]
adding the following line to /var/lib/net-snmp/snmpd.conf:
    createllser centos20186748 MD5 "20186748" DES
adding the following line to /etc/snmp/snmpd.conf:
    rauser centos20186748
[root@localhost test]#
```

Paso 7

Luego reiniciamos el servicio con **systemctl restart snmpd** y comprobamos el estado con **systemctl status snmpd**

```
centOs-server-20186748 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@localhost test]# systemctl restart snmpd
[root@localhost test]# systemctl status snmpd
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/usr/lib/systemd/system/snmpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Tue 2019-10-01 16:38:02 EDT; 5s ago
     Main PID: 4631 (snmpd)
    CGroup: /system.slice/snmpd.service
            └─4631 /usr/sbin/snmpd -LSB-6d -f

Oct 01 16:38:01 localhost.localdomain systemd[1]: Starting Simple Network Management Protocol (.....
Oct 01 16:38:02 localhost.localdomain snmpd[4631]: NET-SNMP version 5.7.2
Oct 01 16:38:02 localhost.localdomain systemd[1]: Started Simple Network Management Protocol (S.....
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost test]#
```

Trabajando con SNMP

SNMP nos ofrece un sistema simple para extraer información de nuestro servidor. Cada una de las diferentes informaciones se almacenan en un tipo de variable las cuales llamamos con los comandos **snmpget** y **snmwalk**, donde dependiendo la versión que tengamos configurada asignamos los parámetros de seguridad. En este caso veremos el funcionamiento con la versión 3. Su sintaxis es **snmpget -v3 -l [tipo de autenticación] -u [usuario] -a MD5 -A [frase de autenticación] [ip del servidor] [variable]**. Vamos a utilizar como ejemplo **sysUpTime.0** que nos muestra el tiempo desde que este sistema de administración (el snmp) fue inicializado.

centos20186748@localhost:~

File Edit View Search Terminal Help

```
[centos20186748@localhost ~]$ snmpget -v3 -l authNoPriv -u centos20186748 -a MD5 -A 20186748 10.0.2.4 sysUpTime.0  
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (10301) 0:01:43.01  
[centos20186748@localhost ~]$
```



centos20186748@localhost:~

Documents

snmp (~/Documents) - gedit

1 / 4

Como habíamos mencionado snmp almacena la información en forma de variables, donde cada una almacena un dato específico, por lo que simplemente basta con cambiar la variable al final para acceder a dicha información. Ahora veremos algunas variables practica, como **hrSystemInitialLoadParameters.0**, que nos muestra los parametros iniciales del sistema.

centos20186748@localhost:~

File Edit View Search Terminal Help

```
[centos20186748@localhost ~]$ snmpget -v3 -l authNoPriv -u centos20186748 -a MD5 -A 20186748 10.0.2.4 hrSystemInitialLoadParameters.0  
HOST-RESOURCES-MIB::hrSystemInitialLoadParameters.0 = STRING: "BOOT_IMAGE=/vmlinuz-3.10.0-1062.1.1.el7.x86_64 root=UUID=5d64b2ce-cc25-4a20-b0bd-dccabf374ecc ro crashkerne  
[centos20186748@localhost ~]$
```

```
centOs-server-20186748 [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
(root@localhost usr)# cd /src  
-bash: cd: /src: No such file or directory  
(root@localhost usr)# cd ./src  
(root@localhost src)# ls  
debug kernels  
(root@localhost src)# cd ./kernels  
(root@localhost kernels)# ls  
3.10.0-1062.1.1.el7.x86_64 3.10.0-1062.1.1.el7.x86_64.debug  
(root@localhost kernels)#
```

centos20186748@localhost:~

Documents

snmp (~/.Documents)

Right Ctrl

1 / 4

Right Ctrl

Otro de los tipos de variables son las **hrDeviceDesc**, que nos muestran información acerca del hardware del equipo. En el caso del **hrDeviceDesc.196608**. Nos da información acerca del procesador de nuestro servidor.

centos20186748@localhost:~

File Edit View Search Terminal Help

```
[centos20186748@localhost ~]$ snmpget -v3 -l authNoPriv -u centos20186748 -a MD5 -A 20186748 10.0.2.4 hrDeviceDescr.196608
HOST-RESOURCES-MIB::hrDeviceDescr.196608 = STRING: GenuineIntel: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz
[centos20186748@localhost ~]$
```



centos20186748@localhost:~

Documents

snmp (~/.Documents) - gedit

1 / 4

El **hrDeviceDesc.262146**. Nos da información acerca de la interfaz de red activa en el servidor.

centos20186748@localhost:~

File Edit View Search Terminal Help

```
[centos20186748@localhost ~]$ snmpget -v3 -l authNoPriv -u centos20186748 -a MD5 -A 20186748 10.0.2.4 hrDeviceDescr.196608
HOST-RESOURCES-MIB::hrDeviceDescr.196608 = STRING: GenuineIntel: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz
[centos20186748@localhost ~]$ snmpget -v3 -l authNoPriv -u centos20186748 -a MD5 -A 20186748 10.0.2.4 hrDeviceDescr.262146
HOST-RESOURCES-MIB::hrDeviceDescr.262146 = STRING: network interface enp0s3
[centos20186748@localhost ~]$
```



centos20186748@localhost:~

Documents

snmp (~/.Documents) - gedit

1 / 4

Otro de los tipos de variables son las **hrInstalled**, que nos muestran informacion acerca de los programas que tenemos instalado. **hrInstalled** tambien nos da informacion especifica de cierto programa, como el nombre del mismo con **hrInstalledName.[id]**.

centos20186748@localhost:~

File Edit View Search Terminal Help

```
[centos20186748@localhost ~]$ snmpget -v3 -l authNoPriv -u centos20186748 -a MD5 -A 20186748 10.0.2.4 hrSWInstalledName.495  
HOST-RESOURCES-MIB::hrSWInstalledName.495 = STRING: "zlib-devel-1.2.7-18.el7"  
[centos20186748@localhost ~]$
```



centos20186748@localhost:~

Documents

snmp (~/.Documents) - gedit

1 / 4

Con **hrInstalled**, también podemos conseguir la fecha exacta en la que el programa se instaló, simplemente agregando **hrInstalledDate.[id]**

centos20186748@localhost:~

File Edit View Search Terminal Help

```
[centos20186748@localhost ~]$ snmpget -v3 -l authNoPriv -u centos20186748 -a MD5 -A 20186748 10.0.2.4 hrSWInstalledName.495
HOST-RESOURCES-MIB::hrSWInstalledName.495 = STRING: "zlib-devel-1.2.7-18.el7"
[centos20186748@localhost ~]$ snmpget -v3 -l authNoPriv -u centos20186748 -a MD5 -A 20186748 10.0.2.4 hrSWInstalledDate.495
HOST-RESOURCES-MIB::hrSWInstalledDate.495 = STRING: 2019-9-30,16:37:35.0,-4:0
[centos20186748@localhost ~]$
```



centos20186748@localhost:~

Documents

snmp (~/.Documents) - gedit

1 / 4