Entre otras cosas SNMP se utiliza para poder monitorizar maquinas que tengan este servicio arrancado

fuente: www.linuxparatodos.net

SNMP (Simple Network Management Protocol) es un protocolo ampliamente utilizado en la administración de redes para supervisar la salud y el bienestar del equipo de la red, equipo de computo y otros dispositivos. Net- **SNMP** , el software utilizado en este documento, es un conjunto de aplicaciones utilizados para implementar
SNMP
v1,
SNMP
v2c y
SNMP
v3 utilizando IPv4 y/o IPv6.

Software requerido.

- net-**snmp**-5.0.9
- net-**snmp**-utils-5.0.9

Snmpd es un servicio que regularmente se instala de modo predefinido en la mayoría de las distribuciones, aunque no está habilitado en los servicios de arranque del sistema. El paquete net-**snmp**-utils no suele instalarse de modo predefinido, por tanto se puede ejecutar lo siguiente para realizar la instalación del software necesario:

Sistemas que utilicen yum:

yum -y install net-	**snmp**	net-	**snmp**	-utils
up2date -i net-	**snmp**	net-	**snmp**	-utils

Procedimientos

Fichero de configuración.

El fichero /**etc**/**snmp**/**snmpd.conf** que se instala por defecto es una verdadera maraña de comentarios y opciones de todo tipo. Lo más recomendable será cerrar un fichero nuevo y limpio de contenido.

```
cd /etc/ snmp
mv snmpd.conf snmpd.conf-OLD
touch snmpd.conf
```

Listas de control de acceso.

Se deben crear las listas de control de acceso (ACL) correspondientes en el fichero /**etc**/**snmp**/**snmpd.conf**
y que servirán para definir quien tendrá acceso hacia el servicio
snmpd
. A una de estas listas se le otorgará permiso de acceso de lectura y escritura para lo que sea necesario y a la otra de solo lectura. Por razones de seguridad solo la interfaz 127.0.0.1 será la de lectura escritura. Se otorgará permiso de acceso de solo lectura a una red o bien a una IP en la otra lista de control de acceso (ACL).

De modo tal se podrían agregar un par de líneas como las siguientes:

```
com2sec local 127.0.0.1/32 Cl4v3-d3-Acc3s0
com2sec miredlocal 192.168.1.0/24 Cl4v3-d3-Acc3s0
```

En lo anterior la primera línea significa que habrá una lista de control de acceso denominada *«local»*
y que corresponderá solo a 127.0.0.1/32, asignando
Cl4v3-d3-Acc3s0
como clave de acceso. La segunda línea hace lo mismo pero definiendo a la red 192.168.1.0/24. Se puede definir lo que uno guste mientras no sea la clave de root, esto porque dicha clave se transmite a través de la red en forma de texto simple (es decir, sin cifrar).

Definición de grupos.

Se van a crear dos grupos: **MyRWGroup** y **MyROGroup**. El primero será un grupo al que se asignarán más adelante permisos de **lectura escritura**
y el segundo será un grupo al que posteriormente se asignarán permisos de
solo lectura
. Por cada grupo se asignan tres líneas que especifican el tipo de acceso que se permitirá en un momento dado a un grupo en particular. Es decir,
MyRWGroup
se asocia a
local
y

MyROGroup
a
miredlocal
.

```
#Se asigna local al gru lectura escritura
group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local

#Se asigna miredlocal a solo lectura
group MyROGroup v1 miredlocal
group MyROGroup v2c miredlocal
group MyROGroup usm miredlocal
```

Ramas permitidas.

Se especifican las ramas que se van a permitir ver a través del servicio. Lo más común, para, por ejemplo, utilizarse con MRTG, es lo siguiente:

```
## name   incl/excl subtree   mask(optional)
view all  included  .1       80
```

Asignación de permisos a los grupos.

Se debe especificar que permisos tendrán los dos grupos, MyROGroup y MyRWGroup. Son de especial interés las últimas columnas.

```
## group        context  sec.model sec.level prefix read   write notif
access MyROGroup &amp;quot;&amp;quot;      any      noauth    exact  all    none  none
access MyRWGroup &amp;quot;&amp;quot;      any      noauth    exact  all    all   all
```

Parámetros de carácter informativo.

Se definen dos parámetros de carácter informativo para que cuando utilicen aplicaciones cliente como MRTG se incluya algo de información acerca de que sistema se está accediendo.

```
syslocation Servidor     Linux                    en SU-SERVIDOR.algun-dominio.net
syscontact Administrador (fulano@algun-dominio.net)
```

Un ejemplo real.

El ejemplo que mostramos a continuación se utiliza en todas las PC que posee el autor en casa y la oficina. Solo bastará reemplazar **redlocal** por lo que uno considere apropiado y reemplazar **192.168.1.0/24** por **la red** o la IP desde donde se

requiera acceder con un cliente
snmp
, como MRTG.

```
# Listas de control de acceso (ACL)
## sec.name source community (alias clave de acceso)
com2sec local 127.0.0.1/32 Cl4v3-d3-Acc3s0
com2sec miredlocal 192.168.1.0/24 Cl4v3-d3-Acc3s0 #Se asigna ACL al grupo de lectura escritura
group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local #Se asigna ACL al grupo de solo lectura
group MyROGroup v1 miredlocal
group MyROGroup v2c miredlocal
group MyROGroup usm miredlocal # Ramas MIB que se permiten ver
## name   incl/excl subtree   mask(optional)
view all  included  .1       80 # Establece permisos de lectura y escritura
## group        context  sec.model sec.level prefix read   write notif
access MyROGroup &amp;quot;&amp;quot;      any       noauth    exact  all    none  none
access MyRWGroup &amp;quot;&amp;quot;      any       noauth    exact  all    all   all # Información de Contacto de
syslocation Servidor      Linux                    en amdk6.linuxparatodos.com.mx
syscontact Administrador (fulano@algun-dominio.net)
```

Si es necesario añadir más equipos para que accedan al servicio **snmp**, solo hay que hacer lo siguiente:

1.

Agregar una ACL con un nombre único. Ejemplo:

```
com2sec                 micueva                 192.168.1.251 Cl4v3-d3-Acc3s0
```

2.

Agregar un juego reglas que asignen al grupo, en este caso **micueva**, con lo siguiente:

```
group                   otrogrupo               v1 local
group                   otrogrupo               v2c local
group                   otrogrupo               usm local
```

3.

Agregar una línea donde se establece que permisos tendrá el grupo **otrogrupo**. En este ejemplo, va a ser de solo lectura:

```
access MyROGroup &quot;&quot; any noauth exact all none none
```

Iniciar el servicio y añadirlo a los servicios de arranque del sistema

Inicie el servicio de **SNMP** y añada éste al resto de los servicios que arrancan junto con el sistema:

```
service snmpd start
chkconfig snmpd on
```

Comprobaciones.

Suponiendo que sea signó como clave de acceso **Cl4v3-d3-Acc3s0** en un sistema cuya dirección IP es **192.168.1.254**, para probar si la configuración funciona, solo hay que ejecutar los dos siguiente mandatos a fin verificar que devuelvan información acerca del sistema consultado.

```
snmpwalk -v 1 192.168.1.254 -c Cl4v3-d3-Acc3s0
snmpwalk -v 1 192.168.1.254 -c Cl4v3-d3-Acc3s0 interfac
```