

Monitorización de infraestructuras con Nagios.

Ángela Bonilla Gómez

Curso 2019/2020

I.E.S. Triana

Administración de sistemas informáticos en red.

Tabla de Contenidos

Capítulo 1. Introducción e información general.....	6
Paso 1. Introducción.....	6
Paso 2. Datos generales del Proyecto.....	6
Paso 3. Objetivos y características.....	7
Paso 4. Recursos y entornos utilizados.....	9
Capítulo 2. Instalación y configuración de Nagios.....	11
Paso 1. Requisito previo.....	11
Paso 2. Crear usuario Nagios.....	16
Paso 3. Instala el servicio Nagios Core.....	17
Paso 4. Configura Apache con autenticación.....	21
Paso 5. Instalación de complementos de Nagios.....	24
Paso 6. Verificar la configuración.....	25
Paso 7. Acceder a la interfaz web de Nagios.....	27
Capítulo 3. Monitorización de cliente Linux.....	30
Paso 1. Configurar NRPE en el host de Linux.....	30
Paso 2. Agregar host de Linux en Nagios.....	34
Paso 3. Verificar el host en la interfaz web de Nagios.....	38
Capítulo 4. Monitorización de cliente Windows.....	40
Paso 1. Instalar NSClient ++.....	40
Paso 2. Agregar host en el servidor Nagios.....	42
Paso 3. Verificar el host en la interfaz web de Nagios.....	46

	3
Paso 4. Configurar IP fija.....	47
Capítulo 5. Notificaciones por correo.....	51
Paso 1. Configuración.....	51
Paso 2. Resultado.....	53
Capítulo 6. Monitorizar servicio Linux.....	54
Paso 1. Instalaciones necesarias.....	54
Paso 2. Configuraciones necesarias.....	55
Paso 3. Monitorizar servicio SSH.....	57
Paso 4. Monitorizar servicio HTTP.....	58
Paso 5. Monitorizar servicio PING.....	59
Paso 6. Monitorizar disco.....	60
Paso 7. Monitorizar usuarios.....	61
Paso 8. Monitorizar procesos.....	62
Paso 9. Monitorizar swap.....	63
Paso 10. Monitorizar carga.....	64
Paso 11. Monitorizar TCP.....	65
Paso 12. Comprobación del funcionamiento.....	66
Capítulo 7. Monitorizar servicios Windows.....	67
Capítulo 8. Asignar iconos a Nagios. Status map.....	75
Paso 1. Dónde localizar las imágenes existentes.....	75
Paso 2. Modificación de los ficheros.....	76
Paso 3. Visualizar las imágenes.....	78

Capítulo 9. Instalación y configuración de PNP4Nagios.....	80
Paso 1. Instalaciones necesarias.....	80
Paso 2. Ficheros de configuración.....	84
Paso 3. Solucionar errores.....	91
Paso 4. Graficación de hosts y servicios.....	93
Paso 5. Comprobación del funcionamiento.....	98
Capítulo 10-Monitorizar MySQL.....	102
Paso 1. Instalación y configuración de la máquina.....	102
Paso 2. Descargar plugin necesario.....	109
Paso 3. Instalar el plugin.....	110
Paso 4. Configurar permisos de MySQL.....	112
Paso 5. Configurar archivos de Nagios.....	113
Capítulo 11-Crear y añadir mi propio plugin.....	118
Paso 1. Creación de los comandos.....	118
Paso 2. Creación y ejecución del script.....	119
Paso 3. Agregar servicio de Nagios.....	121
Paso 4. Comprobación del funcionamiento.....	124
Capítulo 12-Monitorizar impresora.....	125
Paso 1. Requisitos previos.....	125
Paso 2. Comprobar IP de la impresora a monitorizar.....	129
Paso 3. Configuración del servidor.....	131
Paso 4. Comprobar estado y funcionamiento.....	137

Capítulo 13. Otras opciones del menú de Nagios.....	139
Capítulo 14. Nagios Log Server.....	148
Paso 1. Qué es, características.....	148
Paso 2. Elementos vistos en la práctica.....	149
Capítulo 15. Nagios Network Analyzer.....	158
Paso 1. Qué es, características.....	158
Paso 2. Elementos vistos en la práctica.....	161
Capítulo 16. Total de dispositivos monitorizados.....	168
Lista de referencias.....	169

Capítulo 1

Introducción e información general

Paso 1. Introducción

En este documento, mostraremos un proyecto en el cual se instala Nagios, se configura y se demuestra sus funcionalidades.

- ¿Qué es Nagios?
 - Nagios es un sistema de monitorización de redes de código abierto, que vigila los equipos (hardware) y servicios, alertando de un mal funcionamiento obteniendo métricas en tiempo real, pudiendo prevenir problemas de disponibilidad o desastres en la infraestructura informática.
 - Una de sus características principales es la monitorización de servicios de red (SMTP, HTTP, POP, etc.), la monitorización de los recursos de sistemas de hardware, independencias de sistemas operativos, monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.

Paso 2. Datos generales del Proyecto.

Se va a montar un entorno simulado monitorizando dos máquinas (Linux, Windows) en el que veremos la carga CPU, RAM, Disco duro, etc. También utilizaremos algunos servicios y haremos uso de plugins.

- **Necesidades a cubrir en el contexto real:**

- En el ámbito laboral, el núcleo central, es la información de la estructura TI de las empresas.
- La red es vital en la agilización de las operaciones empresariales con la que es posible monitorizar el rendimiento para garantizar la estabilidad y la seguridad de la información.
- Es ahí cuando surge la idea de utilizar un sistema como Nagios con la confianza que aporta para las redes, servidores y aplicaciones, ya que para muchas empresas es fundamental garantizar la eficiencia y la funcionalidad de las operaciones informáticas en todo momento.

Paso 3. Objetivos y características.

El objetivo del proyecto es tener controlado los servicios, detectar posibles errores a tiempo tanto de hardware, software y servicios, para poder repararlo.

Que las organizaciones y sus áreas puedan acceder a toda la información sobre el funcionamiento, la disponibilidad y el rendimiento de la red (y servicios conectados) para mejorar el tiempo de actividad, disminuir tiempos de espera y optimizar las operaciones.

- **Características de Nagios:**

- Genera alertas que te permite afrontar el problema a tiempo.
- Vigila de forma constante las redes y los sistemas de una empresa.
- Capaz de reconocer puntos fuertes y débiles de todos los sistemas en cada momento.

- Es de código abierto.
- Ofrece imagen de todos los componentes críticos.
- Multitud de plugins desarrollados por terceros para monitorizar prácticamente todo.

- **Alternativas a Nagios:**

- Nrpe:
 - Es un programa que se comunica entre el servidor nagios y los equipos a monitorizar, el cual indica el estado de todo lo que configuremos. De NRPE deberemos realizar una pequeña instalación en el cliente. La diferencia más importante es que NRPE ejecuta chequeos en modo activo.
- Openssh-server:
 - Es un programa que nos facilita el intercambio de ficheros, el control de equipos y la ejecución de servicios y ficheros.
- Apache2:
 - Es el programa que nos dará el servicio web para el entorno web de las distintas aplicaciones.
- Pnp4nagios:
 - Te muestra en forma de gráficos cada servicio de cada host de diferentes periodos de tiempo y almacena automáticamente los datos en bases de datos RRD.
 - Es un módulo oportuno para los administradores de redes, ya que tienes un buen control administrativo de todos los servicios en diferentes periodos

de tiempo, pudiendo hacer comparativas de calidad entre los servicios y otras opciones que desee el administrador.

Paso 4. Recursos y entornos utilizados.

- VirtualBox
 - Máquina virtual con Ubuntu Server 18.04
 - 2048 MB de RAM
 - 50 GB de memoria
 - Configuración de red: adaptador puente.
 - Máquina virtual con Ubuntu Desktop 18.04
 - 1576 MB de RAM
 - 40 GB de memoria
 - Configuración de red: adaptador puente.
 - Máquina virtual con Windows 7
 - 2048 MB de RAM
 - 10 GB de memoria
 - Configuración de red: adaptador puente.
 - Máquina virtual con Ubuntu Desktop 14.04
 - 1525 MB de RAM
 - 10 GB de memoria
 - Configuración de red: adaptador puente.

- Máquina real con Windows 10
- Impresora EPSON
- Nagios
- pnp4nagios
- Nagios LS
- Nagios NA

Capítulo 2

Instalación y configuración de Nagios.

Paso 1. Requisitos previos.

Para realizar este proyecto he usado un sistema Ubuntu, por lo que suponemos que está ya instalado, nuestro primer requisito entonces es instalar Apache y PHP. Usaremos los siguientes comandos para completarlo:

- Usaremos los siguientes comandos para instalar los paquetes requeridos para Nagios:

- `sudo apt-get update`

```
root@usuario:/home/usuario# apt-get update
Obj:1 http://es.archive.ubuntu.com/ubuntu bionic InRelease
Des:2 http://es.archive.ubuntu.com/ubuntu bionic-updates InRelease [88,7 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu bionic-backports InRelease [74,6 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu bionic-security InRelease [88,7 kB]
Des:5 http://es.archive.ubuntu.com/ubuntu bionic/main Translation-es [364 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu bionic/restricted Translation-es [1.960 B]
Des:7 http://es.archive.ubuntu.com/ubuntu bionic/universe Translation-es [1.259 kB]
Des:8 http://es.archive.ubuntu.com/ubuntu bionic/multiverse Translation-es [74,9 kB]
Descargados 1.952 kB en 3s (566 kB/s)
Leyendo lista de paquetes... Hecho
```

- `sudo apt-get install wget build-essential unzip openssl libssl-dev`

```
root@usuario:/home/usuario# apt-get install wget build-essential unzip openssl libssl-dev
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
openssl ya está en su versión más reciente (1.1.1-1ubuntu2.1~18.04.5).
fijado openssl como instalado manualmente.
wget ya está en su versión más reciente (1.19.4-1ubuntu2.2).
fijado wget como instalado manualmente.
Se instalarán los siguientes paquetes adicionales:
binutils binutils-common binutils-x86-64-linux-gnu cpp cpp-7 dpkg-dev fakeroot g++ g++-7
gcc-7 gcc-7-base libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl
libasan4 libatomici libbinutils libc-dev-bin libc6-dev libcc1-0 libcilkrtss5 libdpkg-perl
libfakeroot libfile-fcntllock-perl libgcc-7-dev libgomp1 libis119 libitm1 liblsan0 libmpc
libmpx2 libquadmath0 libstdc++-7-dev libtsan0 libubsan0 linux-libc-dev make manpages-dev
Paquetes sugeridos:
binutils-doc cpp-doc gcc-7-locales debian-keyring g++-multilib g++-7-multilib gcc-7-doc
libstdc++6-7-dbg gcc-multilib autoconf automake libtool flex bison gdb gcc-doc gcc-7-mult
libgcc1-dbg libgomp1-dbg libitm1-dbg libatomici-dbg libasan4-dbg liblsan0-dbg libtsan0-db
libubsan0-dbg libcilkrtss5-dbg libmpx2-dbg libquadmath0-dbg glibc-doc bzr libssl-doc
libstdc++-7-doc make-doc zip
Se instalarán los siguientes paquetes NUEVOS:
binutils binutils-common binutils-x86-64-linux-gnu build-essential cpp cpp-7 dpkg-dev fak
g++ g++-7 gcc gcc-7 gcc-7-base libalgorithm-diff-perl libalgorithm-diff-xs-perl
libalgorithm-merge-perl libasan4 libatomici libbinutils libc-dev-bin libc6-dev libcc1-0
libcilkrtss5 libdpkg-perl libfakeroot libfile-fcntllock-perl libgcc-7-dev libgomp1 libis11
libitm1 liblsan0 libmpc3 libmpx2 libquadmath0 libssl-dev libstdc++-7-dev libtsan0 libubsa
linux-libc-dev make manpages-dev unzip
0 actualizados, 42 nuevos se instalarán, 0 para eliminar y 21 no actualizados.
Se necesita descargar 44,8 MB de archivos.
Se utilizarán 174 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

- Ahora Apache y PHP:

- sudo apt-get install apache2 php libapache2-mod-php php-gd libgd-dev

```
root@usuario:/home/usuario# apt-get install apache2 php libapache2-mod-php php-gd libgd-dev
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  apache2-bin apache2-data apache2-utils fontconfig-config fonts-dejavu-core libapache2-mod-php7.2
  libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libexpat1-dev libfontconfig1
  libfontconfig1-dev libfreetype6-dev libgd3 libice-dev libice6 libjbig-dev libjbig0 libjpeg-dev
  libjpeg-turbo8 libjpeg-turbo8-dev libjpeg8 libjpeg8-dev liblua5.2-0 liblzma-dev libpng-dev
  libpng-tools libpthread-stubs0-dev libsm-dev libsm6 libsodium23 libtiff-dev libtiff5
  libtiff5-dev libtiffxx5 libvpx-dev libvpx5 libwebp6 libx11-dev libx11-doc libxau-dev libxcb1-dev
  libxdmcp-dev libxpm-dev libxpm4 libxt-dev libxt6 php-common php7.2 php7.2-cli php7.2-common
  php7.2-gd php7.2-json php7.2-opcache php7.2-readline pkg-config ssl-cert x11-common
  x11proto-core-dev x11proto-dev xorg-sgml-doctools xtrans-dev zlib1g-dev
Paquetes sugeridos:
  www-browser apache2-doc apache2-suexec-pristine | apache2-suexec-custom php-pear libgd-tools
  libice-doc liblzma-doc libsm-doc libxcb-doc libxt-doc openssl-blacklist
Se instalarán los siguientes paquetes NUEVOS:
  apache2 apache2-bin apache2-data apache2-utils fontconfig-config fonts-dejavu-core
  libapache2-mod-php libapache2-mod-php7.2 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libexpat1-dev libfontconfig1 libfontconfig1-dev libfreetype6-dev libgd-dev
  libgd3 libice-dev libice6 libjbig-dev libjbig0 libjpeg-dev libjpeg-turbo8 libjpeg-turbo8-dev
  libjpeg8 libjpeg8-dev liblua5.2-0 liblzma-dev libpng-dev libpng-tools libpthread-stubs0-dev
  libsm-dev libsm6 libsodium23 libtiff-dev libtiff5 libtiff5-dev libtiffxx5 libvpx-dev libvpx5
  libwebp6 libx11-dev libx11-doc libxau-dev libxcb1-dev libxdmcp-dev libxpm-dev libxpm4 libxt-dev
  libxt6 php php-common php-gd php7.2 php7.2-cli php7.2-common php7.2-gd php7.2-json
  php7.2-opcache php7.2-readline pkg-config ssl-cert x11-common x11proto-core-dev x11proto-dev
  xorg-sgml-doctools xtrans-dev zlib1g-dev
0 actualizados, 69 nuevos se instalarán, 0 para eliminar y 21 no actualizados.
Se necesita descargar 18,0 MB de archivos.
Se utilizarán 69,7 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] _
```

- Debemos poner la IP fija para no perder la IP de nuestro servidor, ya que por defecto está activado el DHCP y nos la irá cambiando, por lo que tendríamos que estar continuamente actualizando los archivos de configuración.

```
GNU nano 2.9.3                               /etc/network/interfaces

# ifupdown has been replaced by netplan(5) on this system. See
# /etc/netplan for current configuration.
# To re-enable ifupdown on this system, you can run:
#   sudo apt install ifupdown

#Configuracion de IP fija_
auto enp0s3
iface enp0s3 inet static
address 192.168.1.141
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1

[ Wrote 13 lines ]
```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^Y Replace ^U Uncut Text ^T To Spell ^L Go To Line M-E Redo

- También tendremos que modificar este otro fichero:

- nano /etc/netplan/50-cloud-init.yaml

```
GNU nano 2.9.3                               /etc/netplan/50-cloud-init.yaml      Modified

# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.1.141/24]
version: 2

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^D Cur Pos  M-U Undo
^X Exit      ^R Read File  ^Y Replace   ^U Uncut Text ^T To Spell  ^C Go To Line M-E Redo
```

- Aplicamos los cambios, reiniciamos los servicios de red y comprobamos el estado.
 - netplan apply
 - systemctl restart networking.service / systemctl status networking.service

```
root@usuario:/home/usuario# netplan apply
root@usuario:/home/usuario# systemctl restart networking.service
root@usuario:/home/usuario# systemctl status networking.service
● networking.service - Raise network interfaces
  Loaded: loaded (/lib/systemd/system/networking.service; enabled; vendor preset: enabled)
  Active: active (exited) since Tue 2020-04-28 19:02:01 CEST; 6s ago
    Docs: man:interfaces(5)
 Process: 3655 ExecStop=/sbin/ifdown -a --read-environment --exclude=lo (code=exited, status=0/SUCCESS)
 Process: 3774 ExecStart=/sbin/ifup -a --read-environment (code=exited, status=0/SUCCESS)
 Process: 3761 ExecStartPre=/bin/sh -c [ "$CONFIGURE_INTERFACES" != "no" ] && [ -n "$(ifquery --rea
 Main PID: 3774 (code=exited, status=0/SUCCESS)

abr 28 19:02:00 usuario systemd[1]: Starting Raise network interfaces...
abr 28 19:02:01 usuario systemd[1]: Started Raise network interfaces.
lines 1-11/11 (END)
```

- Hacemos ping para comprobar que funciona correctamente.

- ping 192.168.1.1 - Nuestra puerta de enlace
- ping google.com

```
root@usuario:/usr/local/pnp4nagios# ifconfig enp0s3 down
root@usuario:/usr/local/pnp4nagios# ifconfig enp0s3 up
root@usuario:/usr/local/pnp4nagios# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=13.0 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=8.06 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=8.29 ms
^C
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 8.068/9.800/13.036/2.291 ms
root@usuario:/usr/local/pnp4nagios# ping google.com
PING google.com (216.58.211.46) 56(84) bytes of data.
64 bytes from muc03s14-in-f46.1e100.net (216.58.211.46): icmp_seq=1 ttl=46 time=93.6 ms
64 bytes from muc03s14-in-f46.1e100.net (216.58.211.46): icmp_seq=2 ttl=46 time=90.0 ms
64 bytes from muc03s14-in-f46.1e100.net (216.58.211.46): icmp_seq=3 ttl=46 time=90.0 ms
64 bytes from muc03s14-in-f46.1e100.net (216.58.211.46): icmp_seq=4 ttl=46 time=83.0 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 83.020/89.215/93.682/3.867 ms
```

Paso 2. Crear usuario Nagios.

- En primer lugar, creamos una nueva cuenta de usuario para Nagios en su sistema y asignamos una contraseña.
 - sudo adduser nagios
- Ahora creamos un grupo para la configuración de Nagios "nagcmd" y agregamos el usuario de nagios a este grupo. Además, agregamos el usuario nagios en el grupo Apache.
 - sudo groupadd nagcmd
 - sudo usermod -a -G nagcmd nagios
 - sudo usermod -a -G nagcmd www-data

```
root@usuario:/home/usuario# adduser nagios
Adding user `nagios' ...
Adding new group `nagios' (1001) ...
Adding new user `nagios' (1001) with group `nagios' ...
Creating home directory `/home/nagios' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for nagios
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
root@usuario:/home/usuario# groupadd nagcmd
root@usuario:/home/usuario# usermod -a -G nagcmd nagios
root@usuario:/home/usuario# usermod -a -G nagcmd www-data
```

Paso 3. Instala el servicio Nagios Core.

Comenzaremos con la instalación central de Nagios.

- Descargamos el último servicio central de Nagios desde el sitio oficial.
 - cd / opt /
 - wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.5.tar.gz
 - tar xzf nagios-4.4.5.tar.gz

```
root@usuario:/home/usuario# cd /opt/
root@usuario:/opt# wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.5.tar.gz
--2020-03-25 15:47:24-- https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.5.tar.gz
Resolving assets.nagios.com (assets.nagios.com)... 72.14.181.71, 2600:3c00:f03c:91ff:fedf:b821
Connecting to assets.nagios.com (assets.nagios.com)|72.14.181.71|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11304463 (11M) [application/x-gzip]
Saving to: 'nagios-4.4.5.tar.gz'

nagios-4.4.5.tar.gz      100%[=====] 10,78M 2,90MB/s   in 3,7s

2020-03-25 15:47:28 (2,90 MB/s) - 'nagios-4.4.5.tar.gz' saved [11304463/11304463]

root@usuario:/opt# tar xzf nagios-4.4.5.tar.gz
```

- Ahora accedemos a la carpeta y usamos los siguientes comandos para finalizar la configuración e instalación:
 - `cd nagios-4.4.5`
 - `sudo ./configure --with-command-group=nagcmd`

```
config.status: creating t-tap/Makefile
config.status: creating include/config.h
config.status: creating lib/snprintf.h
config.status: creating lib/iobroker.h

Creating sample config files in sample-config/ ...

*** Configuration summary for nagios 4.4.5 2019-08-20 ***:

General Options:
-----
      Nagios executable: nagios
      Nagios user/group: nagios,nagios
      Command user/group: nagios,nagcmd
      Event Broker: yes
      Install ${prefix}: /usr/local/nagios
      Install ${includedir}: /usr/local/nagios/include/nagios
      Lock file: /run/nagios.lock
      Check result directory: /usr/local/nagios/var/spool/checkresults
      Init directory: /lib/systemd/system
      Apache conf.d directory: /etc/apache2/sites-available
      Mail program: /bin/mail
      Host OS: linux-gnu
      IOBroker Method: epoll

Web Interface Options:
-----
      HTML URL: http://localhost/nagios/
      CGI URL: http://localhost/nagios/cgi-bin/
Traceroute (used by WAP):
```

Review the options above for accuracy. If they look okay,
type 'make all' to compile the main program and CGIs.

```
root@usuario:/opt/nagios-4.4.5# _
```

- sudo make all
- sudo make install

```
make[1]: Leaving directory '/opt/nagios-4.4.5'
make install-basic
make[1]: Entering directory '/opt/nagios-4.4.5'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/libexec
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/var
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/var/archives
/usr/bin/install -c -m 775 -o nagios -g nagcmd -d /usr/local/nagios/var/spool/checkresults
chmod g+s /usr/local/nagios/var/spool/checkresults

*** Main program, CGIs and HTML files installed ***

You can continue with installing Nagios as follows (type 'make'
without any arguments for a list of all possible options):

make install-init
  - This installs the init script in /lib/systemd/system

make install-commandmode
  - This installs and configures permissions on the
    directory for holding the external command file

make install-config
  - This installs sample config files in /usr/local/nagios/etc

make[1]: Leaving directory '/opt/nagios-4.4.5'
```

- sudo make install-init
- sudo make install-daemoninit

```
root@usuario:/opt/nagios-4.4.5# make install-init
/usr/bin/install -c -m 755 -d -o root -g root /lib/systemd/system
/usr/bin/install -c -m 755 -o root -g root startup/default-service /lib/systemd/system/nagios.service
root@usuario:/opt/nagios-4.4.5# make install-daemoninit
/usr/bin/install -c -m 755 -d -o root -g root /lib/systemd/system
/usr/bin/install -c -m 755 -o root -g root startup/default-service /lib/systemd/system/nagios.service
Created symlink /etc/systemd/system/multi-user.target.wants/nagios.service → /lib/systemd/system/nagios.service.

*** Init script installed ***
```

- sudo make install-config

```
root@usuario:/opt/nagios-4.4.5# make install-config
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc/objects
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/nagios.cfg /usr/local/nagios/etc/nagios.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/cgi.cfg /usr/local/nagios/etc/cgi.cfg
/usr/bin/install -c -b -m 660 -o nagios -g nagios sample-config/resource.cfg /usr/local/nagios/etc/resource.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/templates.cfg /usr/local/nagios/etc/objects/templates.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/commands.cfg /usr/local/nagios/etc/objects/commands.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/contacts.cfg /usr/local/nagios/etc/objects/contacts.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/timeperiods.cfg /usr/local/nagios/etc/objects/timeperiods.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/localhost.cfg /usr/local/nagios/etc/objects/localhost.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/windows.cfg /usr/local/nagios/etc/objects/windows.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/printer.cfg /usr/local/nagios/etc/objects/printer.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/switch.cfg /usr/local/nagios/etc/objects/switch.cfg

*** Config files installed ***

Remember, these are *SAMPLE* config files. You'll need to read
the documentation for more information on how to actually define
services, hosts, etc. to fit your particular needs.
```

- sudo make install-commandmode
- sudo make install-exfoliation

```
root@usuario:/opt/nagios-4.4.5# make install-commandmode
/usr/bin/install -c -m 775 -o nagios -g nagcmd -d /usr/local/nagios/var/rw
chmod g+s /usr/local/nagios/var/rw

*** External command directory configured ***

root@usuario:/opt/nagios-4.4.5# make install-exfoliation

*** Exfoliation theme installed ***
NOTE: Use 'make install-classicui' to revert to classic Nagios theme
```

- Ahora copiamos las secuencias de comandos de los controladores de eventos en el directorio libexec. Estos archivos binarios proporcionan múltiples desencadenantes de eventos para la interfaz web Nagios.
 - cp -R contrib/eventhandlers/ /usr/local/nagios/libexec/
 - chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers

```
root@usuario:/opt/nagios-4.4.5# cp -R contrib/eventhandlers/ /usr/local/nagios/libexec/
root@usuario:/opt/nagios-4.4.5# chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers
root@usuario:/opt/nagios-4.4.5#
```

Paso 4. Configura Apache con autenticación.

- Creamos un archivo de configuración de Apache para su servidor Nagios como se muestra a continuación:
 - sudo nano /etc/apache2/conf-available/nagios.conf

```
<Directory "/usr/local/nagios/sbin">
  Options ExecCGI
  AllowOverride None
  Order allow,deny
  Allow from all
  AuthName "Restricted Area"
  AuthType Basic
  AuthUserFile /usr/local/nagios/etc/htpasswd.users
  Require valid-user
```

```
</Directory>
```

```
Alias /nagios "/usr/local/nagios/share"
```

```
<Directory "/usr/local/nagios/share">
```

```
    Options None
```

```
    AllowOverride None
```

```
    Order allow,deny
```

```
    Allow from all
```

```
    AuthName "Restricted Area"
```

```
    AuthType Basic
```

```
    AuthUserFile /usr/local/nagios/etc/htpasswd.users
```

```
    Require valid-user
```

```
</Directory>
```

```
GNU nano 2.9.3                               /etc/apache2/conf-available/nagios.conf

ScriptAlias /nagios/cgi-bin "/usr/local/nagios/sbin"

<Directory "/usr/local/nagios/sbin">
    Options ExecCGI
    AllowOverride None
    Order allow,deny
    Allow from all
    AuthName "Restricted Area"
    AuthType Basic
    AuthUserFile /usr/local/nagios/etc/htpasswd.users
    Require valid-user
</Directory>

Alias /nagios "/usr/local/nagios/share"

<Directory "/usr/local/nagios/share">_
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
    AuthName "Restricted Area"
    AuthType Basic
    AuthUserFile /usr/local/nagios/etc/htpasswd.users
    Require valid-user
</Directory>

[ Wrote 25 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  M-U Undo
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^L Go To Line M-E Redo
```

- Necesitamos configurar la autenticación apache para el usuario nagiosadmin . Hasta que una razón más específica use este nombre de usuario como "nagiosadmin", de lo contrario, necesitaría más cambios en la configuración.
 - htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

```
root@usuario:/opt/nagios-4.4.5# htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
```

- Ahora habilitamos la configuración de Apache y reiniciamos el servicio de Apache para que la nueva configuración surta efecto.
 - sudo a2enconf nagios
 - sudo a2enmod cgi rewrite

```
root@usuario:/opt/nagios-4.4.5# a2enconf nagios
Enabling conf nagios.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@usuario:/opt/nagios-4.4.5# a2enmod cgi rewrite
Enabling module cgi.
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
```

- sudo service apache2 restart

```
root@usuario:/opt/nagios-4.4.5# service apache2 restart
root@usuario:/opt/nagios-4.4.5# systemctl status apache2.service
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
            └─apache2-systemd.conf
    Active: active (running) since Wed 2020-03-25 16:15:38 UTC; 3s ago
      Process: 22392 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
      Process: 22397 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 22413 (apache2)
       Tasks: 6 (limit: 2318)
      CGroup: /system.slice/apache2.service
              ├─22413 /usr/sbin/apache2 -k start
              ├─22418 /usr/sbin/apache2 -k start
              ├─22419 /usr/sbin/apache2 -k start
              ├─22420 /usr/sbin/apache2 -k start
              ├─22421 /usr/sbin/apache2 -k start
              └─22422 /usr/sbin/apache2 -k start

mar 25 16:15:38 usuario systemd[1]: Stopped The Apache HTTP Server.
mar 25 16:15:38 usuario systemd[1]: Starting The Apache HTTP Server...
mar 25 16:15:38 usuario apachectl[22397]: AH00558: apache2: Could not reliably determine the server's
mar 25 16:15:38 usuario systemd[1]: Started The Apache HTTP Server.
lines 1-21/21 (END)
```

Paso 5. Instalación de complementos de Nagios.

- Después de instalar y configurar el servicio principal de Nagios, descargamos la última fuente de nagios-plugins y la instalamos utilizando los siguientes comandos:

- cd /opt
- wget http://www.nagios-plugins.org/download/nagios-plugins-2.2.1.tar.gz
- tar xzf nagios-plugins-2.2.1.tar.gz
- cd nagios-plugins-2.2.1

```
root@usuario:/opt/nagios-4.4.5# cd /opt/
root@usuario:/opt# wget http://www.nagios-plugins.org/download/nagios-plugins-2.2.1.tar.gz
--2020-03-25 16:17:28--  http://www.nagios-plugins.org/download/nagios-plugins-2.2.1.tar.gz
Resolving www.nagios-plugins.org (www.nagios-plugins.org)... 72.14.186.43
Connecting to www.nagios-plugins.org (www.nagios-plugins.org)|72.14.186.43|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://nagios-plugins.org/download/nagios-plugins-2.2.1.tar.gz [following]
--2020-03-25 16:17:29--  http://nagios-plugins.org/download/nagios-plugins-2.2.1.tar.gz
Resolving nagios-plugins.org (nagios-plugins.org)... 72.14.186.43
Reusing existing connection to www.nagios-plugins.org:80.
HTTP request sent, awaiting response... 200 OK
Length: 2728818 (2,6M) [application/x-gzip]
Saving to: 'nagios-plugins-2.2.1.tar.gz'

nagios-plugins-2.2.1.tar 100%[=====] 2,60M 2,13MB/s   in 1,2s

2020-03-25 16:17:30 (2,13 MB/s) - 'nagios-plugins-2.2.1.tar.gz' saved [2728818/2728818]

root@usuario:/opt# tar xzf nagios-plugins-2.2.1.tar.gz
root@usuario:/opt# cd nagios-plugins-2.2.1
root@usuario:/opt/nagios-plugins-2.2.1#
```

- Ahora compilamos e instalamos los complementos de Nagios:

- sudo ./configure --with-nagios-user=nagios --with-nagios-group=nagios
--with-openssl
- sudo make
- sudo make install

Paso 6. Verificar la configuración.

- Usamos los comandos de Nagios para verificar el archivo de instalación y configuración de Nagios.

- /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

```
Last Modified: 2019-08-20
License: GPL

Website: https://www.nagios.org
Reading configuration data...
    Read main config file okay...
    Read object config files okay...

Running pre-flight check on configuration data...

Checking objects...
    Checked 8 services.
    Checked 1 hosts.
    Checked 1 host groups.
    Checked 0 service groups.
    Checked 1 contacts.
    Checked 1 contact groups.
    Checked 24 commands.
    Checked 5 time periods.
    Checked 0 host escalations.
    Checked 0 service escalations.
Checking for circular paths...
    Checked 1 hosts
    Checked 0 service dependencies
    Checked 0 host dependencies
    Checked 5 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors: 0

Things look okay - No serious problems were detected during the pre-flight check
root@usuario:/opt/nagios-plugins-2.2.1# service nagios start
root@usuario:/opt/nagios-plugins-2.2.1# systemctl enable nagios
root@usuario:/opt/nagios-plugins-2.2.1#
```

- Despu s de verificar con éxito, iniciamos el servicio central de Nagios:
 - service nagios start
 - service nagios status

```

root@usuario:/opt/nagios-plugins-2.2.1# service nagios start
root@usuario:/opt/nagios-plugins-2.2.1# service nagios status
● nagios.service - Nagios Core 4.4.5
  Loaded: loaded (/lib/systemd/system/nagios.service; enabled; vendor preset: enabled)
  Active: active (running) since Mon 2020-04-27 19:19:06 CEST; 24min ago
    Docs: https://www.nagios.org/documentation
 Main PID: 3179 (nagios)
   Tasks: 8 (limit: 2318)
  CGroup: /system.slice/nagios.service
          ├─3179 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
          ├─3180 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
          ├─3181 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
          ├─3182 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
          ├─3183 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
          └─3184 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

abr 27 19:43:29 usuario nagios[3179]: wproc: host=clientew-PC; service=PING; contact=nagiosadmin
abr 27 19:43:29 usuario nagios[3179]: wproc: early_timeout=0; exited_ok=1; wait_status=32512; erro
abr 27 19:43:29 usuario nagios[3179]: wproc: stderr line 01: /bin/sh: 1: /bin/mail: not found
abr 27 19:43:29 usuario nagios[3179]: wproc: stderr line 02: /usr/bin/printf: write error: Broken
abr 27 19:43:31 usuario nagios[3179]: SERVICE NOTIFICATION: nagiosadmin;winserver;CPU Load;CRITICAL;
abr 27 19:43:31 usuario nagios[3179]: wproc: NOTIFY job 56 from worker Core Worker 3180 is a non-che
abr 27 19:43:31 usuario nagios[3179]: wproc: host=winserver; service=CPU Load; contact=nagiosadmin
abr 27 19:43:31 usuario nagios[3179]: wproc: early_timeout=0; exited_ok=1; wait_status=32512; erro
abr 27 19:43:31 usuario nagios[3179]: wproc: stderr line 01: /bin/sh: 1: /bin/mail: not found
abr 27 19:43:31 usuario nagios[3179]: wproc: stderr line 02: /usr/bin/printf: write error: Broken
lines 1-26/26 (END)

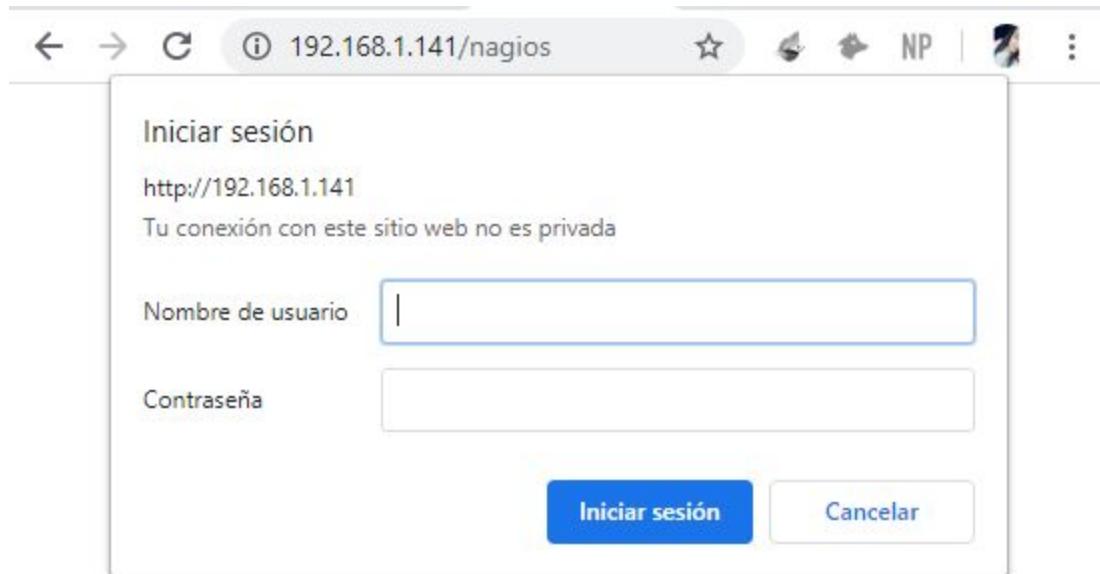
```

- También configuramos Nagios para que se inicie automáticamente en el arranque del sistema:
 - sudo systemctl enable nagios

Paso 7. Acceder a la interfaz web de Nagios.

- Accedemos a nuestra configuración de nagios accediendo al servidor de nagios usando el nombre de host o la dirección IP seguido de / nagios.
 - http://IP/nagios/

- Esto solicitará la autenticación de Apache. Usamos nagiosadmin como nombre de usuario y la contraseña creada en el paso 4 (en mi caso es usuario).



- Despues de iniciar sesión correctamente, veremos la interfaz de Nagios como se muestra a continuación. Aquí podemos usar el botón de la barra lateral para navegar para ver hosts, servicios, alertas, etc.

The screenshot shows the Nagios Core 4.4.5 web interface. The top right features the Nagios Core logo with a green checkmark and the text "Daemon running with PID 9862". Below the logo, it says "Nagios® Core™ Version 4.4.5" and "August 20, 2019 Check for updates". To the left is a sidebar with links for General, Current Status, Reports, and System. The main content area includes sections for "Get Started" (with bullet points about monitoring infrastructure, changing look, adding addons, support, and training) and "Quick Links" (with links to Nagios Library, Labs, Exchange, Support, and the company website). There are also links to download Nagios XI, Log Server, and Network Analyzer.

- Finalmente, hemos instalado y configurado con éxito el servicio principal de Nagios Monitoring Server en nuestro sistema.

The screenshot shows the Nagios Core 4.4.5 web interface displaying the "Service Status Details For All Hosts" table. The table lists 8 matching services across various hosts. The columns include Host, Service, Status, Last Check, Duration, Attempt, and Status Information. The table shows entries for localhost services like Current Load, Current Users, HTTP, PING, Root Partition, SSH, Swap Usage, and Total Processes, all currently in an OK state.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	03-25-2020 18:03:47	0d 0h 42m 58s	1/4	OK - load average: 0.06, 0.02, 0.00
localhost	Current Users	OK	03-25-2020 18:04:25	0d 0h 42m 20s	1/4	USERS OK - 1 users currently logged in
localhost	HTTP	OK	03-25-2020 18:05:02	0d 0h 41m 43s	1/4	HTTP OK - HTTP/1.1 200 OK - 11192 bytes in 0.001 second response time
localhost	PING	OK	03-25-2020 18:05:41	0d 0h 41m 5s	1/4	PING OK - Packet loss = 0%, RTA = 0.11 ms
localhost	Root Partition	OK	03-25-2020 18:06:17	0d 0h 40m 28s	1/4	DISK OK - free space: / 43108 MB (90.63% inode=97%).
localhost	SSH	OK	03-25-2020 18:01:55	0d 0h 39m 50s	1/4	SSH OK - OpenSSH_7.6p1 Ubuntu-4ubuntu0.3 (protocol 2.0)
localhost	Swap Usage	OK	03-25-2020 18:02:32	0d 0h 39m 13s	1/4	SWAP OK - 100% free (2047 MB out of 2047 MB)
localhost	Total Processes	OK	03-25-2020 18:03:10	0d 0h 38m 35s	1/4	PROCS OK: 38 processes with STATE = RSZDT

Capítulo 3

Monitorización de cliente Linux.

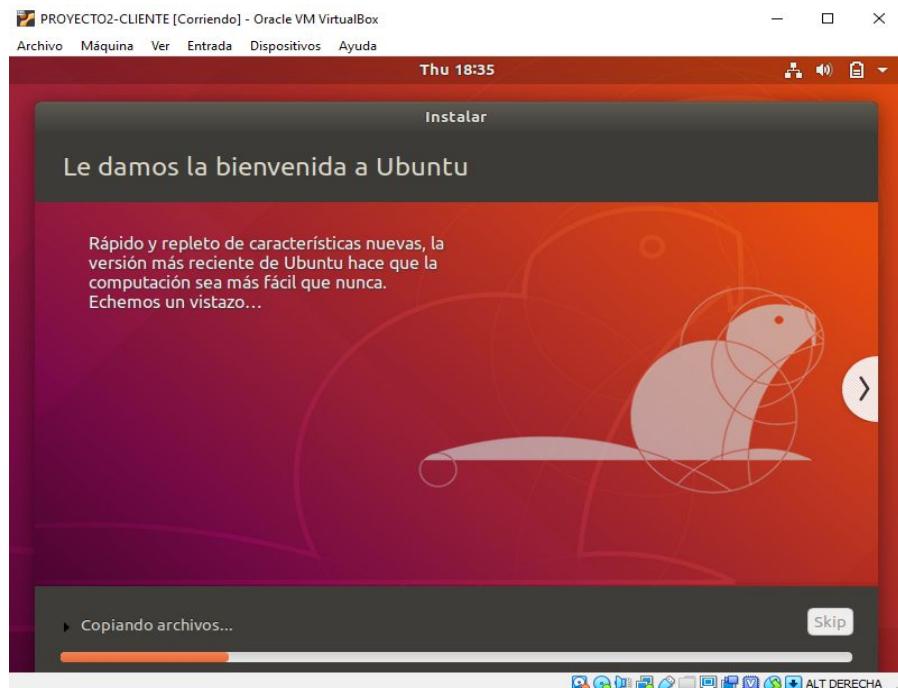
Se debe instalar NRPE en todos los sistemas remotos de Linux para monitorear con Nagios.

NRPE se conoce como Nagios Remote Plugin Executor. En esta configuración, el daemon NRPE se instala en el sistema remoto al que los servicios necesitan monitorear a través del servidor Nagios. NRPE se ejecuta como un demonio en sistemas remotos y espera las solicitudes de Nagios.

Cuando el servidor Nagios necesita verificar el estado de cualquier recurso o aplicación a ese host remoto, envía una señal de comando, cuya definición de comando se almacena en el servicio NRPE. NRPE toma la solicitud del servidor Nagios y ejecuta el comando en el sistema local y envía el resultado a Nagios.

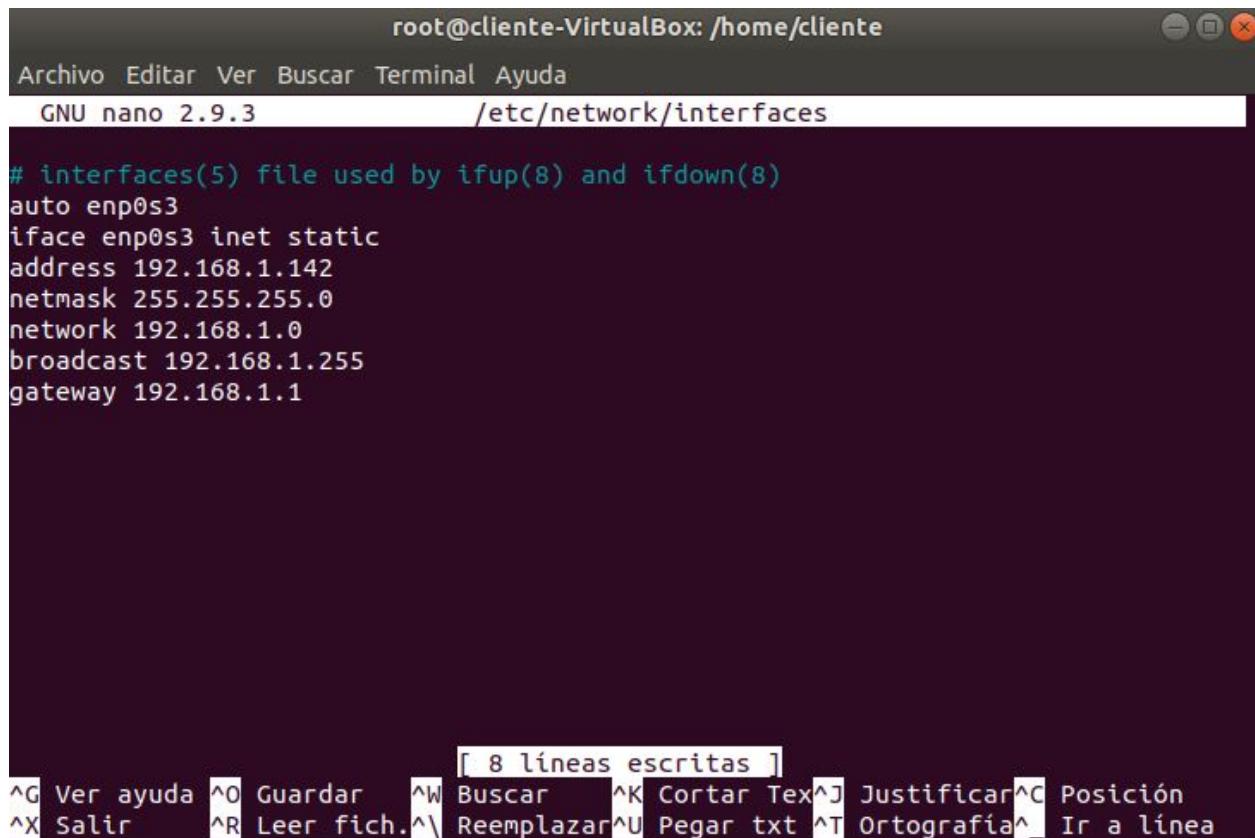
Paso 1. Configurar NRPE en el host de Linux.

A continuación vamos a instalar y configurar NRPE en la máquina cliente y verificar la conectividad con el servidor Nagios.



- En primer lugar, debemos configurar la IP como fija.

- nano /etc/network/interfaces



```
root@cliente-VirtualBox: /home/cliente
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3           /etc/network/interfaces

# interfaces(5) file used by ifup(8) and ifdown(8)
auto enp0s3
iface enp0s3 inet static
address 192.168.1.142
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1

[ 8 líneas escritas ]
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex^J Justificar^C Posición
^X Salir      ^R Leer fich.^\\ Reemplazar^U Pegar txt ^T Ortografía^L Ir a linea
```

- Hacemos ping para comprobar si funciona correctamente.

- ping 192.168.1.1 - Nuestra puerta de enlace.
 - ping google.com

```

root@cliente-VirtualBox:/home/cliente# ifconfig enp0s3 down
root@cliente-VirtualBox:/home/cliente# ifconfig enp0s3 up
root@cliente-VirtualBox:/home/cliente# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=7.77 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=8.28 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=8.32 ms
^C
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 7.778/8.126/8.321/0.268 ms
root@cliente-VirtualBox:/home/cliente# ping google.com
PING google.com (216.58.211.46) 56(84) bytes of data.
64 bytes from mad08s05-in-f14.1e100.net (216.58.211.46): icmp_seq=1 ttl=46 time=
92.3 ms
64 bytes from mad08s05-in-f14.1e100.net (216.58.211.46): icmp_seq=2 ttl=46 time=
90.5 ms
64 bytes from mad08s05-in-f14.1e100.net (216.58.211.46): icmp_seq=3 ttl=46 time=
89.9 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 89.967/90.952/92.351/1.074 ms

```

- Necesitamos instalar el servicio nrpe en un sistema Linux remoto, que debemos monitorear a través del servidor Nagios.
 - sudo apt-get install nagios-nrpe-server nagios-plugins

```

root@cliente-VirtualBox:/home/cliente# apt-get install nagios-nrpe-server nagios-plugins
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libdbi1 libmysqlclient20 libnet-snmp-perl libpq5 libpython-stdlib libtirpc1
  monitoring-plugins monitoring-plugins-basic monitoring-plugins-common
  monitoring-plugins-standard mysql-common python python-crypto python-ldb
  python-minimal python-samba python-tdb python2.7 python2.7-minimal rpcbind
  samba-common samba-common-bin smbclient snmp
Paquetes sugeridos:
  libcrypt-des-perl icinga | icinga2 nagios-plugins-contrib fping postfix
  | sendmail-bin | exim4-daemon-heavy | exim4-daemon-light qstat xinetd
  | inetd python-doc python-tk python-crypto-doc python-gpgme python2.7-doc
  binfmt-support heimdal-clients cifs-utils
Se instalarán los siguientes paquetes NUEVOS:
  libdbi1 libmysqlclient20 libnet-snmp-perl libpq5 libpython-stdlib libtirpc1
  monitoring-plugins monitoring-plugins-basic monitoring-plugins-common
  monitoring-plugins-standard mysql-common nagios-nrpe-server nagios-plugins
  python python-crypto python-ldb python-minimal python-samba python-tdb
  python2.7 python2.7-minimal rpcbind samba-common samba-common-bin smbclient
  snmp
0 actualizados, 26 nuevos se instalarán, 0 para eliminar y 103 no actualizados.
Se necesita descargar 6.886 kB de archivos.
Se utilizarán 34,2 MB de espacio de disco adicional después de esta operación.
;Desea continuar? [S/n] ■

```

- Despues de instalar el servicio NRPE, editamos el archivo de configuración nrpe /etc/nagios/nrpe.cfg en el editor que queramos y agregamos nuestra ip de servicio nagios en los hosts permitidos.
 - nano /etc/nagios/nrpe.cfg
 - allowed_hosts = 127.0.0.1, 192.168.1.141
 - Donde 192.168.1.141 es la dirección IP de mi servidor Nagios.

```

root@cliente-VirtualBox: /home/cliente
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3           /etc/nagios/nrpe.cfg           Modificado

# You can either supply a group name or a GID.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd
nrpe_group=nagios

#
# ALLOWED HOST ADDRESSES
# This is an optional comma-delimited list of IP address or hostnames
# that are allowed to talk to the NRPE daemon. Network addresses with a bit mask
# (i.e. 192.168.1.0/24) are also supported. Hostname wildcards are not currently
# supported.
#
# Note: The daemon only does rudimentary checking of the client's IP
# address. I would highly recommend adding entries in your /etc/hosts.allow
# file to allow only the specified host to connect to the port
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd
allowed_hosts=127.0.0.1, 192.168.1.141

^G Ver ayuda   ^O Guardar   ^W Buscar   ^K Cortar Texto ^J Justificar
^X Salir       ^R Leer fich.  ^\ Reemplazar  ^U Pegar txt  ^T Ortografía

```

- Despues de realizar los cambios anteriores en el archivo de configuración, reiniciamos el servicio NRPE.
 - `sudo /etc/init.d/nagios-nrpe-server restart`

```
root@cliente-VirtualBox:/home/cliente# /etc/init.d/nagios-nrpe-server restart
[....] Restarting nagios-nrpe-server (via systemctl): nagios-nrpe-server.service
[.ok]
```

- Ahora ejecutamos el siguiente comando desde el servidor Nagios para asegurarse de que su nagios pueda conectar el cliente nrpe en un sistema remoto de Linux, aunque este paso no es estrictamente necesario.
 - `/usr/local/nagios/libexec/check_nrpe -H 192.168.1.142`
 - Aquí 192.168.1.142 es nuestra ip remota del sistema Linux.
- Nos debería aparecer algo así.
 - NRPE v2.15

Paso 2. Agregar host de Linux en Nagios.

Veremos cómo agregar un host en su servidor Nagios desde la línea de comandos.

- Descomentamos la siguiente línea del archivo nagios.cfg:
 - `nano /usr/local/nagios/etc/nagios.cfg`

```

root@usuario: /usr/local/nagios/etc
GNU nano 2.9.3                                     nagios.cfg                                         Modified

# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

# Definitions for monitoring a Windows machine
#cfg_file=/usr/local/nagios/etc/objects/windows.cfg

# Definitions for monitoring a router/switch
#cfg_file=/usr/local/nagios/etc/objects/swtch.cfg

# Definitions for monitoring a network printer
#cfg_file=/usr/local/nagios/etc/objects/printer.cfg

# You can also tell Nagios to process all config files (with a .cfg
# extension) in a particular directory by using the cfg_dir
# directive as shown below:

cfg_dir=/usr/local/nagios/etc/servers
#cfg_dir=/usr/local/nagios/etc/printers
#cfg_dir=/usr/local/nagios/etc/switches
#cfg_dir=/usr/local/nagios/etc/routers

# OBJECT CACHE FILE
# This option determines where object definitions are cached when
# Nagios starts/restarts. The CGIs read object definitions from
# this cache file (rather than looking at the object config files
# directly) in order to prevent inconsistencies that can occur

^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     ^L Go To Line

```

- Creamos la carpeta servers y creamos el archivo de configuración /usr/local/nagios/etc/servers/(nombre).cfg.

```

root@usuario:/usr/local/nagios/etc# mkdir servers
root@usuario:/usr/local/nagios/etc# cd servers/
root@usuario:/usr/local/nagios/etc/servers# nano Linux142.cfg

```

- Utilizamos los valores a continuación:
 - Mi IP de host es 192.168.1.142.

- También necesitamos definir un servicio con el host. Por lo tanto, agregamos un servicio de verificación de ping, que verificará continuamente que el host esté activo o no.
- nano /usr/local/nagios/etc/servers/Linux142.cfg

```
#####
```

```
# Linux Host 001 configuration file
```

```
#####
```

```
define host {
```

```
    use          linux-server  
    host_name   cliente-VirtualBox  
    alias       Linux Host 001  
    address     192.168.1.142  
    register    1
```

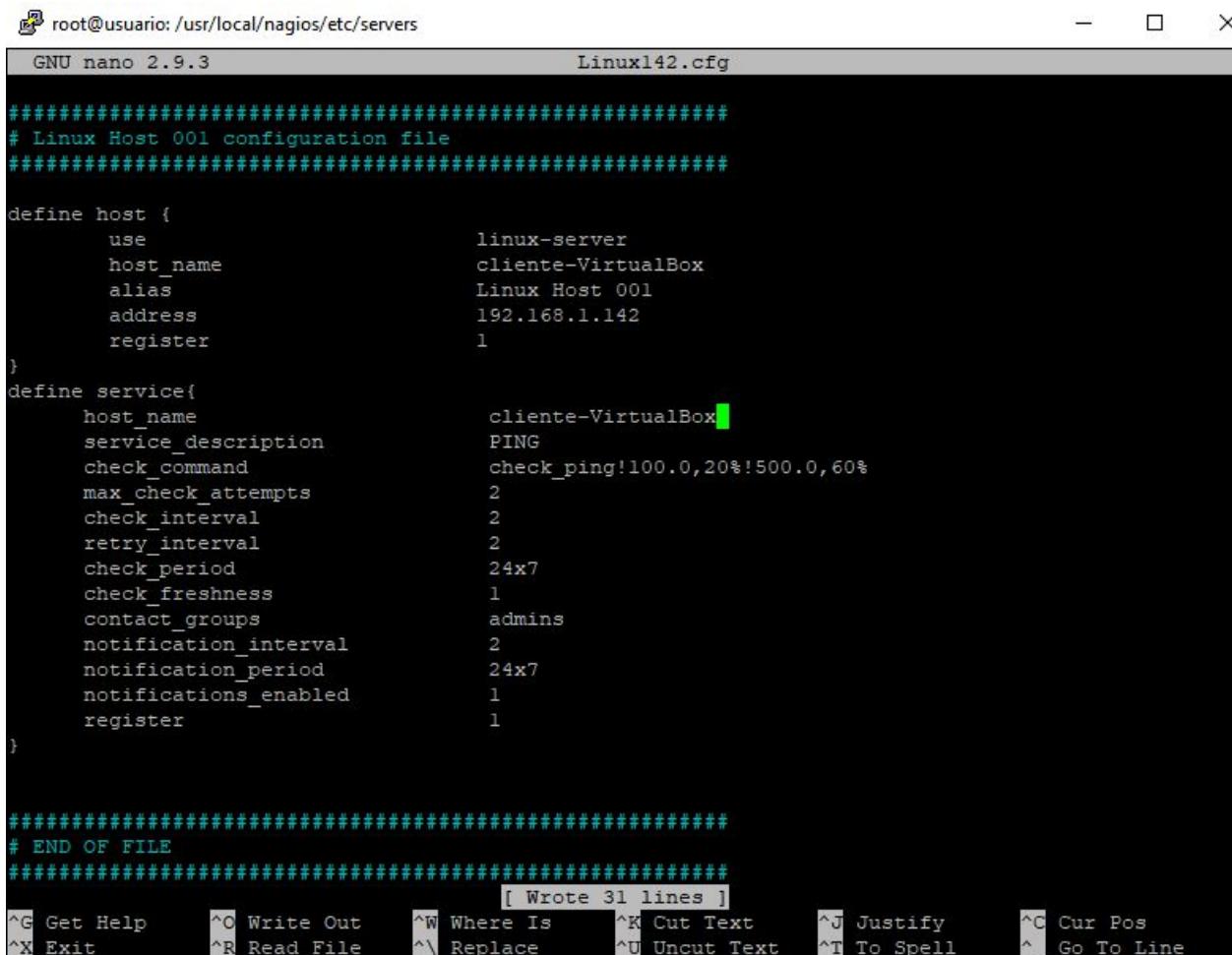
```
}
```

```
define service{
```

```
    host_name   Linux_Host_001  
    service_description PING  
    check_command  check_ping!100.0,20%!500.0,60%  
    max_check_attempts 2  
    check_interval 2
```

```
retry_interval          2
check_period            24x7
check_freshness         1
contact_groups          admins
notification_interval   2
notification_period     24x7
notifications_enabled   1
register                1
}
```

```
#####
# END OF FILE
#####
```



```

root@usuario: /usr/local/nagios/etc/servers
GNU nano 2.9.3                               Linux142.cfg

#####
# Linux Host 001 configuration file
#####

define host {
    use                  linux-server
    host_name            cliente-VirtualBox
    alias                Linux Host 001
    address              192.168.1.142
    register             1
}
define service{
    host_name            cliente-VirtualBox
    service_description   PING
    check_command         check_ping!100.0,20%!500.0,60%
    max_check_attempts    2
    check_interval        2
    retry_interval        2
    check_period          24x7
    check_freshness       1
    contact_groups        admins
    notification_interval 2
    notification_period   24x7
    notifications_enabled 1
    register              1
}

#####
# END OF FILE
#####

[ Wrote 31 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

```

- Ahora reiniciamos el servicio nagios:

- service nagios restart

Paso 3. Verificar el host en la interfaz web de Nagios.

Abrimos nuestra interfaz web de Nagios y comprobamos si hay nuevos hosts de Linux agregados en el servicio central de Nagios. En mi caso, se ve a continuación.

No es seguro | 192.168.1.141/nagios/

Nagios®

General

- Home
- Documentation

Current Status

- Tactical Overview
- Map (Legacy)
- Hosts
- Services
- Host Groups
 - Summary
 - Grid
- Service Groups
 - Summary
 - Grid
- Problems
 - Services (Unhandled)
 - Hosts (Unhandled)
 - Network Outages

Quick Search:

Reports

- Availability
- Trends (Legacy)
- Alerts
 - History
 - Summary
 - Histogram (Legacy)
- Notifications
- Event Log

System

- Comments
- Downtime
- Process Info

Host Status Details For All Host Groups

Limit Results: 100 ▾

Host	Status	Last Check	Duration	Status Information
cliente-VirtualBox	UP	03-27-2020 21:16:15	0d 0h 1m 47s+	PING OK - Packet loss = 0%, RTA = 0.85 ms
localhost	UP	03-27-2020 21:15:06	1d 3h 38m 41s	PING OK - Packet loss = 0%, RTA = 0.06 ms

Results 1 - 2 of 2 Matching Hosts

Nagios®

General

- Home
- Documentation

Current Status

- Tactical Overview
- Map (Legacy)
- Hosts
- Services
- Host Groups
 - Summary
 - Grid
- Service Groups
 - Summary
 - Grid
- Problems
 - Services (Unhandled)
 - Hosts (Unhandled)
 - Network Outages

Quick Search:

Reports

- Availability
- Trends (Legacy)
- Alerts
 - History
 - Summary
 - Histogram (Legacy)
- Notifications
- Event Log

System

- Comments
- Downtime
- Process Info

Host Information

Last Updated: Fri Mar 27 21:18:49 CET 2020
 Updated every 90 seconds
 Nagios® Core™ 4.4.5 - www.nagios.org
 Logged in as nagiosadmin

Host
Linux Host 001
 (cliente-VirtualBox)

Member of
No hostgroups

192.168.1.142

Host State Information

Host Status:	UP (for 0d 0h 2m 34s+)
Status Information:	PING OK - Packet loss = 0%, RTA = 0.85 ms
Performance Data:	rta=0.847000ms;3000.000000;5000.000000;0.000000 pl=0%;80;100;0
Current Attempt:	1/10 (HARD state)
Last Check Time:	03-27-2020 21:16:15
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 4.000 seconds
Next Scheduled Active Check:	03-27-2020 21:21:15
Last State Change:	N/A
Last Notification:	N/A (notification 0)
Is This Host Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	03-27-2020 21:18:44 (0d 0h 0m 5s ago)

Host Commands

- Locate host on map
- Disable active checks of this host
- Re-schedule the next check of this host
- Submit passive check result for this host
- Stop accepting passive checks for this host
- Stop obsessing over this host
- Disable notifications for this host
- Send custom host notification
- Schedule downtime for this host
- Schedule downtime for all services on this host
- Disable notifications for all services on this host
- Enable notifications for all services on this host
- Schedule a check of all services on this host
- Disable checks of all services on this host
- Enable checks of all services on this host
- Disable event handler for this host
- Disable flap detection for this host
- Clear flapping state for this host

Host Comments

Add a new comment

Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
This host has no comments associated with it							

Capítulo 4

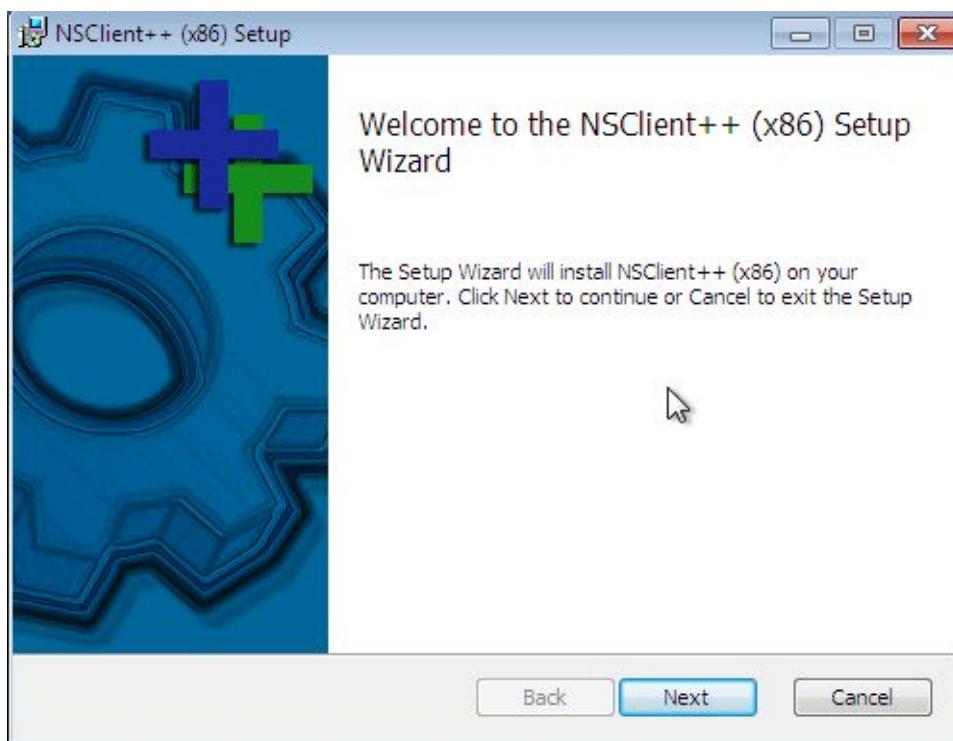
Monitorización de cliente Windows.

Para el cliente de Windows, es necesario instalar el servicio NSClient++.

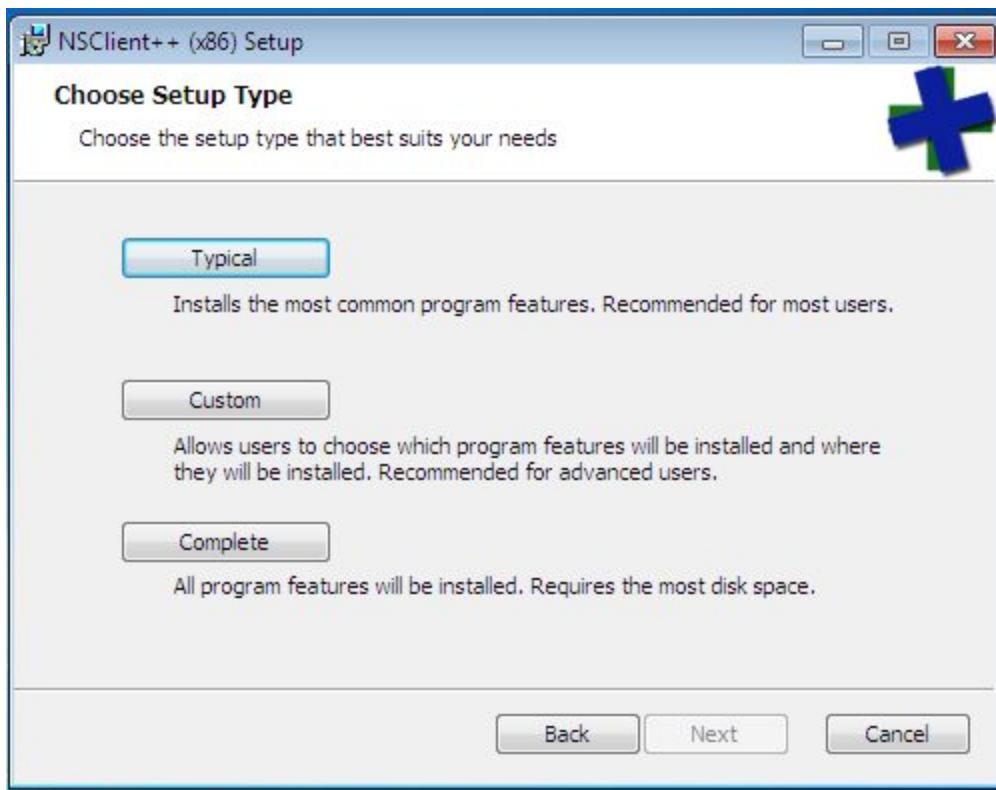
Similar al servicio NRPE en Linux, NSClient++ es el servicio que los hosts de Windows pueden monitorear a través de check_nrpe desde el servidor Nagios.

Paso 1. Instalar NSClient++.

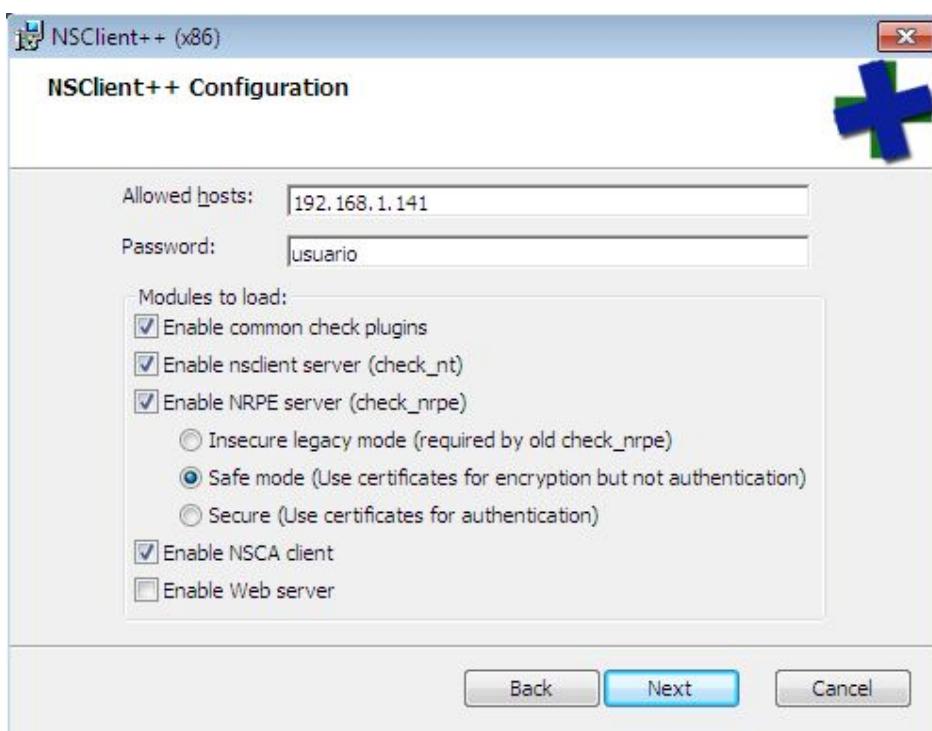
- Descargamos la versión 0.4.1 de NSClient desde su sitio oficial y comenzamos con su instalación de la siguiente manera:
 - El software se llamará NSCP-xxxxxx.msi .
 - Durante el proceso de instalación, deberá ingresar al servidor Nagios para permitir que el servidor conecte al cliente a través de NRPE.
- Comenzamos con la instalación.



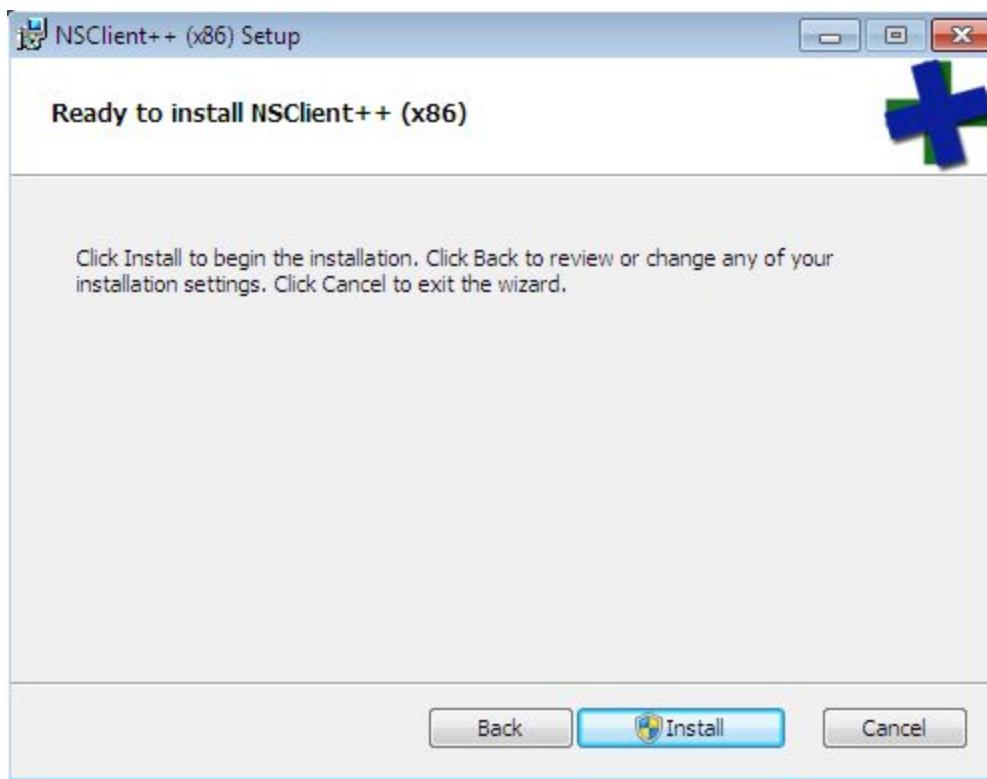
- Hacemos clic en tipo de configuración Completa.



- Ingresamos la IP del servidor Nagios en Hosts permitidos y la contraseña.



- Hacemos clic en el botón Instalar.



- Finalizamos la instalación.

Paso 2. Agregar host en el servidor Nagios.

- Creamos un archivo de configuración /usr/local/nagios/etc/servers/(nombre).cfg con los siguientes valores:
 - Mi Windows hosts ip es 192.168.1.137.
 - También necesitamos definir un servicio con el host. Entonces, agregamos un servicio de verificación de ping, que verificará continuamente que el host esté activo.

```
#####
# Windows Host 001 configuration file
#####

define host {
    use           windows-server
    host_name     Windows_Host_001
    alias         Windows Host 001
    address       192.168.1.10
    register      1
}

define service{
    host_name     Windows_Host_001
    service_description PING
    check_command   check_ping!100.0,20%!500.0,60%
    max_check_attempts 2
    check_interval  2
    retry_interval  2
    check_period    24x7
    check_freshness 1
    contact_groups admins
}
```

```

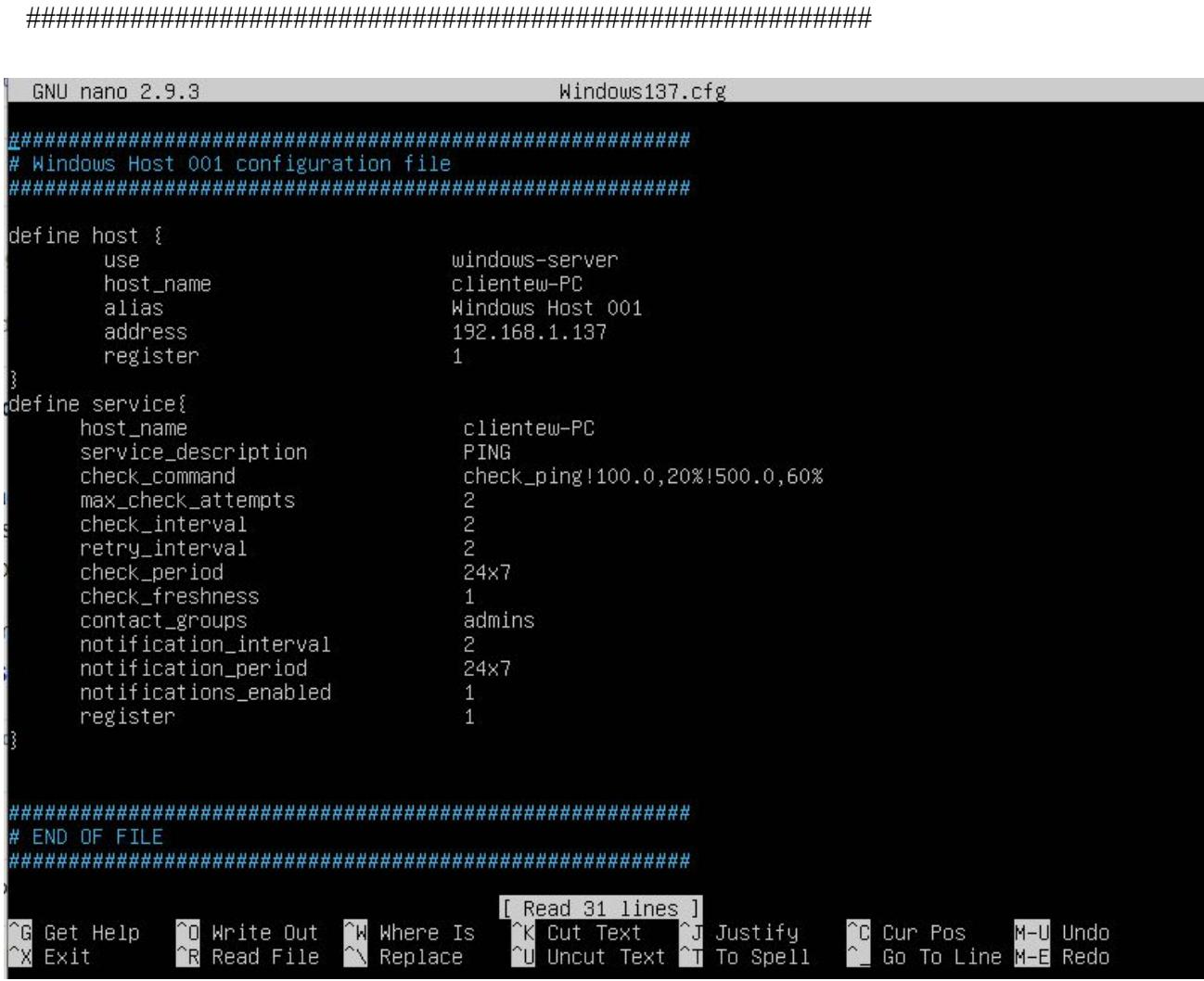
notification_interval      2
notification_period        24x7
notifications_enabled      1
register                  1

}

```

```
#####
# END OF FILE
#####

```



```
GNU nano 2.9.3          Windows137.cfg

#####
# Windows Host 001 configuration file
#####

define host {
    use                  windows-server
    host_name            clientew-PC
    alias                Windows Host 001
    address              192.168.1.137
    register             1
}
define service{
    host_name            clientew-PC
    service_description   PING
    check_command         check_ping!100.0,20%!500.0,60%
    max_check_attempts    2
    check_interval        2
    retry_interval        2
    check_period          24x7
    check_freshness       1
    contact_groups        admins
    notification_interval 2
    notification_period   24x7
    notifications_enabled 1
    register              1
}

#####
# END OF FILE
#####

```

The terminal window shows the configuration file 'Windows137.cfg' being edited with the nano 2.9.3 text editor. The file content is identical to the one shown above, including the host and service definitions and the '# END OF FILE' marker. The bottom of the window displays the nano command-line interface with various keyboard shortcuts for editing.

- Ahora entramos en el archivo de configuración nagios.cfg y habilitamos la carpeta de Windows.

```
GNU nano 2.9.3                                     nagios.cfg

log_file=/usr/local/nagios/var/nagios.log

# OBJECT CONFIGURATION FILE(S)
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.

# You can specify individual object config files as shown below:
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg

# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

# Definitions for monitoring a Windows machine
cfg_file=/usr/local/nagios/etc/objects/windows.cfg

# Definitions for monitoring a router/switch
#cfg_file=/usr/local/nagios/etc/objects/switch.cfg

# Definitions for monitoring a network printer
#cfg_file=/usr/local/nagios/etc/objects/printer.cfg

# You can also tell Nagios to process all config files (with a .cfg
# extension) in a particular directory by using the cfg_dir
[ Wrote 1378 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text  ^J Justify   ^C Cur Pos    M-U Undo
^X Exit      ^R Read File   ^N Replace    ^U Uncut Text ^T To Spell  ^L Go To Line M-E Redo
```

- Si no se encuentran errores en la configuración, reiniciamos el servicio nagios.

```

root@usuario:/usr/local/nagios/etc# service nagios restart
root@usuario:/usr/local/nagios/etc# service nagios status
● nagios.service - Nagios Core 4.4.5
   Loaded: loaded (/lib/systemd/system/nagios.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2020-03-27 21:31:43 CET; 1s ago
     Docs: https://www.nagios.org/documentation
 Process: 4539 ExecStopPost=/bin/rm -f /usr/local/nagios/var/rw/nagios.cmd (code=exited, status=0/S)
 Process: 4525 ExecStop=/bin/kill -s TERM ${MAINPID} (code=exited, status=0/SUCCESS)
 Process: 4588 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exi
 Process: 4577 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=
Main PID: 4593 (nagios)
   Tasks: 8 (limit: 2318)
  CGroup: /system.slice/nagios.service
          ├─4593 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
          ├─4594 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
          ├─4595 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
          ├─4596 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
          ├─4597 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
          ├─4604 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
          └─4605 /usr/local/nagios/libexec/check_ping -H 192.168.1.142 -w 3000.0,80% -c 5000.0,100%
             ├─4606 /bin/ping -n -U -W 30 -c 5 192.168.1.142

mar 27 21:31:43 usuario nagios[4593]: qh: Socket '/usr/local/nagios/var/rw/nagios.qh' successfully i
mar 27 21:31:43 usuario nagios[4593]: qh: core query handler registered
mar 27 21:31:43 usuario nagios[4593]: qh: echo service query handler registered
mar 27 21:31:43 usuario nagios[4593]: qh: help for the query handler registered
mar 27 21:31:43 usuario nagios[4593]: wproc: Successfully registered manager as @wproc with query ha
mar 27 21:31:43 usuario nagios[4593]: wproc: Registry request: name=Core Worker 4597;pid=4597
mar 27 21:31:43 usuario nagios[4593]: wproc: Registry request: name=Core Worker 4596;pid=4596
mar 27 21:31:43 usuario nagios[4593]: wproc: Registry request: name=Core Worker 4595;pid=4595
mar 27 21:31:43 usuario nagios[4593]: wproc: Registry request: name=Core Worker 4594;pid=4594
mar 27 21:31:43 usuario nagios[4593]: Successfully launched command file worker with pid 4604
lines 1-30/30 (END)

```

Paso 3. Verificar el host en la interfaz web de Nagios.

Abrimos la interfaz web de nagios y comprobamos si hay nuevos hosts agregados en el servicio central de nagios. En mi caso, se ve a continuación.

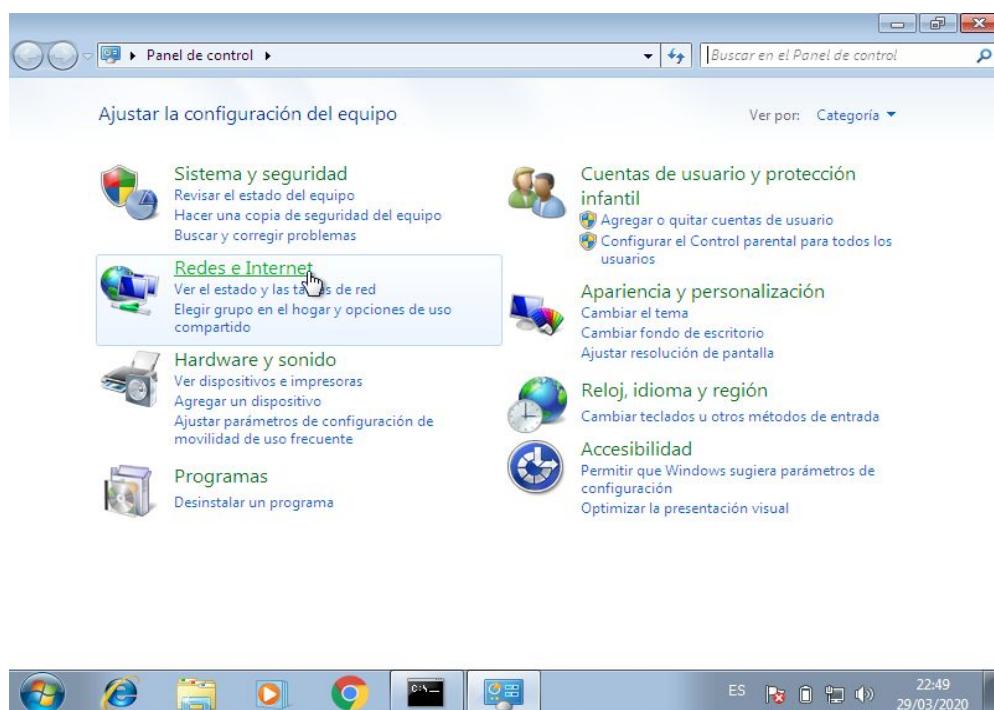
The screenshot shows the Nagios web interface at the URL <http://192.168.1.141/nagios/>. The left sidebar has navigation links for General, Current Status, Hosts, Services, and Host Groups. The main content area includes:

- Current Network Status:** Last Updated: Fri Mar 27 21:41:41 CET 2020. Shows Nagios® Core™ 4.4.5 - www.nagios.org.
- Host Status Totals:** Up: 3, Down: 1, Unreachable: 0, Pending: 0. All Problems: 1, All Types: 4.
- Service Status Totals:** Ok: 10, Warning: 0, Unknown: 0, Critical: 7, Pending: 0. All Problems: 7, All Types: 17.
- Host Status Details For All Host Groups:** A table showing host status information for three hosts: cliente-VirtualBox, cliente-PC, and localhost. All hosts are UP.

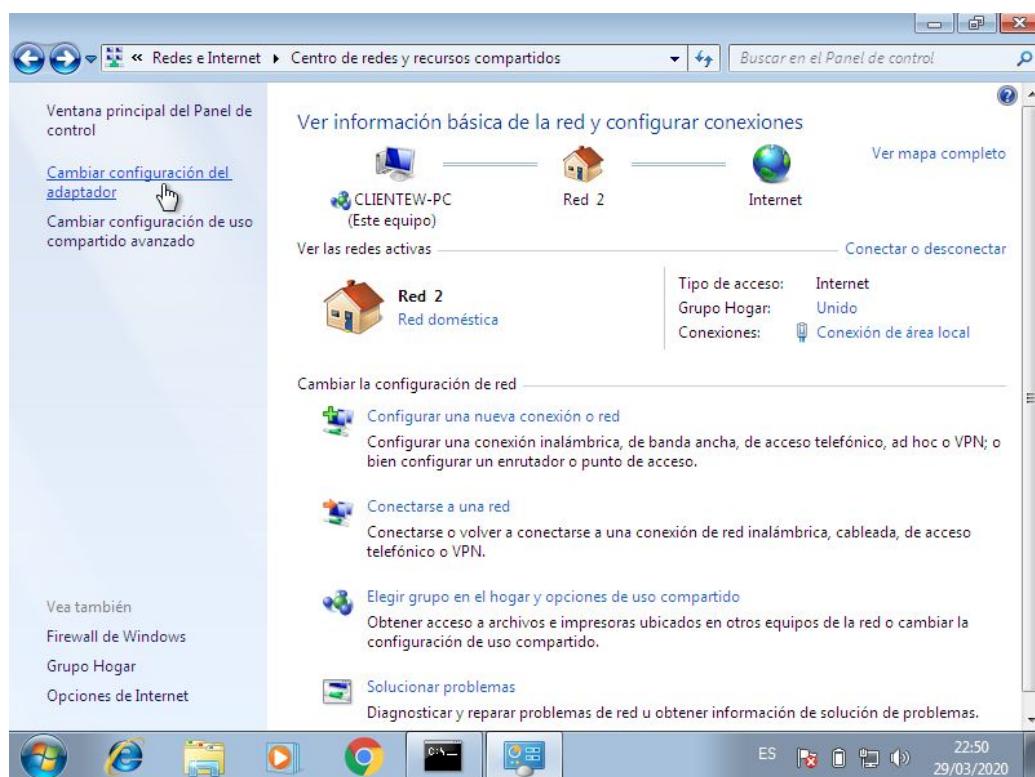
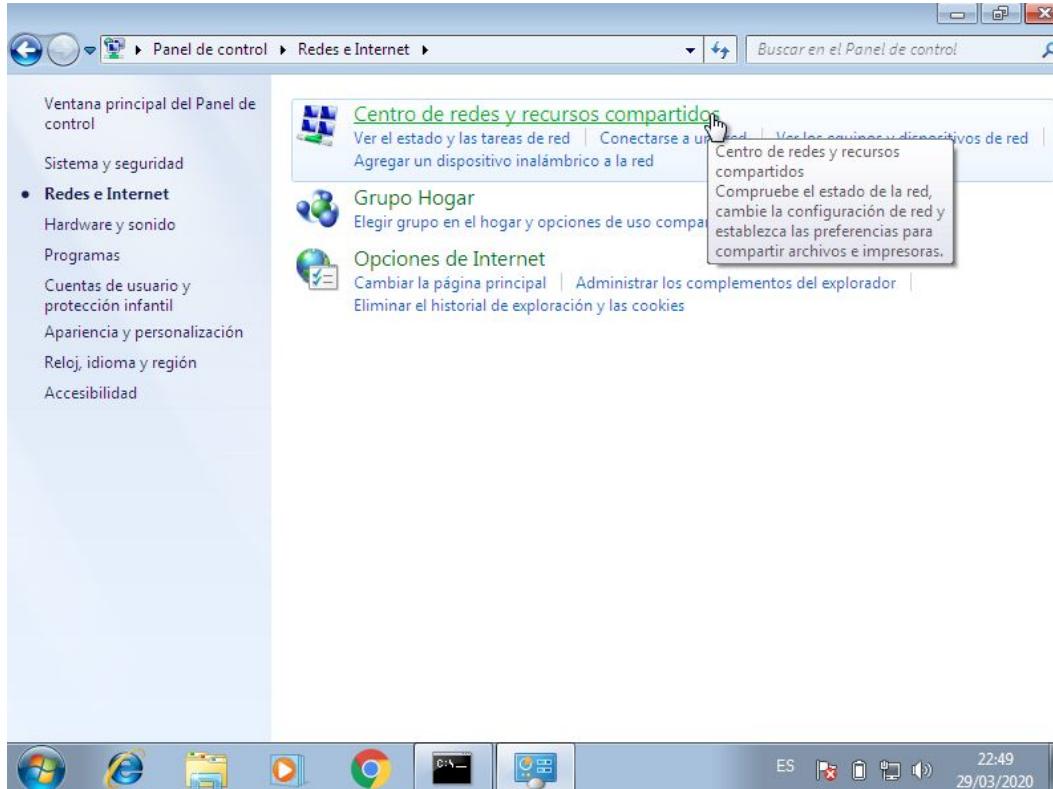
The screenshot shows the Nagios web interface at the URL 192.168.1.141/nagios/. The left sidebar contains navigation links for General, Documentation, Current Status, Reports, and System. The main content area displays 'Host Information' for 'Windows Host 001 (clientew-PC)'. It shows the host is up ('UP') for 0d 0h 0m 44s, with PING OK - Packet loss = 0%, RTA = 0.74 ms. The 'Host State Information' section shows various status metrics like Performance Data, Current Attempt, and Check Type. The 'Host Commands' section lists actions like 'Locate host on map' and 'Disable active checks of this host'. The 'Host Comments' section allows for adding or deleting comments.

Paso 4. Configurar IP fija.

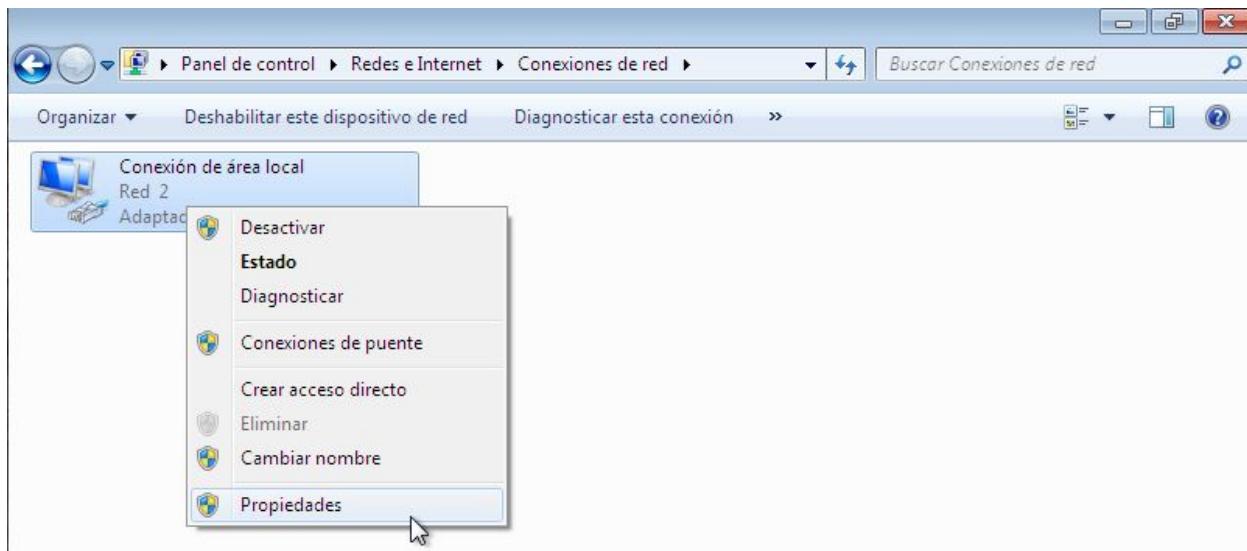
- Para que no nos cambie la IP y tengamos que modificar constantemente los archivos debemos configurarla de la siguiente manera.
 - Primero entramos en el panel de control y en redes e internet.



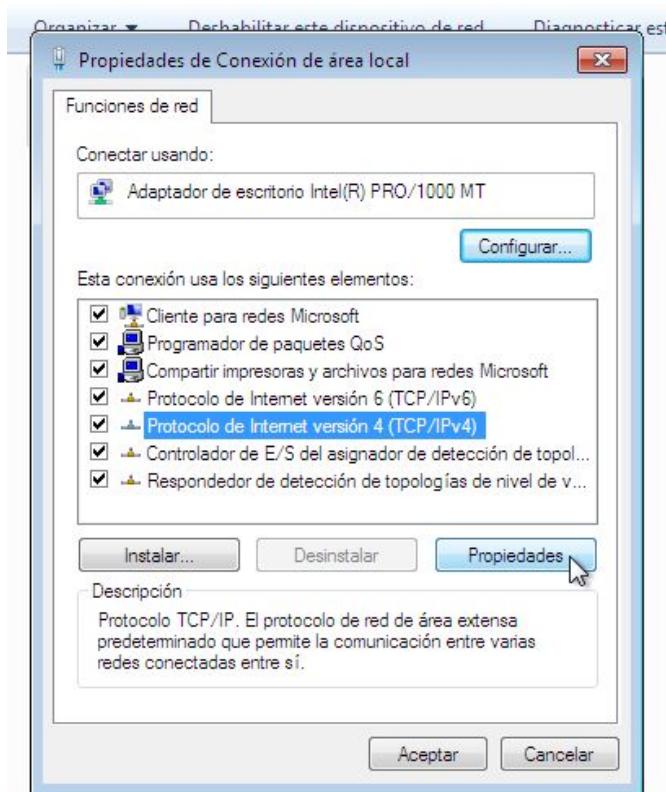
- A continuación, entramos en centro de redes y recursos compartidos y en cambiar configuración del adaptador.



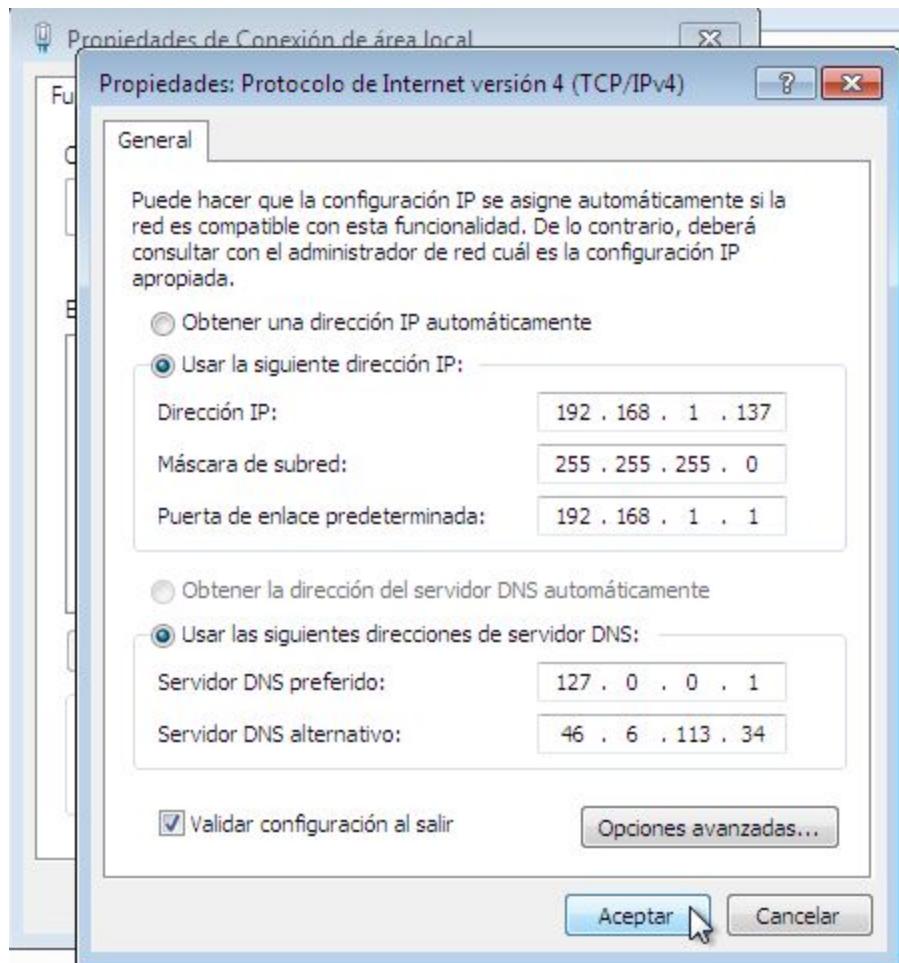
- Ahora hacemos click con el botón derecho y entramos en propiedades.



- Elegimos IPv4 y hacemos click en propiedades.



- Por último configuramos manualmente todo lo necesario, le damos a validar configuración al salir y aceptamos.



Capítulo 5

Notificaciones por correo.

Paso 1. Configuración.

- Primeramente editaremos el fichero de contactos donde se puede configurar la dirección o direcciones de correo donde vamos a enviar las notificaciones.
 - `sudo nano /usr/local/nagios/etc/objects/contacts.cfg`
 - Ejemplo:

```
define contact{

    contact_name      nagiosadmin      ; Short name of user
    use               generic-contact   ; Inherit default values from generic-contact
    alias             Nagios Admin     ; Full name of user
    email             micorreo@electrónico.com ;<< Dirección para notificaciones ***
}

}
```

```

GNU nano 2.9.3                               /usr/local/nagios/etc/objects/contacts.cfg      Modified

#####
# CONTACTS.CFG - SAMPLE CONTACT/CONTACTGROUP DEFINITIONS
#
#
# NOTES: This config file provides you with some example contact and contact
# group definitions that you can reference in host and service
# definitions.
#
# You don't need to keep these definitions in a separate file from your
# other object definitions. This has been done just to make things
# easier to understand.
#
#####

#
# CONTACTS
#
#####

# Just one contact defined by default - the Nagios admin (that's you)
# This contact definition inherits a lot of default values from the
# 'generic-contact' template which is defined elsewhere.

define contact {

    contact_name          nagiosadmin           ; Short name of user
    use                   generic-contact        ; Inherit default values from generic-contact t$
    alias                Nagios Admin          ; Full name of user
    email                angelaagmez@gmail.com ; <<***** CHANGE THIS TO YOUR EMAIL ADDRESS *****

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo
^X Exit       ^R Read File   ^L Replace    ^U Uncut Text ^I To Spell   ^P Go To Line M-E Redo

```

- Ponemos el servidor en la zona horaria correcta:
 - sudo timedatectl set-timezone Europe/Madrid

- Damos permisos a la carpeta de cola:
 - sudo chmod 777 /var/spool/mqueue-client/

```
root@usuario:/opt/nagios-plugins-2.2.1# timedatectl set-timezone Europe/Madrid
root@usuario:/opt/nagios-plugins-2.2.1# chmod 777 /var/spool/mqueue-client/
chmod: cannot access '/var/spool/mqueue-client/': No such file or directory
root@usuario:/opt/nagios-plugins-2.2.1# cd /var/spool/
root@usuario:/var/spool# ls
cron  mail  rsyslog
root@usuario:/var/spool# cd /opt/nagios-plugins-2.2.1
root@usuario:/opt/nagios-plugins-2.2.1# chmod 777 /var/spool/mail/
```

- Ya podemos enviar una notificación de prueba.

Paso 2. Resultado.

- Notificación recibida:

```
root@usuario:/usr/local/nagios/etc/servers# cat /var/mail/root
From nagios@usuario.Home Fri Mar 27 21:01:11 2020
Return-Path: <nagios@usuario.Home>
X-Original-To: root@localhost
Delivered-To: root@localhost
Received: by usuario.Home (Postfix, from userid 1001)
           id 497291E0B90; Fri, 27 Mar 2020 21:01:11 +0100 (CET)
To: root@localhost
Subject: ** PROBLEM Service Alert: localhost/Disk Space is CRITICAL ***
MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit
Message-Id: <20200327200111.497291E0B90@usuario.Home>
Date: Fri, 27 Mar 2020 21:01:11 +0100 (CET)
From: nagios@usuario.Home

***** Nagios *****

Notification Type: PROBLEM

Service: Disk Space
Host: localhost
Address: 127.0.0.1
State: CRITICAL

Date/Time: Fri Mar 27 21:01:11 CET 2020

Additional Info:

DISK CRITICAL - free space: /snap/core/8268 0 MB (0% inode=0%): /snap/core/8689 0 MB (0% inode=0%):
```

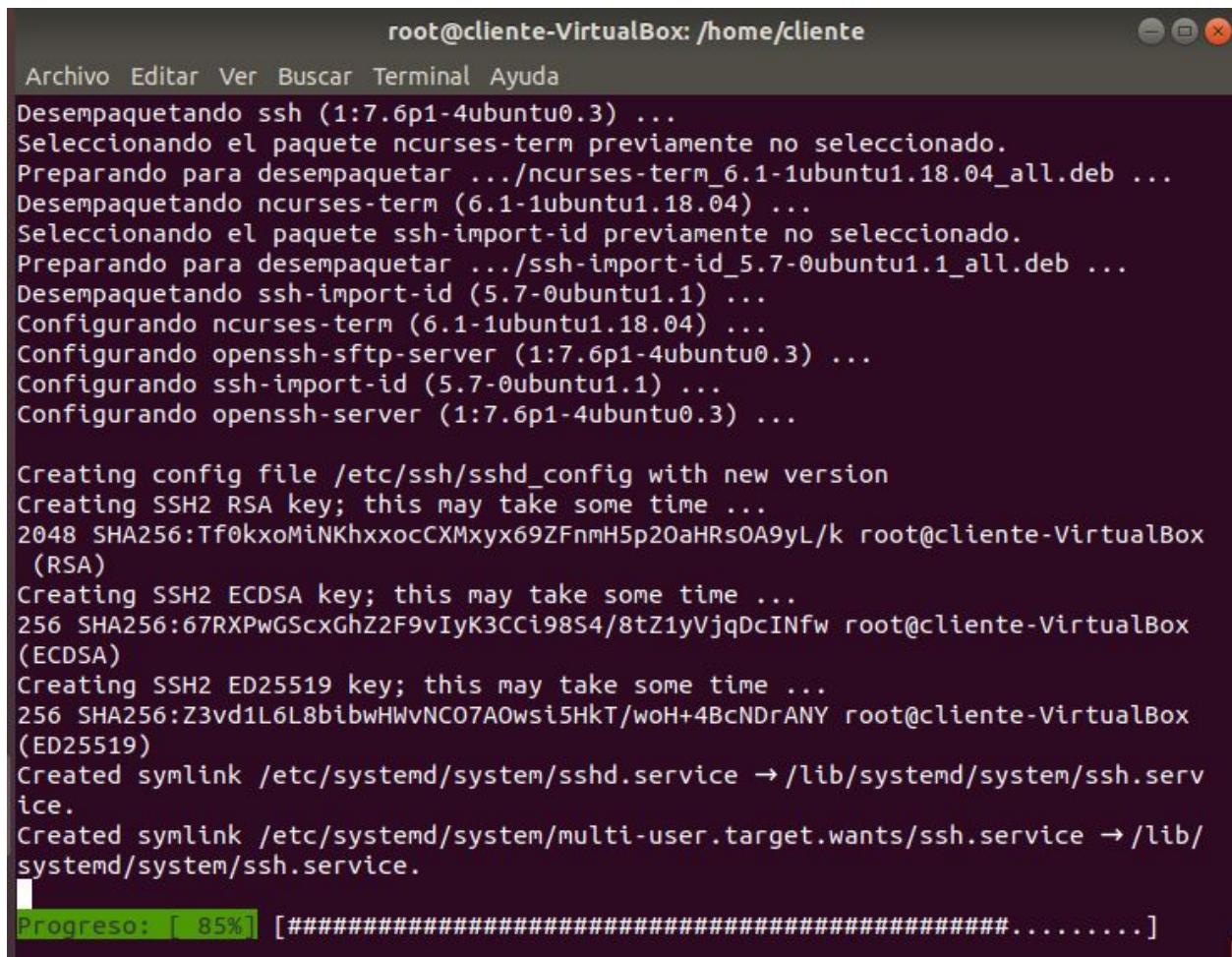
Capítulo 6

Monitorizar servicios Linux

Paso 1. Instalaciones necesarias.

- Instalamos ssh con el siguiente comando:

- apt install ssh



The screenshot shows a terminal window titled "root@cliente-VirtualBox: /home/cliente". The window contains the following text output from an apt install ssh command:

```
root@cliente-VirtualBox: /home/cliente
Archivo Editar Ver Buscar Terminal Ayuda
Desempaquetando ssh (1:7.6p1-4ubuntu0.3) ...
Seleccionando el paquete ncurses-term previamente no seleccionado.
Preparando para desempaquetar .../ncurses-term_6.1-1ubuntu1.18.04_all.deb ...
Desempaquetando ncurses-term (6.1-1ubuntu1.18.04) ...
Seleccionando el paquete ssh-import-id previamente no seleccionado.
Preparando para desempaquetar .../ssh-import-id_5.7-0ubuntu1.1_all.deb ...
Desempaquetando ssh-import-id (5.7-0ubuntu1.1) ...
Configurando ncurses-term (6.1-1ubuntu1.18.04) ...
Configurando openssh-sftp-server (1:7.6p1-4ubuntu0.3) ...
Configurando ssh-import-id (5.7-0ubuntu1.1) ...
Configurando openssh-server (1:7.6p1-4ubuntu0.3) ...

Creating config file /etc/ssh/sshd_config with new version
Creating SSH2 RSA key; this may take some time ...
2048 SHA256:Tf0kxoMiNKhxxocCXMxyx69ZFnmH5p20aHRsOA9yL/k root@cliente-VirtualBox
(RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:67RXPwGScxGhZ2F9vIyK3CCi98S4/8tZ1yVjqDcINfw root@cliente-VirtualBox
(ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:Z3vd1L6L8bibwHWvNC07AOws15HkT/woH+4BcNDrANY root@cliente-VirtualBox
(ED25519)
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/
systemd/system/ssh.service.

[ Progreso: [ 85%] [#####
.....] ]
```

- Instalar plugins nagios en todas la máquinas:
 - Vamos a instalar NRPE en todas las máquinas si no lo tenemos instalado previamente. Es el software que permite ejecutar remotamente los plugins de Nagios en otros equipos, lo que permite monitorizar los parámetros de la máquina remota.
 - `apt install nagios-nrpe-server nagios-nrpe-plugin nagios-plugins`

```
root@cliente-VirtualBox:/home/cliente# apt install nagios-nrpe-server nagios-nrpe-plugin nagios-plugins
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
nagios-nrpe-server ya está en su versión más reciente (3.2.1-1ubuntu1).
nagios-plugins ya está en su versión más reciente (2.2-3ubuntu2).
Se instalarán los siguientes paquetes NUEVOS:
  nagios-nrpe-plugin
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
Se necesita descargar 22,9 kB de archivos.
Se utilizarán 77,8 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Paso 2. Configuraciones necesarias.

- Vamos a editar el fichero:
 - `/etc/nagios/nrpe.cfg`
- Debemos permitir el acceso al servidor de Nagios añadiendo su IP, este proceso lo vamos a realizar en todas las máquinas, para ello en todas las máquinas añadimos la ip del servidor y permitimos que se reciban argumentos en los comandos.
 - `allowed_hosts=127.0.0.1,[IP_Maquina]`
 - `dont_blame_nrpe=1`

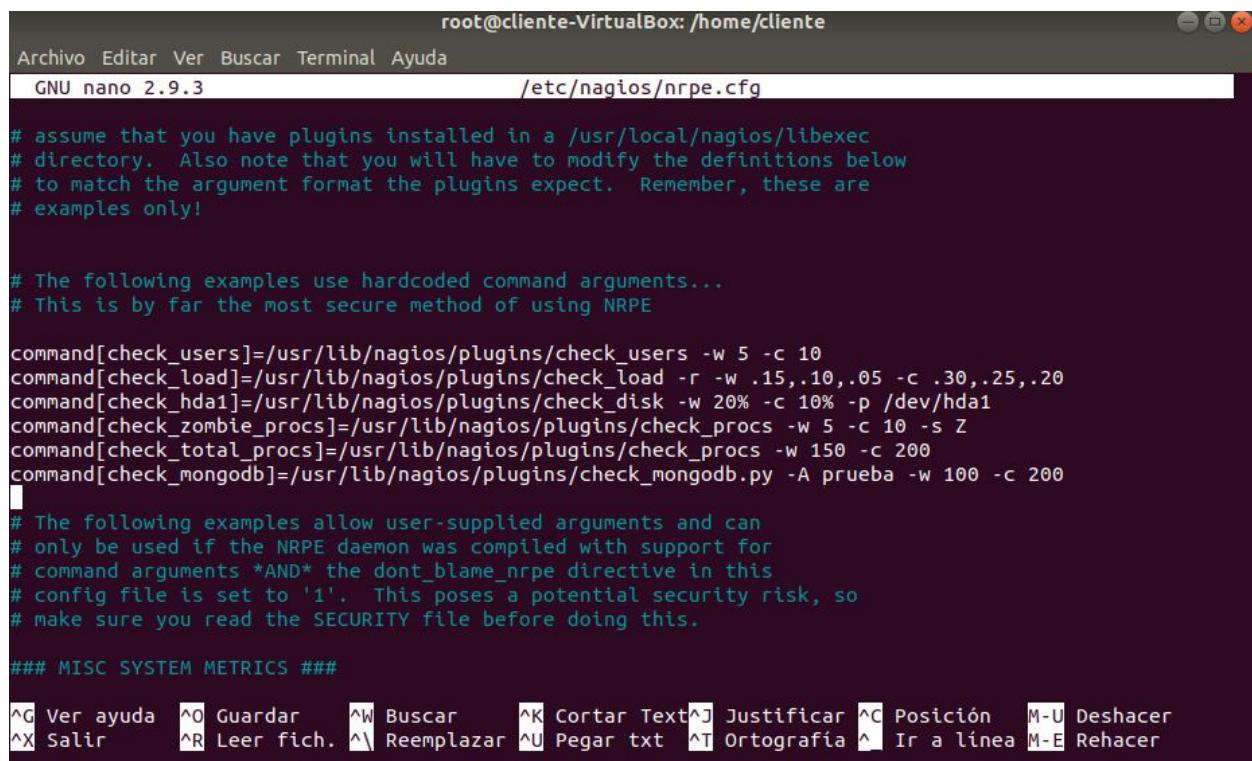
```
GNU nano 2.9.3                               /etc/nagios/nrpe.cfg

# NRPE GROUP
# This determines the effective group that the NRPE daemon should run as.
# You can either supply a group name or a GID.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd
nrpe_group=nagios

#
# ALLOWED HOST ADDRESSES
# This is an optional comma-delimited list of IP address or hostnames
# that are allowed to talk to the NRPE daemon. Network addresses with a bit mask
# (i.e. 192.168.1.0/24) are also supported. Hostname wildcards are not currently
# supported.
#
# Note: The daemon only does rudimentary checking of the client's IP
# address. I would highly recommend adding entries in your /etc/hosts.allow
# file to allow only the specified host to connect to the port
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd
allowed_hosts=127.0.0.1,192.168.1.144
dont_blame_nrpe=1

#
# COMMAND ARGUMENT PROCESSING
# This option determines whether or not the NRPE daemon will allow clients
[ Wrote 375 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo
^X Exit      ^R Read File  ^Y Replace   ^U Uncut Text ^T To Spell   ^L Go To Line M-E Redo
```

- En este fichero, más abajo, vienen ya algunos plugins predefinidos al cual le cambiaremos los valores a nuestro interés.
- Principalmente podremos cambiar los valores “-w (warm)” y “-c (critical)” donde en cada línea le estaremos diciendo que si el valor de “-w” es superado nos lo indique como advertencia y si supera el valor de “-c” nos lo indique como una situación crítica.
- Estos son los diferentes plugins que vamos a configurar (vamos a dejar la mayoría de los que vienen por defecto):



```

root@cliente-VirtualBox: /home/cliente
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3           /etc/nagios/nrpe.cfg

# assume that you have plugins installed in a /usr/local/nagios/libexec
# directory. Also note that you will have to modify the definitions below
# to match the argument format the plugins expect. Remember, these are
# examples only!

# The following examples use hardcoded command arguments...
# This is by far the most secure method of using NRPE

command[check_users]=/usr/lib/nagios/plugins/check_users -w 5 -c 10
command[check_load]=/usr/lib/nagios/plugins/check_load -r -w .15,.10,.05 -c .30,.25,.20
command[check_hda1]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /dev/hda1
command[check_zombie_procs]=/usr/lib/nagios/plugins/check_procs -w 5 -c 10 -s Z
command[check_total_procs]=/usr/lib/nagios/plugins/check_procs -w 150 -c 200
command[check_mongodb]=/usr/lib/nagios/plugins/check_mongodb.py -A prueba -w 100 -c 200

# The following examples allow user-supplied arguments and can
# only be used if the NRPE daemon was compiled with support for
# command arguments *AND* the dont_blame_nrpe directive in this
# config file is set to '1'. This poses a potential security risk, so
# make sure you read the SECURITY file before doing this.

### MISC SYSTEM METRICS ###

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Text^J Justificar ^C Posición M-U Deshacer
^X Salir    ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^ I Ir a línea M-E Rehacer

```

- Reiniciamos el servicio en todas las máquinas:

- service nagios-nrpe-server restart

Paso 3. Monitorizar servicio SSH.

- Vamos a controlar el estado del servicio SSH en Linux, para ello entramos en el fichero creado y escribimos al final:

```
GNU nano 2.9.3          /usr/local/nagios/etc/servers/Linux142.cfg ^

#####
# Linux Host 001 configuration file
#####

define host {
    use                  linux-server
    host_name            cliente-VirtualBox
    alias                Linux Host 001
    address              192.168.1.144
    register             1
}
define service{
    host_name            cliente-VirtualBox
    service_description  PING
    check_command        check_ping!100.0,20%!500.0,60%
    max_check_attempts   2
    check_interval       2
    retry_interval       2
    check_period         24x7
    check_freshness      1
    contact_groups       admins
    notification_interval 2
    notification_period  24x7
    notifications_enabled 1
    register             1
}

define service{
    use                  generic-service
    host_name            cliente-VirtualBox
    service_description  SSH
    check_command        check_ssh
}

#####
[ Read 37 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

```

- Reiniciamos el servicio:

- /etc/init.d/nagios3 restart

```
root@usuario:/home/usuario# /etc/init.d/nagios3 restart
[ ok ] Restarting nagios3 (via systemctl): nagios3.service.
```

Paso 4. Monitorizar servicio HTTP.

- Agregamos el servicio en el fichero de nuestro host.

- nano /usr/local/nagios/etc/servers/Linux142.cfg

```

■ define service{

    use          generic-service,srv-pnp

    host_name    cliente-VirtualBox

    service_description HTTP

    check_command  check_http

}

```

```

define service{
    use          generic-service,srv-pnp
    host_name    cliente-VirtualBox
    service_description HTTP
    check_command  check_http
}

```

Paso 5. Monitorizar servicio PING.

- Agregamos el servicio en el fichero de nuestro host.

- nano /usr/local/nagios/etc/servers/Linux142.cfg

```

■ define service{

    use          generic-service,srv-pnp

    host_name    cliente-VirtualBox

    service_description PING

    check_command  check_ping

}

```

```
define service{
    use generic-service,srv-pnp
    host_name cliente-VirtualBox
    service_description PING
    check_command check_ping
}
```

- Nos vamos al fichero commands.cfg y editamos los parámetros \$ARG1\$, \$ARG2\$ y \$ARG3\$.
 - nano /usr/local/nagios/etc/objects/commands.cfg

```
define command {
    command_name check_ping
    command_line $USER1$/check_ping -H $HOSTADDRESS$ -w 10.0,80% -c 15.0,100% -p 5
}
```

Paso 6. Monitorizar disco.

- Agregamos el servicio en el fichero de nuestro host.
 - nano /usr/local/nagios/etc/servers/Linux142.cfg
 - define service{
 - use generic-service,srv-pnp
 - host_name cliente-VirtualBox
 - service_description LOCAL DISK
 - check_command check_local_disk

```
define service{
    use generic-service,srv-pnp
    host_name cliente-VirtualBox
    service_description LOCAL DISK
    check_command check_local_disk
}
```

- Nos vamos al fichero commands.cfg y editamos los parámetros \$ARG1\$, \$ARG2\$ y \$ARG3\$ según nos convenga.
 - nano /usr/local/nagios/etc/objects/commands.cfg

```
define command {
    command_name check_local_disk
    command_line $USER1$/check_disk -w 40% -c 15% -p /dev/sda2
}
```

Paso 7. Monitorizar usuarios.

- Agregamos el servicio en el fichero de nuestro host.
 - nano /usr/local/nagios/etc/servers/Linux142.cfg
 - define service{
 - use generic-service,srv-pnp
 - host_name cliente-VirtualBox
 - service_description LOCAL USERS
 - check_command check_local_users

```
define service{
    use generic-service,srv-pnp
    host_name cliente-VirtualBox
    service_description LOCAL USERS
    check_command check_local_users
}
```

- Nos vamos al fichero commands.cfg y editamos los parámetros \$ARG1\$ y \$ARG2\$.
 - nano /usr/local/nagios/etc/objects/commands.cfg

```
define command {
    command_name check_local_users
    command_line $USER1$/check_users -w 4 -c 5
}
```

Paso 8. Monitorizar procesos.

- Agregamos el servicio en el fichero de nuestro host.
 - nano /usr/local/nagios/etc/servers/Linux142.cfg
 - define service{
 - use generic-service,srv-pnp
 - host_name cliente-VirtualBox
 - service_description LOCAL PROCESS
 - check_command check_local_procs

```
define service{
    use generic-service,srv-pnp
    host_name cliente-VirtualBox
    service_description LOCAL PROCESS
    check_command check_local_procs
}
```

- Nos vamos al fichero commands.cfg y editamos los parámetros \$ARG1\$ y \$ARG2\$.
 - nano /usr/local/nagios/etc/objects/commands.cfg

```
define command {
    command_name check_local_procs
    command_line $USER1$/check_procs -w 250 -c 400 -s bash
}
```

Paso 9. Monitorizar swap.

- Agregamos el servicio en el fichero de nuestro host.
 - nano /usr/local/nagios/etc/servers/Linux142.cfg
 - define service{
 - use generic-service,srv-pnp
 - host_name cliente-VirtualBox
 - service_description LOCAL SWAP
 - check_command check_local_swap

```
define service{
    use generic-service,srv-pnp
    host_name cliente-VirtualBox
    service_description LOCAL SWAP
    check_command check_local_swap
}
```

- Nos vamos al fichero commands.cfg y editamos los parámetros \$ARG1\$ y \$ARG2\$.
 - nano /usr/local/nagios/etc/objects/commands.cfg

```
define command {
    command_name check_local_swap
    command_line $USER1$/check_swap -w 40% -c 15%
}
```

Paso 10. Monitorizar carga.

- Agregamos el servicio en el fichero de nuestro host.
 - nano /usr/local/nagios/etc/servers/Linux142.cfg
 - define service{
 - use generic-service,srv-pnp
 - host_name cliente-VirtualBox
 - service_description LOCAL LOAD
 - check_command check_local_load

```
define service{
    use generic-service,srv-pnp
    host_name cliente-VirtualBox
    service_description LOCAL LOAD
    check_command check_local_load
}
```

- Nos vamos al fichero commands.cfg y editamos los parámetros \$ARG1\$ y \$ARG2\$.
 - nano /usr/local/nagios/etc/objects/commands.cfg

```
define command {
    command_name check_local_load
    command_line $USER1$/check_load -w 15,10,5 -c 30,25,20
}
```

Paso 11. Monitorizar TCP.

- Agregamos el servicio en el fichero de nuestro host.
 - nano /usr/local/nagios/etc/servers/Linux142.cfg
 - define service{
 - use generic-service,srv-pnp
 - host_name cliente-VirtualBox
 - service_description TCP
 - check_command check_tcp

```
define service{
    use generic-service,srv-pnp
    host_name cliente-VirtualBox
    service_description TCP
    check_command check_tcp
}
```

- Nos vamos al fichero commands.cfg y editamos los parámetros \$ARG1\$ y \$ARG2\$.
 - nano /usr/local/nagios/etc/objects/commands.cfg

```
define command {
    command_name check_tcp
    command_line $USER1$/check_tcp -H $HOSTADDRESS$ -p 22 5666
}
```

Paso 12. Comprobación del funcionamiento.

- Comprobamos en el navegador que está todo correctamente y no nos da ningún tipo de problema:

The screenshot shows the Nagios web interface with the following sections:

- Current Network Status:** Last Updated: Tue Apr 21 19:42:33 CEST 2020. Shows 1 Up, 0 Down, 0 Unreachable, and 0 Pending hosts.
- Host Status Totals:** Shows 9 Ok, 0 Warning, 0 Unknown, 0 Critical, and 0 Pending services.
- Service Status Details For Host 'cliente-VirtualBox':** A table listing services and their status. Services include HTTP, LOCAL DISK, LOCAL LOAD, LOCAL PROCESS, LOCAL SWAP, LOCAL USERS, PING, SSH, and TCP. All services are shown as OK.
- Left Sidebar:** Includes links for General, Home, Documentation, Current Status (with a sub-menu for Tactical Overview, Map (Legacy), Hosts, Services, Host Groups, Service Groups, Problems, Reports, and Availability).
- Bottom Footer:** Results 1 - 9 of 9 Matching Services.

Capítulo 7

Monitorizar servicios Windows

- Entramos en el archivo que creamos para nuestro host de Windows:
 - cd /usr/local/nagios/etc/servers
 - nano Windows137.cfg

- Escribimos los servicios que queramos monitorizar:
 - Creamos un servicio para monitorizar la versión de NSClient++ que hemos instalado.

```

■ define service {

    use          generic-service

    host_name    clientew-PC

    service_description  NSClient++ Version

    check_command   check_nt!CLIENTVERSION

}

```

```

define service {
    use          generic-service
    host_name    clientew-PC
    service_description  NSClient++ Version
    check_command   check_nt!CLIENTVERSION
}

```

- Creamos un servicio para monitorizar el uptime del servidor.

```
■ define service {

    use          generic-service
    host_name    clientew-PC
    service_description Uptime
    check_command   check_nt!UPTIME
}
```

```
define service {
    use          generic-service
    host_name    clientew-PC
    service_description Uptime
    check_command   check_nt!UPTIME
}
```

- Creamos un servicio para monitorizar la carga de CPU.

```
■ define service {

    use          generic-service
    host_name    clientew-PC
    service_description CPU Load
    check_command   check_nt!CPULOAD!-l 5,80,90
}
```

```
define service {
    use          generic-service
    host_name    clientew-PC
    service_description CPU Load
    check_command   check_nt!CPULOAD!-l 5,80,90
}
```

- Creamos un servicio para monitorizar el uso de la memoria.

```
■ define service {
    use          generic-service
    host_name    clientew-PC
    service_description Memory Usage
    check_command   check_nt!MEMUSE!-w 80 -c 90
}
```

```
define service {
    use          generic-service
    host_name    clientew-PC
    service_description Memory Usage
    check_command   check_nt!MEMUSE!-w 80 -c 90
}
```

- Creamos un servicio para monitorizar el uso del disco.

```
■ define service {
    use          generic-service
    host_name    clientew-PC
    service_description C:\ Drive Space
    check_command   check_nt!USEDISKSPACE!-l c -w 80 -c 90
}
```

```
define service {
    use          generic-service
    host_name    clientew-PC
    service_description C:\ Drive Space
    check_command   check_nt!USEDISKSPACE!-l c -w 80 -c 90
}
```

- Creamos un servicio para monitorizar el servicio W3SVC.

```
■ define service {  
  
    use          generic-service  
  
    host_name    clientew-PC  
  
    service_description  W3SVC  
  
    check_command      check_nt!SERVICESTATE!-d SHOWALL -l  
  
    W3SVC  
  
}
```

```
define service {  
    use          generic-service  
    host_name    clientew-PC  
    service_description  W3SVC  
    check_command      check_nt!SERVICESTATE!-d SHOWALL -l W3SVC  
}
```

- Creamos un servicio para monitorizar el proceso Explorer.exe.

```
■ define service {  
  
    use          generic-service  
  
    host_name    clientew-PC  
  
    service_description  Explorer  
  
    check_command      check_nt!PROCSTATE!-d SHOWALL -l  
  
    Explorer.exe  
  
}
```

```
define service {
    use generic-service
    host_name clientew-PC
    service_description Explorer
    check_command check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe
}
```

- Así quedaría el fichero de configuración total:

GNU nano 2.9.3 Windows137.cfg

```
host_name clientew-PC
service_description NSClient++ Version
check_command check_nt!CLIENTVERSION

}

define service {
    use generic-service
    host_name clientew-PC
    service_description Uptime
    check_command check_nt!UPTIME
}

define service {
    use generic-service
    host_name clientew-PC
    service_description CPU Load
    check_command check_nt!CPULOAD!-1 5,80,90
}

define service {
    use generic-service
    host_name clientew-PC
    service_description Memory Usage
    check_command check_nt!MEMUSE!-w 80 -c 90
}

define service {
    use generic-service
    host_name clientew-PC
    service_description C:\ Drive Space
    check_command check_nt!USEDISKSPACE!-1 c -w 80 -c 90
}

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

```
GNU nano 2.9.3                               Windows137.cfg

3

define service {
    use                      generic-service
    host_name                clientew-PC
    service_description        W3SVC
    check_command              check_nt!SERVICESTATE!-d SHOWALL -1 W3SVC
}

define service {
    use                      generic-service
    host_name                clientew-PC
    service_description        Explorer
    check_command              check_nt!PROCSTATE!-d SHOWALL -1 Explorer.exe
}

#####
# END OF FILE
#####

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

- Para que no nos de ningún tipo de error tenemos que modificar el archivo commands.cfg y añadir lo siguiente en nt y nrpe:

```

GNU nano 2.9.3          /usr/local/nagios/etc/objects/commands.cfg

command_line  $USER1$/check_tcp -H $HOSTADDRESS$ -p $ARG1$ $ARG2$


define command {
    command_name  check_udp
    command_line   $USER1$/check_udp -H $HOSTADDRESS$ -p $ARG1$ $ARG2$
}

define command {
    command_name  check_nt
    command_line   $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -s usuario -v $ARG1$ $ARG2$
}

define command {
    command_name  check_nrpe
    command_line   $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$ -t 25
}

#####
#
# # SAMPLE PERFORMANCE DATA COMMANDS
#
# These are sample performance data commands that can be used to send performance
# data output to two text files (one for hosts, another for services). If you
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  M-U Undo
^X Exit      ^R Read File  ^L Replace  ^U Uncut Text ^T To Spell  ^_ Go To Line M-E Redo

```

- Comprobamos en el navegador, que en Nagios está todo en funcionamiento igual que en capítulo anterior con Linux.

The screenshot shows the Nagios web interface. On the left, there's a navigation sidebar with links like General, Home, Documentation, Current Status, and various monitoring sections. The main content area displays the 'Current Network Status' with a summary table showing 1 Up, 0 Down, 0 Unreachable, and 0 Pending hosts. Below this are 'Host Status Totals' and 'Service Status Totals' tables. The 'Service Status Details For Host 'clientew-PC'' section contains a table with columns: Host, Service, Status, Last Check, Duration, Attempt, and Status Information. The table lists several services: C:\ Drive Space (WARNING), CPU Load (OK), Explorer (OK), Memory Usage (OK), NSClient++ Version (OK), PING (OK), Uptime (OK), and W3SVC (CRITICAL). The status information for W3SVC indicates it was not found.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
clientew-PC	C:\ Drive Space	WARNING	04-21-2020 20:18:58	0d 0h 15m 15s	3/3	c - total: 9.90 Gb - used: 8.25 Gb (83%) - free: 1.65 Gb (17%)
	CPU Load	OK	04-21-2020 20:21:35	0d 0h 2m 38s	1/3	CPU Load 0% (5 min average)
	Explorer	OK	04-21-2020 20:18:01	0d 0h 6m 12s	1/3	explorer.exe: Running
	Memory Usage	OK	04-21-2020 20:18:05	0d 0h 6m 8s	1/3	Memory usage: total:4095.14 MB - used: 422.97 MB (10%) - free: 3672.18 MB (90%)
	NSClient++ Version	OK	04-21-2020 20:22:52	0d 0h 1m 21s	1/3	NSClient++ 0.4.1.73 2012-12-17
	PING	OK	04-21-2020 20:22:25	0d 0h 5m 52s	1/2	PING OK - Packet loss = 0%, RTA = 0.61 ms
	Uptime	OK	04-21-2020 20:19:18	0d 0h 4m 55s	1/3	System Uptime - 0 day(s) 0 hour(s) 44 minute(s)
	W3SVC	CRITICAL	04-21-2020 20:20:05	0d 3h 4m 18s	3/3	W3SVC: Not found

- Ejemplo de otro host Windows 10 que he configurado y añadido:

Nagios®

General

- Home
- Documentation

Current Status

- Tactical Overview Map (Legacy)
- Hosts
- Services
- Host Groups
 - Summary
 - Grid
- Service Groups
 - Summary
 - Grid
- Problems
- Services (Unhandled)
- Hosts (Unhandled)
- Network Outages

Quick Search:

Results 1 - 8 of 8 Matching Services

Current Network Status

Last Updated: Tue Apr 21 18:11:06 CEST 2020
Updated every 90 seconds
Nagios® Core™ 4.4.5 - www.nagios.org
Logged in as nagiosadmin

[View History For This Host](#)
[View Notifications For This Host](#)
[View Service Status Detail For All Hosts](#)

Host Status Totals

Up	0	Down	0	Unreachable	0	Pending	0
All Problems	1	All Types	0				
0		1					

Service Status Totals

Ok	6	Warning	1	Unknown	0	Critical	1	Pending	0
All Problems	6	All Types	1						
2		8							

Service Status Details For Host 'clientew2-PC'

Host	Service	Status	Last Check	Duration	Attempt	Status Information
clientew2-PC	C:\ Drive Space	OK	04-21-2020 18:10:37	0d 1h 0m 29s	1/3	c: - total: 930,28 Gb - used: 376,47 Gb (40%) - free 553,81 Gb (60%)
	CPU Load	OK	04-21-2020 18:01:50	0d 0h 59m 16s	1/3	CPU Load 11% (5 min average)
	Explorer	OK	04-21-2020 18:03:03	0d 0h 58m 3s	1/3	explorer.exe: Running
	Memory Usage	WARNING	04-21-2020 18:08:17	0d 0h 12m 49s	3/3	Memory usage: total: 14059,22 MB - used: 12095,14 MB (86%) - free: 1964,08 MB (14%)
	NSClient++ Version	OK	04-21-2020 18:05:30	0d 0h 55m 36s	1/3	NSClient++, 0.4.1.73 2012-12-17
	PING	OK	04-21-2020 18:10:08	0d 2h 26m 25s	1/2	PING OK - Packet loss = 0%, RTA = 0.87 ms
	Uptime	OK	04-21-2020 18:06:43	0d 0h 54m 23s	1/3	System Uptime - 6 day(s) 2 hour(s) 1 minute(s)
	W3SVC	CRITICAL	04-21-2020 18:01:56	0d 0h 49m 10s	3/3	W3SVC: Not found

Capítulo 8

Asignar iconos a Nagios. Status map.

Paso 1. Dónde localizar las imágenes existentes.

- Las imágenes que Nagios cogerá se guardan en el siguiente directorio:
 - `usr/local/nagios/share/images/logos`

aix.gif	freebsd40.gif	mandrake.jpg	router40.jpg	switch.gif
aix.jpg	freebsd40.jpg	mandrake.png	router40.png	switch.gif
aix.png	freebsd40.png	monitor.png	router.gd2	thin-client.gif
amiga.gd2	globe.png	nagios.gd2	router.gif	thin-client.gif
amiga.gif	graph.gif	nagios.gif	san.gif	turbolinux.gif
amiga.jpg	hp-printer40.gd2	nagiosvrml.png	satellite.png	turbolinux.jpg
amiga.png	hp-printer40.gif	netbsd.gif	server.png	turbolinux.png
apple.gd2	hp-printer40.jpg	netbsd.jpg	signal.png	ultrapenguin.gif
apple.gif	hp-printer40.png	netbsd.png	slackware.gif	ultrapenguin.jpg
apple.jpg	hpux.gd2	next.gif	slackware.jpg	ultrapenguin.png
apple.png	hpux.gif	next.jpg	slackware.png	unicos.gif
beos.gd2	hpux.jpg	next.png	stampede.gif	unicos.jpg
beos.gif	hpux.png	ng-switch40.gd2	stampede.jpg	unicos.png
beos.jpg	hub.gif	ng-switch40.gif	stampede.png	unknown.gif
beos.png	internet_device.png	ng-switch40.jpg	stampede.png	webcamera.png
bluetooth.png	internet.gif	ng-switch40.png	station.gif	wifi.gif
caldera.gd2	ip-pbx.gd2	notebook.gif	storm.gif	wifi.modem.png
caldera.gif	ip-pbx.gif	notebook.gd2	storm.jpg	wifi_modem.png
caldera.jpg	irix.gd2	novell140.gd2	storm.png	win40.gif
cat1900.gd2	irix.gif	novell140.gif	sun40.gif	win40.jpg
cat2900.gd2	irix.jpg	novell140.jpg	sun40.jpg	win40.png
cat5000.gd2	irix.png	novell140.png	sun40.png	workstation.gif
database.gd2	linux40.gd2	openbsd.gif	sun40.gif	workstation.jpg
database.gif	linux40.gif	openbsd.jpg	sun40.jpg	workstation.png
debian.gd2	linux40.jpg	openbsd.png	sun40.png	workstation_locked.png
debian.gif	linux40.png	printer.gif	sunlogo.gif	yellowdog.gif
debian.jpg	logo.gif	printer.gd2	sunlogo.jpg	yellowdog.jpg
debian.png	mac40.gd2	rack-server.gif	suse.gif	yellowdog.png
desktop-server.gd2	mac40.gif	redhat.gif	suse.jpg	
desktop-server.gif	mac40.jpg	redhat.gd2	suse.png	
ethernet_card.png	mainframe.gd2	redhat.jpg	switch40.gif	
fax.gif	mainframe.gif	redhat.png	switch40.gif	
firewall.gd2	mandrake.gd2	router40.gd2	switch40.jpg	
firewall.gif				

root@usuario:/usr/local/nagios/share/images/logos#

- Este directorio no lo tocaremos, sólo si queremos cambiar alguna imagen por otra, tan simple como eliminar un archivo y copiar el nuevo o simplemente machacar uno sobre otro.

Paso 2. Modificación de los ficheros.

- Los ficheros a modificar en mi caso se encuentran en /usr/local/nagios/etc/servers.
- Dichos ficheros son los hosts creados manualmente. Pasamos a editar uno de ellos y encontraremos una estructura parecida a ésta:

```

○ define host {

    host_name           Nombre del host
    alias               Informacion sobre el host
    address             Direccion IP
    icon_image          nombre.gif
    statusmap_image     nombre.gd2
    register            1
}

```

- Lo que nos interesa es la parte en cursiva, “icon_image” y “statusmap_image”.
- El primer host que vamos a usar, como es Linux elegimos las imágenes “linux40.gif” y “linux40.gd2”.

```
GNU nano 2.9.3                               Linux142.cfg

#####
# Linux Host 001 configuration file
#####

define host {
    use                      linux-server
    host_name                cliente-VirtualBox
    alias                     Linux Host 001
    address                  192.168.1.144
    register                 1
    icon_image               linux40.gif
    statusmap_image          linux40.gd2_
}
```

- El segundo host, como es Windows elegimos las imágenes “win40.gif” y “win40.gd2”.

```
GNU nano 2.9.3                               Windows137.cfg

#####
# Windows Host 001 configuration file
#####

define host {
    use                      windows-server
    host_name                clientew-PC
    alias                     Windows Host 001
    address                  192.168.1.137
    register                 1
    icon_image               win40.gif
    statusmap_image          win40.gd2_
}
```

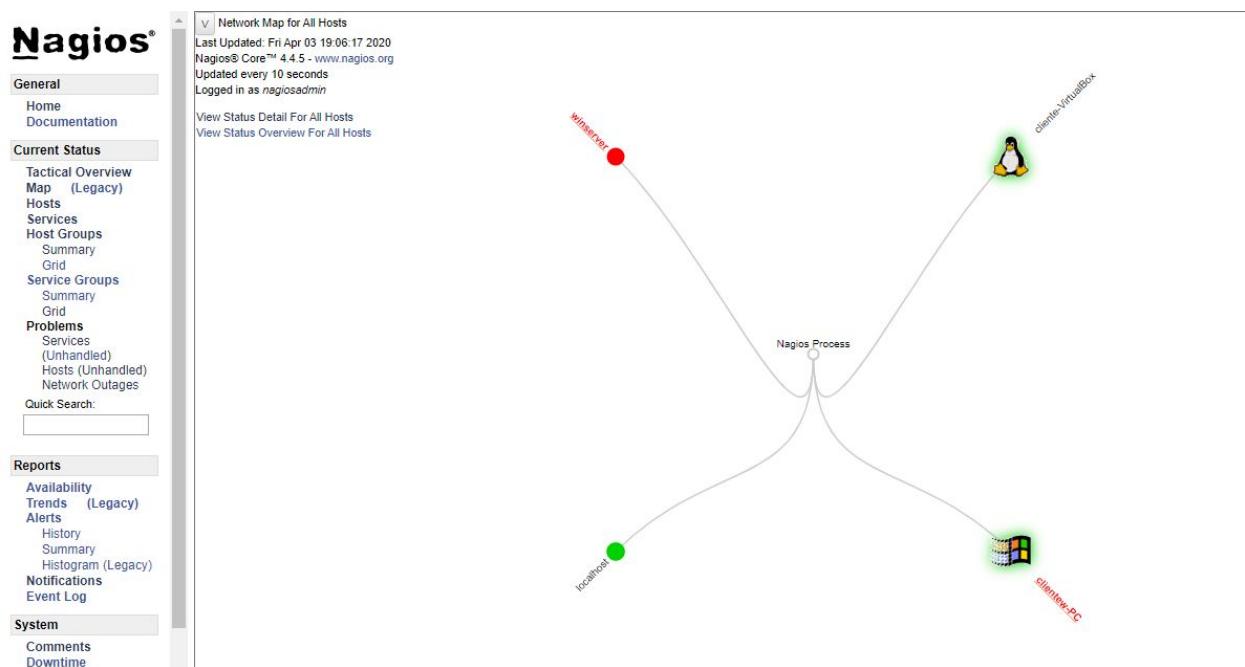
- Guardamos y reiniciamos el servicio:
 - service nagios restart

```
root@usuario:/usr/local/nagios/etc/servers# service nagios restart
root@usuario:/usr/local/nagios/etc/servers# _
```

Paso 3. Visualizar las imágenes.

Ahora en el map deberíamos encontrar el host definido cambiando lo que nos aparecía antes por la imagen de un Windows y un Linux.

Tendremos que hacer esto con cada uno de los host que tengamos si queremos que nos aparezca cualquier imagen.



Current Network Status
 Last Updated: Sat Apr 4 18:46:17 CEST 2020
 Updated every 90 seconds
 Nagios® Core™ 4.4.5 - www.nagios.org
 Logged in as nagiosadmin

[View Service Status Detail For All Host Groups](#)
[View Status Overview For All Host Groups](#)
[View Status Summary For All Host Groups](#)
[View Status Grid For All Host Groups](#)



Host Status Details For All Host Groups

Limit Results:

Host	Status	Last Check	Duration	Status Information
cliente-VirtualBox	 UP	04-04-2020 18:44:40	0d 0h 26m 37s	PING OK - Packet loss = 0%, RTA = 1.08 ms
clientew-PC	 DOWN	04-04-2020 18:45:21	0d 0h 20m 25s	CRITICAL - Host Unreachable (192.168.1.137)
localhost	 UP	04-04-2020 18:43:39	1d 7h 48m 54s	PING OK - Packet loss = 0%, RTA = 0.09 ms
winserver	 DOWN	04-04-2020 18:43:36	0d 3h 54m 7s	CRITICAL - Host Unreachable (192.168.1.2)

Capítulo 9

Instalación y configuración de PNP4Nagios.

Paso 1. Instalaciones necesarias.

- Instalamos dependencias como rrdtools y phpxml:

- `sudo apt-get install librrds-perl rrdtool`

```
root@usuario:/usr/local/nagios/etc/servers# apt-get install librrds-perl rrdtool
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  fontconfig libcairo2 libdatrie1 libgraphite2-3 libharfbuzz0b libpango-1.0-0 libpang
  libpangoft2-1.0-0 libpixman-1-0 librrd8 libthai-data libthai0 libxcb-render0 libxcb
  libxrender1
Se instalarán los siguientes paquetes NUEVOS:
  fontconfig libcairo2 libdatrie1 libgraphite2-3 libharfbuzz0b libpango-1.0-0 libpang
  libpangoft2-1.0-0 libpixman-1-0 librrd8 librrds-perl libthai-data libthai0 libxcb-r
  libxcb-shm0 libxrender1 rrdtool
0 actualizados, 17 nuevos se instalarán, 0 para eliminar y 22 no actualizados.
Se necesita descargar 2.250 KB de archivos.
Se utilizarán 6.702 KB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] _
```

- `sudo apt-get install php7.2-xml`

```
root@usuario:/usr/local/nagios/etc/servers# apt-get install php7.2-xml
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  php7.2-xml
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 22 no actualizados.
Se necesita descargar 107 KB de archivos.
Se utilizarán 455 KB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 php7.2-xml amd64
.18.04.3 [107 KB]
Descargados 107 kB en 4s (29,2 kB/s)
Seleccionando el paquete php7.2-xml previamente no seleccionado.
(Leyendo la base de datos ... 79591 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../php7.2-xml_7.2.24-0ubuntu0.18.04.3_amd64.deb ...
Desempaquetando php7.2-xml (7.2.24-0ubuntu0.18.04.3) ...
Configurando php7.2-xml (7.2.24-0ubuntu0.18.04.3) ...
Creating config file /etc/php/7.2/mods-available/dom.ini with new version
Creating config file /etc/php/7.2/mods-available/simplexml.ini with new version
-
```

- Descargamos pnp4nagios:

- cd /tmp
- sudo wget

<https://sourceforge.net/projects/pnp4nagios/files/PNP0.6/pnp4nagios-0.6.26.tar.gz>

```
root@usuario:/home/usuario# cd /tmp/
root@usuario:/tmp# wget https://sourceforge.net/projects/pnp4nagios/files/PNP-0.6/
pnp4nagios-0.6.26.tar.gz
--2020-04-04 19:06:53-- https://sourceforge.net/projects/pnp4nagios/files/PNP-0.6/
/pnp4nagios-0.6.26.tar.gz
Resolving sourceforge.net (sourceforge.net)... 216.105.38.13
Connecting to sourceforge.net (sourceforge.net)|216.105.38.13|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://sourceforge.net/projects/pnp4nagios/files/PNP-0.6/pnp4nagios-0.6
.26.tar.gz/ [following]
--2020-04-04 19:06:59-- https://sourceforge.net/projects/pnp4nagios/files/PNP-0.6
/pnp4nagios-0.6.26.tar.gz/
Reusing existing connection to sourceforge.net:443.
HTTP request sent, awaiting response... 302 Found
Location: https://sourceforge.net/projects/pnp4nagios/files/PNP-0.6/pnp4nagios-0.6
.26.tar.gz/download [following]
--2020-04-04 19:07:00-- https://sourceforge.net/projects/pnp4nagios/files/PNP-0.6
/pnp4nagios-0.6.26.tar.gz/download
Reusing existing connection to sourceforge.net:443.
HTTP request sent, awaiting response... 302 Found
```

```
HTTP request sent, awaiting response... 200 OK
Length: 3039265 (2,9M) [application/x-gzip]
Saving to: 'pnp4nagios-0.6.26.tar.gz'

pnp4nagios-0.6.26.ta 34%[=====>] 1,01M 50,1KB/s eta 39s
```

- Descomprimimos:

- sudo tar zxvf pnp4nagios-0.6.26.tar.gz
- cd pnp4nagios-0.6.26

- Instalamos:

- sudo ./configure

```
*** Configuration summary for pnp4nagios-0.6.26 08-21-2017 ***

General Options:
-----
Nagios user/group:          nagios nagios
Install directory:          /usr/local/pnp4nagios
HTML Dir:                  /usr/local/pnp4nagios/share
Config Dir:                /usr/local/pnp4nagios/etc
Location of rrdtool binary: /usr/bin/rrdtool Version 1.7.0
RRDs Perl Modules:         FOUND (Version 1.5001)
RRD Files stored in:       /usr/local/pnp4nagios/var/perfdata
process_perfdata.pl Logfile: /usr/local/pnp4nagios/var/perfdata.log
Perfdata files (NPCD) stored in: /usr/local/pnp4nagios/var/spool

Web Interface Options:
-----
HTML URL:                  http://localhost/pnp4nagios
Apache Config File:         /etc/httpd/conf.d/pnp4nagios.conf

Review the options above for accuracy. If they look okay,
type 'make all' to compile.
```

- sudo make all

```

root@usuario:/tmp/pnp4nagios-0.6.26# make all
cd ./src && make
make[1]: Entering directory '/tmp/pnp4nagios-0.6.26/src'
gcc -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o utils.o utils.c
utils.c: In function 'check_sig':
utils.c:211:14: warning: 'Caught the Signal '' directive output truncated writing
19 bytes into a region of size 8 [-Wformat-truncation=]
    "Caught the Signal '%d' but don't care about this.\n", signr);
    ^~~~~~^~~~~~
In file included from /usr/include/stdio.h:862:0,
                  from ../include/pnp.h:8,
                  from utils.c:17:
/usr/include/x86_64-linux-gnu/bits/stdio2.h:64:10: note: '__builtin_snprintf_chk
' output between 50 and 60 bytes into a destination of size 8
        return __builtin_snprintf_chk (__s, __n, __USE_FORTIFY_LEVEL - 1,
        ^~~~~~^~~~~~
        __bos (__s), __fmt, __va_arg_pack ());
        ^~~~~~^~~~~~
gcc -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o config.o config.c
gcc -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o logging.o logging.c
gcc -g -O2 -DHAVE_CONFIG_H -DNSCORE -o npcd npcd.c utils.o config.o logging.o -lpt
hread
gcc -fPIC -g -O2 -DHAVE_CONFIG_H -DNSCORE -o npcdmod.o npcdmod.c -shared -fPIC
make[1]: Leaving directory '/tmp/pnp4nagios-0.6.26/src'
cd ./share && make
make[1]: Entering directory '/tmp/pnp4nagios-0.6.26/share'
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/tmp/pnp4nagios-0.6.26/share'
cd ./scripts && make
make[1]: Entering directory '/tmp/pnp4nagios-0.6.26/scripts'
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/tmp/pnp4nagios-0.6.26/scripts'
chmod a+r ./contrib/ssi/status-header.ssi

*** Compile finished ***

make install
- This installs the main program and HTML files

make fullinstall
- This installs the main program, runlevel scripts, config and HTML files

```

- sudo make fullinstall

```

/usr/bin/perl summary fullinstall

*** Configuration summary for pnp4nagios-0.6.26 08-21-2017 ***

General Options:
-----
Nagios user/group:          nagios nagios
Install directory:          /usr/local/pnp4nagios
HTML Dir:                  /usr/local/pnp4nagios/share
Config Dir:                /usr/local/pnp4nagios/etc
Location of rrdtool binary: /usr/bin/rrdtool Version 1.7.0
RRDs Perl Modules:          FOUND (Version 1.5001)
RRD Files stored in:       /usr/local/pnp4nagios/var/perfdata
process_perfdata.pl Logfile: /usr/local/pnp4nagios/var/perfdata.log
Perfdata files (NPCD) stored in: /usr/local/pnp4nagios/var/spool

Web Interface Options:
-----
HTML URL:                  http://localhost/pnp4nagios
Apache Config File:         /etc/httpd/conf.d/pnp4nagios.conf

*** Main program, Scripts and HTML files installed ***
Enjoy.

```

Paso 2. Ficheros de configuración.

- Creamos el vínculo al fichero de configuración del sitio en apache2:

```
○ sudo ln -s /etc/httpd/conf.d/pnp4nagios.conf  
      /etc/apache2/sitesenabled/pnp4nagios.conf
```

- Eliminamos el fichero de configuración:

```
○ sudo rm -rf /usr/local/pnp4nagios/share/install.php
```

- Activamos la recopilación de datos de rendimiento en Nagios:

- Para ello tendremos que editar el fichero /usr/local/nagios/etc/nagios.cfg:

```
■ sudo nano /usr/local/nagios/etc/nagios.cfg
```

- Buscamos el “process_performance_data” y lo ponemos en 1:

```
■ process_performance_data=1
```

```

GNU nano 2.9.3          /usr/local/nagios/etc/nagios.cfg      Modified

# This determines whether or not Nagios will run any host or
# service event handlers when it is initially (re)started. Unless
# you're implementing redundant hosts, leave this option enabled.
# Values: 1 = enable event handlers, 0 = disable event handlers

enable_event_handlers=1


# PROCESS PERFORMANCE DATA OPTION
# This determines whether or not Nagios will process performance
# data returned from service and host checks. If this option is
# enabled, host performance data will be processed using the
# host_perfdata_command (defined below) and service performance
# data will be processed using the service_perfdata_command (also
# defined below). Read the HTML docs for more information on
# performance data.
# Values: 1 = process performance data, 0 = do not process performance data

process_performance_data=1


# HOST AND SERVICE PERFORMANCE DATA PROCESSING COMMANDS
# These commands are run after every host and service check is
# performed. These commands are executed only if the
# enable_performance_data option (above) is set to 1. The command
# argument is the short name of a command definition that you
# define in your host configuration file. Read the HTML docs for
# more information on performance data.

#host_perfdata_command=process-host-perfdata
#service_perfdata_command=process-service-perfdata


# HOST AND SERVICE PERFORMANCE DATA FILES
# These files are used to store host and service performance data.

^G Get Help  ^C 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  ^L Go To Line

```

- Seguidamente añadimos las líneas siguientes en el mismo fichero:
 - service_perfdata_file=/usr/local/pnp4nagios/var/service-perfdata
 - service_perfdata_file_template=DATATYPE::SERVICEPERFDATA\tTI

```

MET::$TIMET$\tHOSTNAME

::$HOSTNAME$\tSERVICEDESC::$SERVICEDESC$\tSERVICEPERF

DATA::$SERVICEPERFDATA$\tSE

RVICECHECKCOMMAND::$SERVICECHECKCOMMAND$\tHOSTS

TATE::$HOSTSTATE$\tHOSTSTA

TETYPE::$HOSTSTATETYPE$\tSERVICESTATE::$SERVICESTATE

$\tSERVICESTATETYPE::$SERVICES          TATYPE$

service_perfdata_file_mode=a

service_perfdata_file_processing_interval=15

service_perfdata_file_processing_command=process-service-perfdata-file

```

- host_perfdata_file=/usr/local/pnp4nagios/var/host-perfdata


```

host_perfdata_file_template=DATATYPE::HOSTPERFDATA\tTIMET::

$TIMET$\tHOSTNAME::$H

OSTNAME$\tHOSTPERFDATA::$HOSTPERFDATA$\tHOSTCHECK

COMMAND::$HOSTCHECKCOM

MAND$\tHOSTSTATE::$HOSTSTATE$\tHOSTSTATETYPE::$HOST

STATETYPE$


host_perfdata_file_mode=a

host_perfdata_file_processing_interval=15

host_perfdata_file_processing_command=process-host-perfdata-file

```

```

GNU nano 2.9.3          /usr/local/nagios/etc/nagios.cfg      Modified

# performance data.
# Values: 1 = process performance data, 0 = do not process performance data

process_performance_data=1


# HOST AND SERVICE PERFORMANCE DATA PROCESSING COMMANDS
# These commands are run after every host and service check is
# performed. These commands are executed only if the
# enable_performance_data option (above) is set to 1. The command
# argument is the short name of a command definition that you
# define in your host configuration file. Read the HTML docs for
# more information on performance data.

#host_perfdata_command=process-host-perfdata
#service_perfdata_command=process-service-perfdata

host_perfdata_file=/usr/local/pnp4nagios/var/host-perfdata
host_perfdata_file_template=DATATYPE::HOSTPERFDATA\tTIMET::$\tHOSTNAME::$HOSTNAME\tHOSTNAME
host_perfdata_file_mode=a
host_perfdata_file_processing_interval=15
host_perfdata_file_processing_command=process-host-perfdata-file

service_perfdata_file=/usr/local/pnp4nagios/var/service-perfdata
service_perfdata_file_template=DATATYPE::SERVICEPERFDATA\tTIMET::$\tHOSTNAME:$HOSTNAME\tHOSTNAME
service_perfdata_file_mode=a
service_perfdata_file_processing_interval=15
service_perfdata_file_processing_command=process-service-perfdata-file

# HOST AND SERVICE PERFORMANCE DATA FILES
# These files are used to store host and service performance data.
# Performance data is only written to these files if the
# enable_performance_data option (above) is set to 1.

#host_perfdata_file=/usr/local/nagios/var/host-perfdata
#service_perfdata_file=/usr/local/nagios/var/service-perfdata

^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  ^L Go To Line

```

- Ponemos el servicio npcd como automático:

- update-rc.d npcd defaults

- Añadimos en comandos los destinos de datos:

- sudo nano /usr/local/nagios/etc/objects/commands.cfg

- define command{
command_name process-service-perfdata-file
command_line /usr/local/pnp4nagios/libexec/process_perfdata.pl
-bulk=/usr/local/pnp4nagios/var/service-perfdata
}

- define command{
command_name process-host-perfdata-file
command_line /usr/local/pnp4nagios/libexec/process_perfdata.pl
-bulk=/usr/local/pnp4nagios/var/host-perfdata
}

```

GNU nano 2.9.3          /usr/local/nagios/etc/objects/commands.cfg      Modified

#####
#
# SAMPLE PERFORMANCE DATA COMMANDS
#
# These are sample performance data commands that can be used to send performance
# data output to two text files (one for hosts, another for services). If you
# plan on simply writing performance data out to a file, consider using the
# host_perfdata_file and service_perfdata_file options in the main config file.
#
#####

define command {
    command_name    process-host-perfdata
    command_line    /usr/bin/printf "%b" "$LASTHOSTCHECK\$\\t$HOSTNAME\$\\t$HOSTSTATE\$"
}

define command {
    command_name    process-service-perfdata
    command_line    /usr/bin/printf "%b" "$LASTSERVICECHECK\$\\t$HOSTNAME\$\\t$SERVIC\$"
}

define command{
    command_name    process-service-perfdata-file
    command_line    /usr/local/pnp4nagios/libexec/process_perfdata.pl --bulk=/$
}

define command{
    command_name    process-host-perfdata-file
    command_line    /usr/local/pnp4nagios/libexec/process_perfdata.pl --bulk=/$
} █

^G Get Help  ^C 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

```

- Creamos las plantillas que invocaremos desde equipos o servicios:
 - sudo nano /usr/local/nagios/etc/objects/templates.cfg
 - define host {

```
name      host-pnp  
action_url  
/pnp4nagios/index.php/graph?host=$HOSTNAME$&srv=_HOST_  
class='tips'  
rel='/pnp4nagios/index.php/popup?host=$HOSTNAME$&srv=_HOST_  
register 0  
}
```

- define service {
name srv-pnp
action_url
/pnp4nagios/index.php/graph?host=\$HOSTNAME\$&srv=\$SERVICEDE
SC\$' class='tips'
rel='/pnp4nagios/index.php/popup?host=\$HOSTNAME\$&srv=\$SERVIC
EDESC\$
register 0
}

```

GNU nano 2.9.3      /usr/local/nagios/etc/objects/templates.cfg      Modified

define service {
    name          local-service           ; The name of this se$;
    use           generic-service         ; Inherit default val$;
    max_check_attempts 4                 ; Re-check the servic$;
    check_interval   5                 ; Check the service e$;
    retry_interval   1                 ; Re-check the servic$;
    register        0                 ; DONT REGISTER THIS $;
}

# Plantillas que invocaremos desde equipos o servicios

define host {
    name      host-pnp
    action_url /pnp4nagios/index.php/graph?host=$HOSTNAME$&srv=_HOST_ class='tips$'
    register  0
}

define service {
    name      srv-pnp
    action_url /pnp4nagios/index.php/graph?host=$HOSTNAME$&rv=$SERVICEDESC$' clas$;
    register  0
}

```

Paso 3. Solucionar errores.

- Solucionamos el error “sizeof(): Parameter must be an array or an object that implements Countable”
 - Editamos el fichero data.php y vamos a la linea afectada, en este caso la [979]
 - sudo nano /usr/local/pnp4nagios/share/application/models/data.php
 - public function getFirstPage(){
 \$pages = \$this->getPages();
 if(sizeof(\$pages) > 0){
 return urldecode(\$pages[0]);
 }
 }

```

}else{
    return FALSE;
}

}

```

```

/usr/local/pnp4nagios/share/application/models/data.php

        }
    }
    closedir($dh);
} else {
    die("Cannot open directory: $path");
}
}
if(sizeof($pages)>0){
    natSort($pages);
} else{
    return FALSE;
}
return $pages;
}

/*
*/
public function getFirstPage(){
    $pages = $this->getPages();
    if(sizeof($pages) > 0 ){
        return urldecode($pages[0]);
    } else{
        return FALSE;
    }
}

/*
*/
public function getPageDetails($page){
    $this->parse_page_cfg($page);
    return $this->PAGE_DEF['page_name'];
}

/*
*/
^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  ^L Go To Line

```

- Modificaremos la linea “if(sizeof(\$pages) > 0){}” y quedará del siguiente modo

- ```

public function getFirstPage(){

 $pages = $this->getPages();

 if (is_array($pages) && sizeof($pages) > 0){

 return urldecode($pages[0]);

 }else{

 return FALSE;

 }

}

```

```

/*
 *
 */
public function getFirstPage(){
 $pages = $this->getPages();
 if(is_array($pages) && sizeof($pages) > 0){
 return urldecode($pages[0]);
 }else{
 return FALSE;
 }
/*
 *
*/

```

#### Paso 4. Graficación de hosts y servicios.

- Añadimos la graficación en los hosts o servicios:
  - Editando el archivo localhost.cfg y nuestros archivos de host, podemos añadir las plantillas que hemos definido en pasos anteriores, esto lo haremos añadiendo

host-pnp o srv-pnp en la propiedad use, dependiendo de si se trata de un servicio o un host y lo haremos con cada servicio y host que tengamos.

- Ejemplo: sudo nano /usr/local/nagios/etc/objects/localhost.cfg

■ define host{

```
use linux-server,host-pnp ; Al ser la def. del host
utilizamos el host-pnp

host_name localhost
alias localhost
address 127.0.0.1
}
```

■ define service{

```
use local-service,srv-pnp ; Al ser la def. del servicio
utilizamos el srv-pnp

host_name localhost
service_description Current Load
check_command check_local_load!5.0,4.0,3.0!10.0,6.0,4.0
}
```

```
GNU nano 2.9.3 /usr/local/nagios/etc/objects/localhost.cfg Modified

#####
LOCALHOST.CFG - SAMPLE OBJECT CONFIG FILE FOR MONITORING THIS MACHINE
#
#
NOTE: This config file is intended to serve as an *extremely* simple
example of how you can create configuration entries to monitor
the local (Linux) machine.
#
#####

#####
HOST DEFINITION
#
#####

Define a host for the local machine

define host {

 use linux-server,host-pnp; ; Name of host template
 ; This host definition will inherit
 ; in (or inherited by) the listed
 host_name localhost
 alias localhost
 address 127.0.0.1
}

#####

#
HOST GROUP DEFINITION
#
#####

^G Get Help ^C 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 ^L Go To Line
```

```
#####
#
SERVICE DEFINITIONS
#
#####

Define a service to "ping" the local machine

define service {

 use local-service,srv-pnp ; Name of service template
 host_name localhost
 service_description PING
 check_command check_ping!100.0,20%!500.0,60%
}

}
```

GNU nano 2.9.3                                                          Linux142.cfg

```
#####
#
Linux Host 001 configuration file
#
#####

define host {
 use linux-server,host-pnp
 host_name cliente-VirtualBox
 alias Linux Host 001
 address 192.168.1.144
 register 1
 icon_image linux40.gif
 statusmap_image linux40.gd2
}
define service{
 host_name cliente-VirtualBox
 service_description PING
 check_command check_ping!100.0,20%!500.0,60%
 max_check_attempts 2
 check_interval 2
 retry_interval 2
 check_period 24x7
 check_freshness 1
 contact_groups admins
 notification_interval 2
 notification_period 24x7
 notifications_enabled 1
 register 1
}
define service{
 use generic-service,srv-pnp
 host_name cliente-VirtualBox
}

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

```

GNU nano 2.9.3 Windows137.cfg

#####
Windows Host 001 configuration file
#####

define host {
 use windows-server,host-pnp
 host_name clientew-PC
 alias Windows Host 001
 address 192.168.1.137
 register 1
 icon_image win40.gif
 statusmap_image win40.gd2
}
define service{
 host_name clientew-PC
 service_description PING
 check_command check_ping!100.0,20%!500.0,60%
 max_check_attempts 2
 check_interval 2
 retry_interval 2
 check_period 24x7
 check_freshness 1
 contact_groups admins
 notification_interval 2
 notification_period 24x7
 notifications_enabled 1
 register 1
}
define service {
 use generic-service,srv-pnp
 host_name clientew-PC
}
[Read 81 lines]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M
^X Exit ^R Read File ^Y Replace ^U Uncut Text ^T To Spell ^L Go To Line M

```

- Añadimos los pop up de vista previa de los gráficos.

○ sudo cp /tmp/pnp4nagios-0.6.26/contrib/ssi/status-header.ssi

/usr/local/nagios/share/ssi/

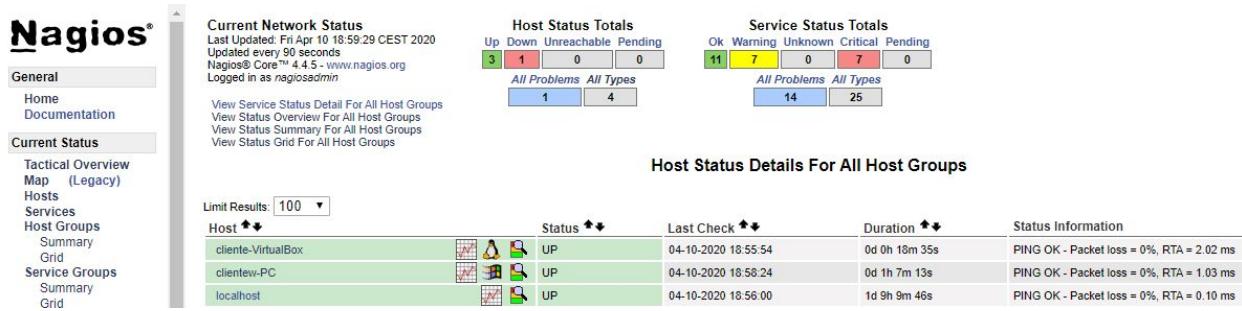
- Reiniciamos Nagios y Apache2, ya que si no lo hacemos nos aparecerá un error.

- service nagios restart
- service apache2 restart

```
root@usuario:/usr/local/pnp4nagios# service nagios restart
root@usuario:/usr/local/pnp4nagios# service apache2 restart
```

## Paso 5. Comprobación del funcionamiento.

- Comprobamos en el navegador web entrando en Nagios que nos aparece un ícono de una gráfica al lado de cada nombre:



- Si entramos en el ícono se nos mostrarán las gráficas de los distintos hosts y sus servicios:

- Localhost:

**Service details localhost -> Host Perpdata**

**Host:** localhost **Service:** Host Perpdata  
**4 Hours** 10.04.20 15:02 - 10.04.20 19:02

**Datasource: Round Trip Times**

Ping times

RTT / ms

120 m  
100 m  
80 m  
60 m  
40 m  
20 m

15:20 15:40 16:00 16:20 16:40 17:00 17:20 17:40 18:00 18:20 18:40 19:00

■ Round Trip Times 0.09 ms Last 0.12 ms Max 0.10 ms Average  
■ Warning 3000.000000ms  
■ Critical 5000.000000ms

**Datasource: Packets Lost**

Packets lost

Packets lost / ms

120  
100  
80  
60  
40  
20  
0

15:20 15:40 16:00 16:20 16:40 17:00 17:20 17:40 18:00 18:20 18:40 19:00

■ Packets Lost 0 % Last 0 % Max 0 % Average  
■ Warning 80%  
■ Critical 100%

**Search**

**Actions**

**My basket**

Basket is empty

**Status**

**Host:** localhost  
**Service:** Host Perpdata  
**Last Check:** 10.04.20 19:01

**Time ranges**

- Overview
- 4 Hours
- 25 Hours
- One Week
- One Month
- One Year

**Services**

- Host Perpdata
- Current Load
- Current Users
- HTTP
- PING
- Root Partition

**Service details localhost -> Current Load**

**Host:** localhost **Service:** Current Load  
**4 Hours** 10.04.20 15:02 - 10.04.20 19:02

**Datasource: load1**

CPU Load for localhost / Current\_Load

Load / ms

100 m  
80 m  
60 m  
40 m  
20 m  
0

15:20 15:40 16:00 16:20 16:40 17:00 17:20 17:40 18:00 18:20 18:40 19:00

■ load 15 0.03 Last 0.01 Average 0.03 Max  
■ Load 5 0.10 Last 0.03 Average 0.10 Max  
■ load 1 0.08 Last 0.02 Average 0.08 Max

**Host:** localhost **Service:** Current Load  
**25 Hours** 09.04.20 18:02 - 10.04.20 19:02

**Datasource: load1**

CPU Load for localhost / Current\_Load

Load / ms

100 m  
80 m  
60 m  
40 m  
20 m  
0

Fri 00:00 Fri 06:00 Fri 12:00 Fri 18:00

■ load 15 0.03 Last 0.01 Average 0.03 Max  
■ Load 5 0.10 Last 0.03 Average 0.10 Max  
■ load 1 0.08 Last 0.02 Average 0.08 Max

**Search**

**Actions**

**My basket**

Basket is empty

**Status**

**Host:** localhost  
**Service:** Current Load  
**Last Check:** 10.04.20 19:00

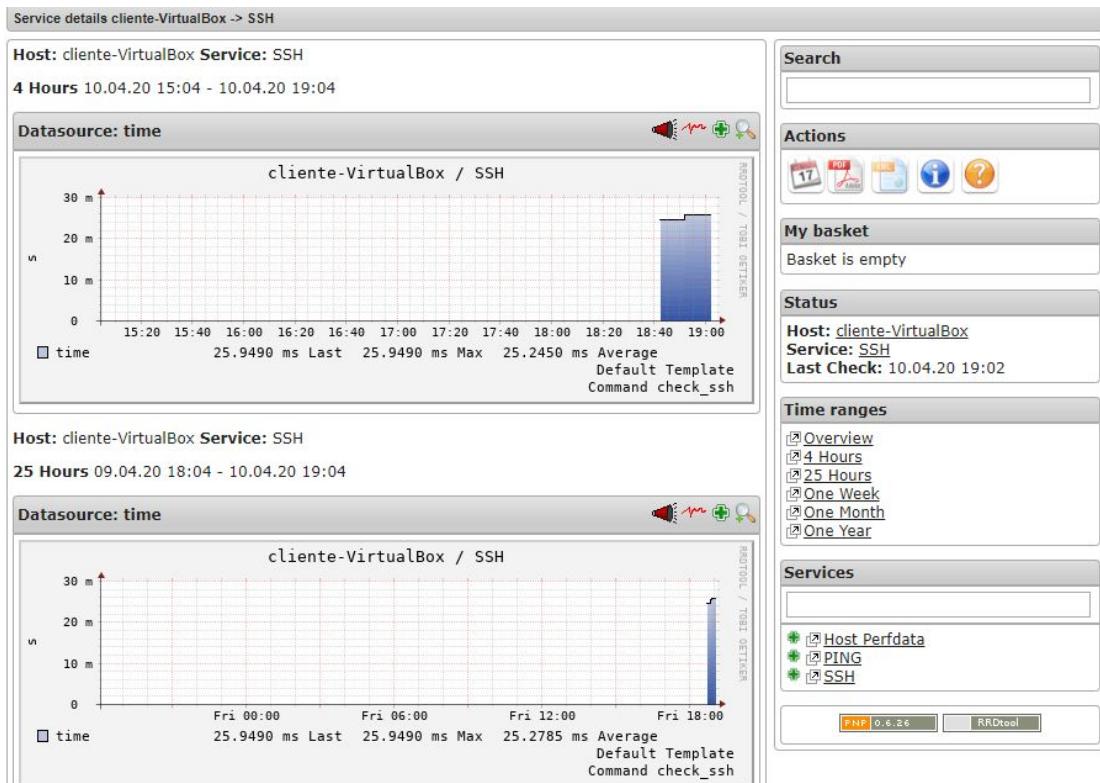
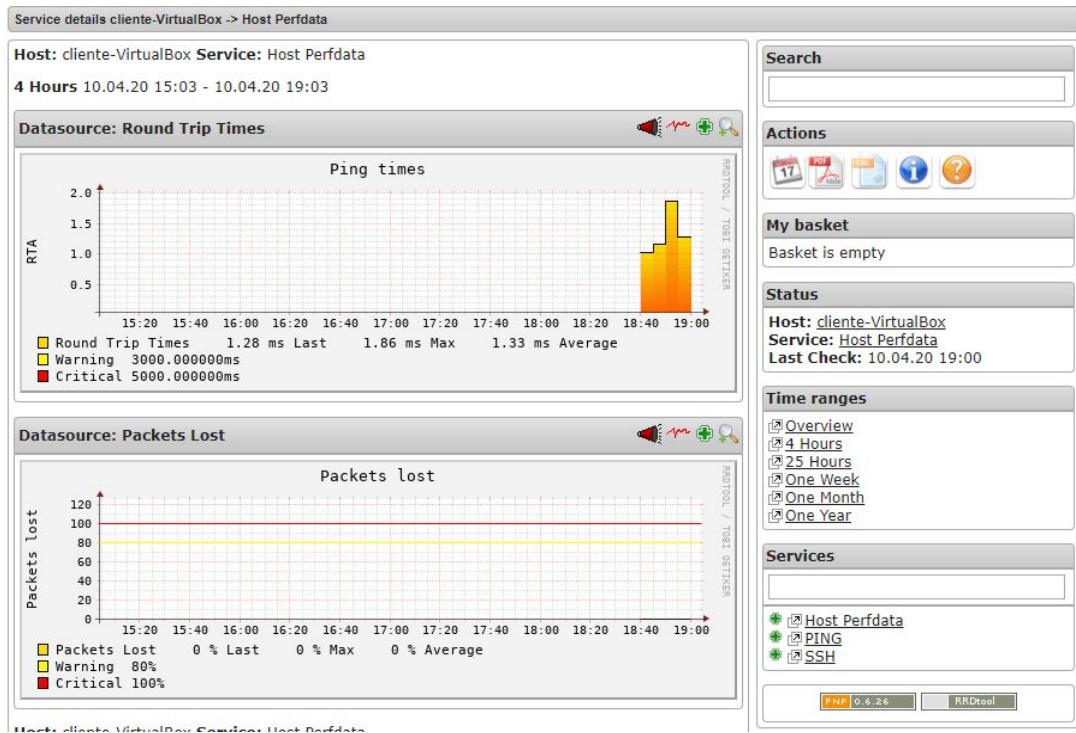
**Time ranges**

- Overview
- 4 Hours
- 25 Hours
- One Week
- One Month
- One Year

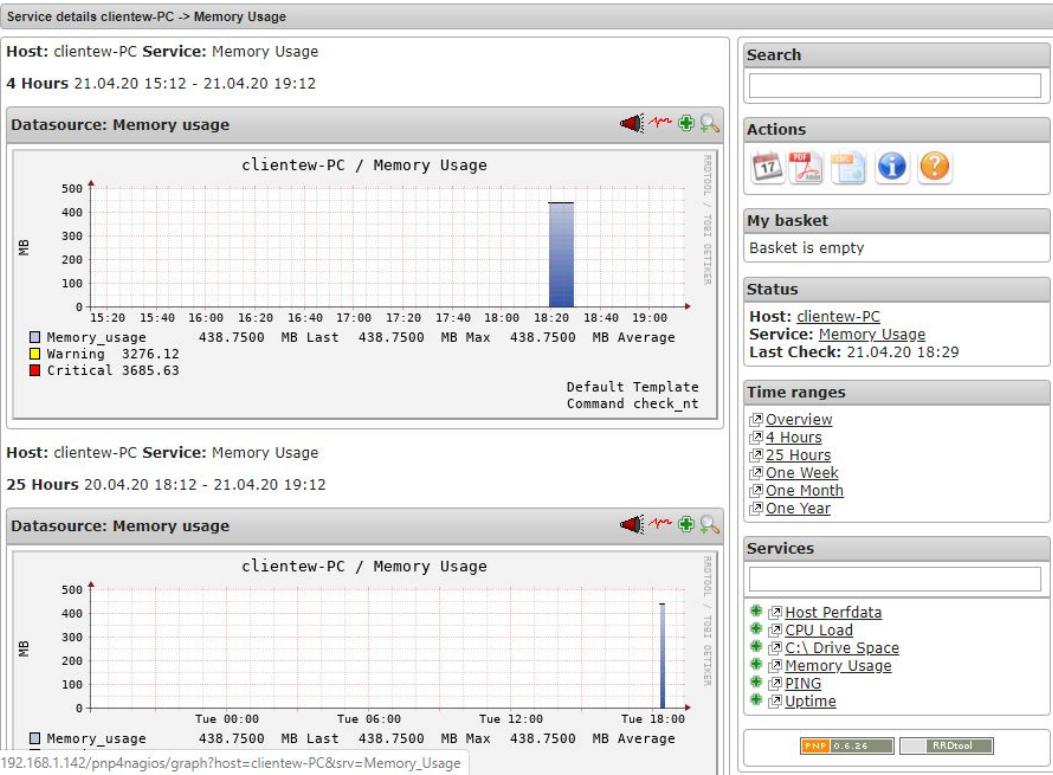
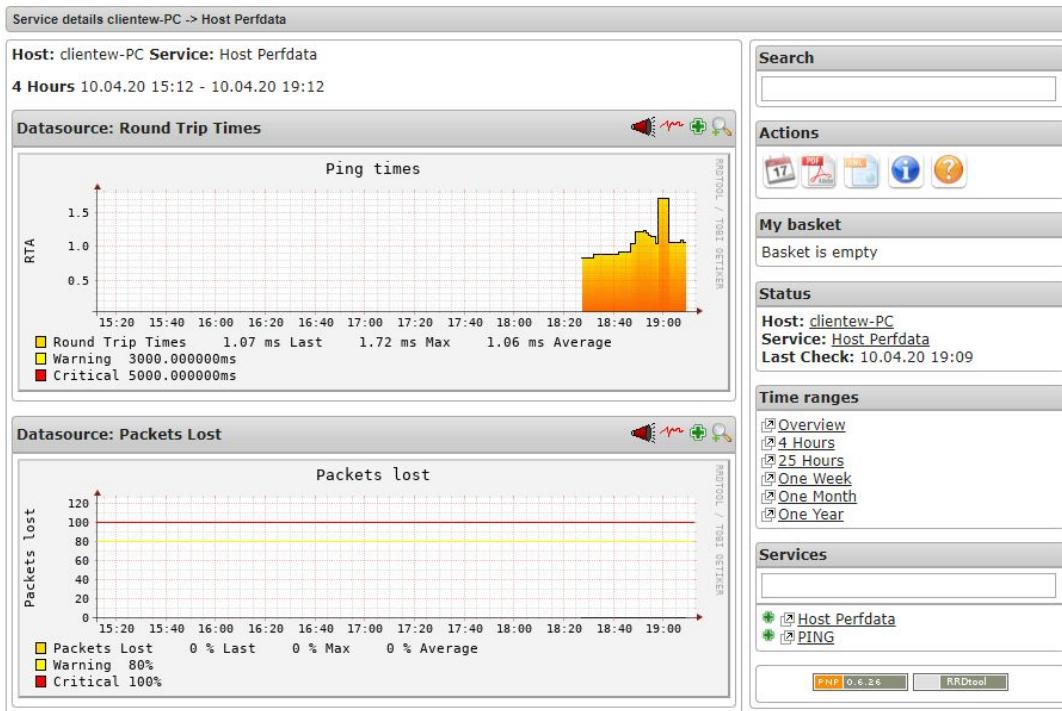
**Services**

- Host Perpdata
- Current Load
- Current Users
- HTTP
- PING
- Root Partition
- SSH
- Swap Usage
- Total Processes

- Linux:



- Windows:



## Capítulo 10

### Monitorizar MySQL

- Vamos a monitorizar MySQL con nuestro servidor Ubuntu.
- Para ello he usado una máquina de Linux, Ubuntu 14.04.
- También necesitamos bajarnos el plugin `check_mysql_health` que nos va a permitir monitorizar los siguientes servicios:
  - MySQL open files
  - MySQL up Time
  - MySQL connection-time

#### Paso 1. Instalación y configuración de la máquina.

- Instalamos la máquina y configuramos la IP fija como ya hemos hecho anteriormente con las demás máquinas.



- nano /etc/network/interfaces
- ifconfig
- ping 192.168.1.1 - para comprobar que hace ping a la puerta de enlace
- ping 8.8.8.8

The screenshot shows a terminal window titled "root@clientelinux14-VirtualBox: /home/clientelinux14". The window title bar also displays "GNU nano 2.2.6" and "Archivo: /etc/network/interfaces". The main content of the terminal is the /etc/network/interfaces configuration file:

```
interfaces(5) file used by ifup(8) and ifdown(8)
auto eth0
iface eth0 inet static
address 192.168.1.144
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

At the bottom of the terminal window, there is a status bar with the message "[ 8 líneas escritas ]". Below the status bar, there is a menu of keyboard shortcuts:

[ 8 líneas escritas ]  
^C Ver ayuda ^O Guardar ^R Leer fich.^Y Pág. ant. ^K Cortar Tex^C Posición  
^X Salir ^J Justificar^W Buscar ^V Pág. sig. ^U PegarTxt ^T Ortografía

```
root@clientelinux14-VirtualBox: /home/clientelinux14
clientelinux14@clientelinux14-VirtualBox:~$ sudo su
[sudo] password for clientelinux14:
root@clientelinux14-VirtualBox:/home/clientelinux14# ifconfig
eth0 Link encap:Ethernet direcciónHW 08:00:27:7e:ed:90
 Direc. inet:192.168.1.144 Difus.:192.168.1.255 Másc:255.255.255.0
 Dirección inet6: fe80::a00:27ff:fe7e:ed90/64 Alcance:Enlace
 ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
 Paquetes RX:79 errores:0 perdidos:0 overruns:0 frame:0
 Paquetes TX:50 errores:0 perdidos:0 overruns:0 carrier:0
 colisiones:0 long.colatX:1000
 Bytes RX:6184 (6.1 KB) TX bytes:8356 (8.3 KB)

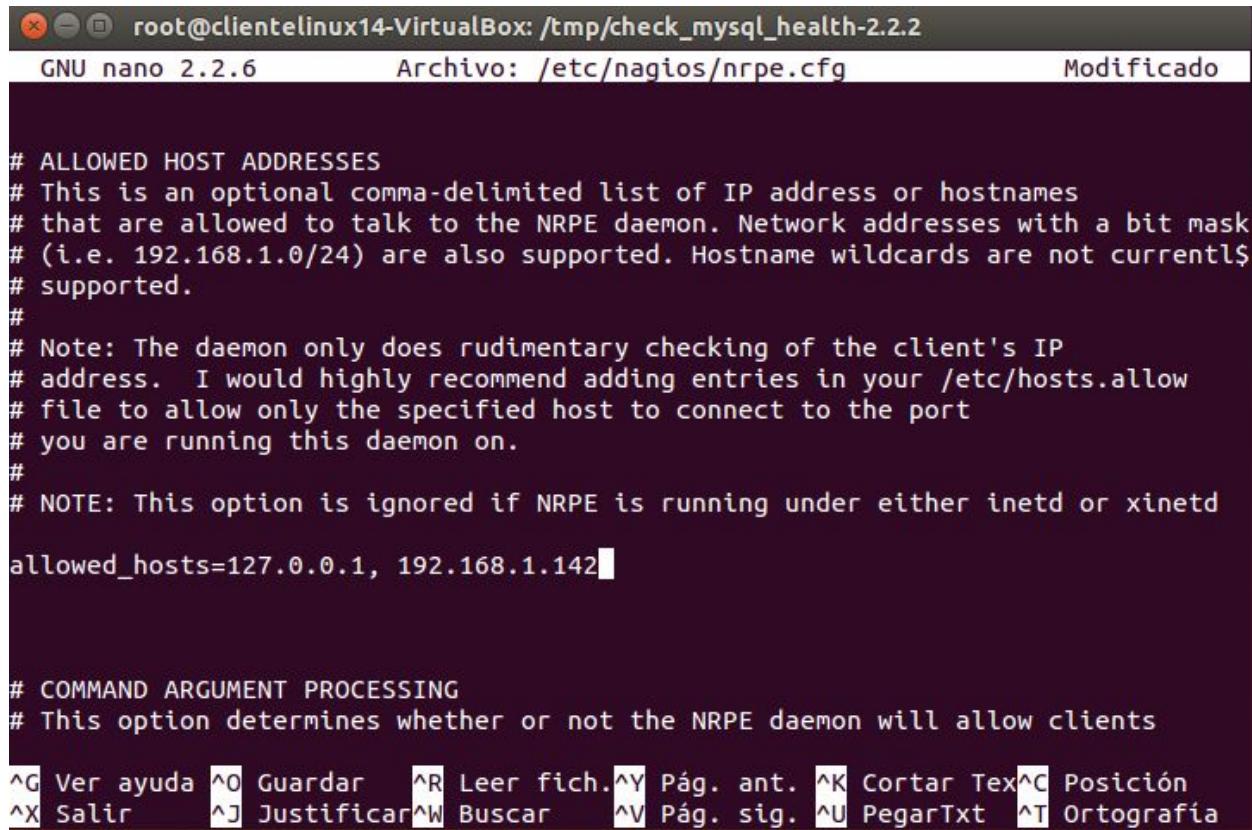
lo Link encap:Bucle local
 Direc. inet:127.0.0.1 Másc:255.0.0.0
 Dirección inet6: ::1/128 Alcance:Anfitrión
 ACTIVO BUCLE FUNCIONANDO MTU:65536 Métrica:1
 Paquetes RX:259 errores:0 perdidos:0 overruns:0 frame:0
 Paquetes TX:259 errores:0 perdidos:0 overruns:0 carrier:0
 colisiones:0 long.colatX:1
 Bytes RX:19617 (19.6 KB) TX bytes:19617 (19.6 KB)
```

```
root@clientelinux14-VirtualBox:/home/clientelinux14# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=12.2 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=7.78 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 7.781/10.012/12.243/2.231 ms
root@clientelinux14-VirtualBox:/home/clientelinux14# ping google.com
ping: unknown host google.com
root@clientelinux14-VirtualBox:/home/clientelinux14# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=23.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=24.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=56 time=24.7 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 23.578/24.418/24.897/0.609 ms
```

- Descargamos e instalamos el servicio nrpe necesario en las máquinas Linux, que debemos monitorear a través del servidor Nagios.

```
root@clientelinux14-VirtualBox:/tmp/check_mysql_health-2.2.2# apt-get install nagios-nrpe-server nagios-plugins
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
 libdbi1 libgssglue1 libnet-snmp-perl libpq5 libtirpc1 nagios-plugins-basic
 nagios-plugins-common nagios-plugins-standard rpcbind snmp whois
Paquetes sugeridos:
 libcrypt-des-perl nagios3 icinga nagios-plugins-contrib postfix sendmail-bin
 exim4-daemon-heavy exim4-daemon-light
Se instalarán los siguientes paquetes NUEVOS:
 libdbi1 libgssglue1 libnet-snmp-perl libpq5 libtirpc1 nagios-nrpe-server
 nagios-plugins nagios-plugins-basic nagios-plugins-common
 nagios-plugins-standard rpcbind snmp whois
0 actualizados, 13 se instalarán, 0 para eliminar y 61 no actualizados.
Necesito descargar 952 kB de archivos.
Se utilizarán 4.910 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

- Después de instalar el servicio NRPE, editamos el archivo de configuración nrpe /etc/nagios/nrpe.cfg y agregamos nuestra ip de servicio nagios en los hosts permitidos.
  - nano /etc/nagios/nrpe.cfg
    - allowed\_hosts = 127.0.0.1, 192.168.1.142
    - Donde 192.168.1.142 es la dirección IP de mi servidor Nagios.



```

root@clientelinux14-VirtualBox: /tmp/check_mysql_health-2.2.2
GNU nano 2.2.6 Archivo: /etc/nagios/nrpe.cfg Modificado

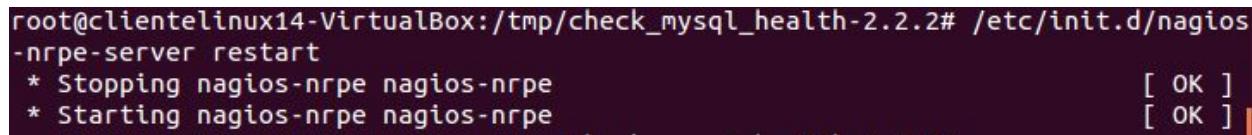
ALLOWED HOST ADDRESSES
This is an optional comma-delimited list of IP address or hostnames
that are allowed to talk to the NRPE daemon. Network addresses with a bit mask
(i.e. 192.168.1.0/24) are also supported. Hostname wildcards are not currently
supported.
#
Note: The daemon only does rudimentary checking of the client's IP
address. I would highly recommend adding entries in your /etc/hosts.allow
file to allow only the specified host to connect to the port
you are running this daemon on.
#
NOTE: This option is ignored if NRPE is running under either inetd or xinetd
allowed_hosts=127.0.0.1, 192.168.1.142

COMMAND ARGUMENT PROCESSING
This option determines whether or not the NRPE daemon will allow clients

^G Ver ayuda ^O Guardar ^R Leer fich.^Y Pág. ant. ^K Cortar Tex^C Posición
^X Salir ^J Justificar^W Buscar ^V Pág. sig. ^U PegarTxt ^T Ortografía

```

- Después de realizar los cambios anteriores en el archivo de configuración, reiniciamos el servicio NRPE.
  - sudo /etc/init.d/nagios-nrpe-server restart



```

root@clientelinux14-VirtualBox:/tmp/check_mysql_health-2.2.2# /etc/init.d/nagios
-nrpe-server restart
* Stopping nagios-nrpe nagios-nrpe [OK]
* Starting nagios-nrpe nagios-nrpe [OK]

```

- Ahora creamos el fichero para monitorear nuestra nueva máquina.
  - nano /usr/local/nagios/etc/servers/Linux144.cfg
  - Agregamos en el fichero:

```
#####
Linux Host 002 configuration file
```

```
#####
```

```
define host {
 use linux-server
 host_name clientlinux14-VirtualBox
 alias Linux Host 002
 address 192.168.1.144
 register 1
}

define service{
```

```
 host_name clientlinux14-VirtualBox
 service_description PING
 check_command check_ping!100.0,20%!500.0,60%
 max_check_attempts 2
 check_interval 2
 retry_interval 2
 check_period 24x7
 check_freshness 1
 contact_groups admins
 notification_interval 2
 notification_period 24x7
 notifications_enabled 1
 register 1
```

```
}
```

```
#####
END OF FILE
#####

```

```
#####
END OF FILE
#####

```

```
GNU nano 2.9.3 /usr/local/nagios/etc/servers/Linux144.cfg

#####
Linux Host 002 configuration file
#####

define host {
 use linux-server
 host_name clientelinux14-VirtualBox
 alias Linux Host 002
 address 192.168.1.144
 register 1
}
define service{
 host_name clientelinux14-VirtualBox
 service_description PING
 check_command check_ping!100.0,20%!500.0,60%
 max_check_attempts 2
 check_interval 2
 retry_interval 2
 check_period 24x7
 check_freshness 1
 contact_groups admins
 notification_interval 2
 notification_period 24x7
 notifications_enabled 1
 register 1
}

#####
END OF FILE
#####

[Read 32 lines]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^Y Replace ^U Uncut Text ^I To Spell ^L Go To Line M-E Redo
```

- Ahora reiniciamos el servicio nagios:

- service nagios restart

```
root@usuario:/usr/local/nagios/etc/servers# service nagios restart
root@usuario:/usr/local/nagios/etc/servers#
```

- Por último abrimos nuestra interfaz web de Nagios y comprobamos si nuestro nuevo host de Linux se ha agregado en el servicio central de Nagios. En mi caso, se ve a continuación.

**Host Information**

Last Updated: Wed Apr 22 17:49:09 CEST 2020  
Updated every 90 seconds  
Nagios® Core™ 4.4.5 - www.nagios.org  
Logged in as nagiosadmin

**Host**  
**Linux Host 002**  
(clientelinux14-VirtualBox)

**Member of**  
**No hostgroups**

192.168.1.144

**Host State Information**

|                                     |                                                                |
|-------------------------------------|----------------------------------------------------------------|
| <b>Host Status:</b>                 | <b>UP</b> (for 0d 0h 36m 26s)                                  |
| <b>Status Information:</b>          | PING OK - Packet loss = 0%, RTA = 0.94 ms                      |
| <b>Performance Data:</b>            | rta=0.945000ms;3000.000000;5000.000000;0.000000 pl=0%;80;100;0 |
| <b>Current Attempt:</b>             | 1/10 (HARD state)                                              |
| <b>Last Check Time:</b>             | 04-22-2020 17:46:30                                            |
| <b>Check Type:</b>                  | ACTIVE                                                         |
| <b>Check Latency / Duration:</b>    | 0.000 / 4,000 seconds                                          |
| <b>Next Scheduled Active Check:</b> | 04-22-2020 17:51:30                                            |
| <b>Last State Change:</b>           | 04-22-2020 17:12:43                                            |
| <b>Last Notification:</b>           | N/A (notification 0)                                           |
| <b>Is This Host Flapping?</b>       | <b>NO</b> (0.00% state change)                                 |
| <b>In Scheduled Downtime?</b>       | <b>NO</b>                                                      |
| <b>Last Update:</b>                 | 04-22-2020 17:49:08 ( 0d 0h 0m 1s ago)                         |

|                        |                |
|------------------------|----------------|
| <b>Active Checks:</b>  | <b>ENABLED</b> |
| <b>Passive Checks:</b> | <b>ENABLED</b> |
| <b>Obsessing:</b>      | <b>ENABLED</b> |
| <b>Notifications:</b>  | <b>ENABLED</b> |
| <b>Event Handler:</b>  | <b>ENABLED</b> |
| <b>Flap Detection:</b> | <b>ENABLED</b> |

**Host Comments**  
○ Add a new comment ━ Delete all comments

**Host Actions**

- Locate host or service
- Disable active checks
- Re-schedule check
- Submit passive check
- Stop accepting notifications
- Stop obsessing over this host
- Disable notifications
- Send custom notifications
- Schedule downtime
- Schedule recovery
- Disable notifications
- Enable notifications
- Schedule a check
- Disable check
- Enable check
- Disable event
- Disable flap detection
- Clear flapping

**Current Network Status**

Last Updated: Sat Apr 25 16:34:52 CEST 2020  
Updated every 90 seconds  
Nagios® Core™ 4.4.5 - www.nagios.org  
Logged in as nagiosadmin

**Host Status Totals**

|    |      |             |         |
|----|------|-------------|---------|
| Up | Down | Unreachable | Pending |
| 4  | 2    | 0           | 0       |

All Problems All Types

|   |   |
|---|---|
| 2 | 6 |
|---|---|

**Service Status Totals**

|    |         |         |          |         |
|----|---------|---------|----------|---------|
| Ok | Warning | Unknown | Critical | Pending |
| 21 | 0       | 0       | 23       | 0       |

All Problems All Types

|    |    |
|----|----|
| 23 | 44 |
|----|----|

**Host Status Details For All Host Groups**

| Limit Results: 100 ▾ | Host ↗                    | Status ↗ | Last Check ↗        | Duration ↗     | Status Information                        |
|----------------------|---------------------------|----------|---------------------|----------------|-------------------------------------------|
|                      | cliente-VirtualBox        | UP       | 04-25-2020 16:31:10 | 0d 11h 51m 38s | PING OK - Packet loss = 0%, RTA = 0.08 ms |
|                      | clientelinux14-VirtualBox | UP       | 04-25-2020 16:33:58 | 0d 0h 0m 54s   | PING OK - Packet loss = 0%, RTA = 0.49 ms |

## Paso 2. Descargar plugin necesario.

- Necesitamos descargar el plugin de check\_mysql\_health necesario para la monitorización de MySql ya que nagios no trae por defecto este paquete.

- cd /tmp
- wget

[https://labs.consol.de/assets/downloads/nagios/check\\_mysql\\_health-2.2.2.tar.gz](https://labs.consol.de/assets/downloads/nagios/check_mysql_health-2.2.2.tar.gz)

```
root@usuario:/home/usuario# cd /tmp/
root@usuario:/tmp# wget https://labs.consol.de/assets/downloads/nagios/check_mysql_health-2.2.2.tar.gz
--2020-04-22 18:03:28-- https://labs.consol.de/assets/downloads/nagios/check_mysql_health-2.2.2.tar.gz
Resolving labs.consol.de (labs.consol.de)... 94.185.89.33, 2a03:3680:0:2::21
Connecting to labs.consol.de (labs.consol.de)|94.185.89.33|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 140250 (137K) [application/octet-stream]
Saving to: 'check_mysql_health-2.2.2.tar.gz'

check_mysql_health-2.2.2. 100%[=====] 136,96K 567KB/s in 0,2s

2020-04-22 18:03:30 (567 KB/s) - 'check_mysql_health-2.2.2.tar.gz' saved [140250/140250]
```

### Paso 3. Instalar el plugin.

- Vamos a proceder a instalar el plugin de nagios MySQL.
  - tar -zxvf check\_mysql\_health-2.2.2.tar.gz
  - cd check\_mysql\_health-2.2.2/

```
check_mysql_health-2.2.2/plugins-scripts/Nagios/DBD/MySQL/Server/Instance/
check_mysql_health-2.2.2/plugins-scripts/Nagios/DBD/MySQL/Server/Instance/Innodb.pm
check_mysql_health-2.2.2/plugins-scripts/Nagios/DBD/MySQL/Server/Instance/Myisam.pm
check_mysql_health-2.2.2/plugins-scripts/Nagios/DBD/MySQL/Server/Instance/Replication.pm
check_mysql_health-2.2.2/plugins-scripts/Nagios/DBD/MySQL/Server/Instance.pm
check_mysql_health-2.2.2/plugins-scripts/Nagios/DBD/MySQL/Server.pm
check_mysql_health-2.2.2/plugins-scripts/Nagios/Extraopts.pm
check_mysql_health-2.2.2/plugins-scripts/subst.in
check_mysql_health-2.2.2/README
check_mysql_health-2.2.2/t/
check_mysql_health-2.2.2/t/check_mysql_health.t
check_mysql_health-2.2.2/t/Makefile.am
check_mysql_health-2.2.2/t/Makefile.in
check_mysql_health-2.2.2/TODO
root@usuario:/tmp# cd check_mysql_health-2.2.2/
root@usuario:/tmp/check_mysql_health-2.2.2#
```

- ./configure --prefix=/usr/local/nagios --with-nagios-user=nagios  
--with-nagios-group=nagios --with-perl=/usr/bin/perl

```

checking how to create a pax tar archive... gnutar
checking whether to enable maintainer-specific portions of Makefiles... no
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
variable with_statefiles_dir is /var/tmp/check_mysql_health
variable with_mymodules_dir is /usr/local/nagios/libexec
variable with_mymodules_dyn_dir is /usr/local/nagios/libexec
checking whether make sets $(MAKE)... (cached) yes
checking for echo... /bin/echo
checking for sed... /bin/sed
checking for grep... /bin/grep
checking for cat... /bin/cat
checking for sh... /bin/sh
checking for perl... /usr/bin/perl
checking for gzip... /bin/gzip
checking for gawk... /usr/bin/gawk
checking that generated files are newer than configure... done
configure: creating ./config.status
config.status: creating Makefile
config.status: creating plugins-scripts/Makefile
config.status: creating plugins-scripts/subst
config.status: creating t/Makefile
 --with-perl: /usr/bin/perl
 --with-statefiles-dir: /var/tmp/check_mysql_health
 --with-nagios-user: nagios
 --with-nagios-group: nagios
 --with-mymodules-dir: /usr/local/nagios/libexec
 --with-mymodules-dyn-dir: /usr/local/nagios/libexec

```

- make
- make install
- Aquí tenemos el plugin de MySQL instalado.

```

root@usuario:/usr/local/nagios/libexec# ls
check_apt check_file_age check_load check_ntp_peer check_simap check_users
check_breeze check_flexlm check_log check_ntp_time check_smtp check_wave
check_by_ssh check_ftp check_mailq check_nwstat check_spop eventhandlers
check_clamd check_http check_mrtg check_oracle check_ssh negate
check_cluster check_icmp check_mrtgtraf check_overcr check_ssmtp urlize
check_dhcp check_ide_smart check_mysql_health check_ping check_swap utils.pm
check_dig check_ifoperstatus check_nagios check_pop check_tcp utils.sh
check_disk check_ifstatus check_nntp check_procs check_time
check_disk_smb check_imap check_nttsp check_real check_udp
check_dns check_ircd check_nt check_rpc check_ups
check_dummy check_jabber

```

#### Paso 4. Configurar permisos de MySQL.

- Procedemos a crear y darle los permisos necesarios a nuestro usuario en la máquina cliente.

- mysql -u root -p

```
root@clientelinux14-VirtualBox:/tmp/check_mysql_health-2.2.2# mysql -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 42
Server version: 5.5.62-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

- mysql> CREATE USER 'all'@'%' IDENTIFIED BY 'all';

```
mysql> CREATE USER 'all'@'%' IDENTIFIED BY 'all';
Query OK, 0 rows affected (0.06 sec)
```

- En mi caso he creado dos usuarios, pero no es necesario.

```
mysql> CREATE USER 'usuario'@'%' IDENTIFIED BY 'usuario';
Query OK, 0 rows affected (0.00 sec)

mysql> quit;
Bye
```

- Para que no nos de ningún tipo de error instalaremos también el MySQL server:

```
root@clientelinux14-VirtualBox:/tmp/check_mysql_health-2.2.2# apt-get install mysql-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
 libaio1 libdbd-mysql-perl libdbi-perl libhtml-template-perl libmysqlclient18
 libterm-readkey-perl mysql-client-5.5 mysql-common mysql-server-5.5
 mysql-server-core-5.5
Paquetes sugeridos:
 libldb-perl libnet-daemon-perl libplrpc-perl libsql-statement-perl
 libipc-sharedcache-perl tinyca mailx
Se instalarán los siguientes paquetes NUEVOS:
 libaio1 libdbd-mysql-perl libdbi-perl libhtml-template-perl libmysqlclient18
 libterm-readkey-perl mysql-client-5.5 mysql-common mysql-server
 mysql-server-5.5 mysql-server-core-5.5
0 actualizados, 11 se instalarán, 0 para eliminar y 61 no actualizados.
Necesito descargar 8.879 kB de archivos.
Se utilizarán 90,2 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

## Paso 5. Configurar archivos de Nagios.

- Lo primero que tenemos que hacer es editar el fichero nagios.cfg
  - nano /usr/local/nagios/etc/nagios.cfg
  - Una vez dentro del fichero agregamos la siguiente línea:
    - cfg\_file=/usr/local/nagios/etc/objects/mysqlmonitor.cfg
  - En mi caso yo tengo creado el fichero /usr/local/nagios/etc/servers/Linux144.cfg , por lo que no me es necesario agregar la línea anterior.
- Ahora editamos el fichero commands.cfg y para entrar usamos la siguiente sentencia:
  - nano /usr/local/nagios/etc/objects/commands.cfg
  - Agregamos al final esta línea:
    - define command{
  - command\_name check\_mysql\_health

```
command_line $USER1$/check_mysql_health -H $ARG1$ -port
$ARG2$ -username $ARG3$ -password $ARG4$ -mode $ARG5$

}
```

```
GNU nano 2.9.3 /usr/local/nagios/etc/objects/commands.cfg

command_line $USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -s usuario -v $ARG1$ $ARG2$
}

define command {
command_name check_nrpe
command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$ -t 25
}

define command{
command_name check_mysql_health
command_line $USER1$/check_mysql_health -H $ARG1$ -port $ARG2$ -username $ARG3$ -password $ARG4$ -$}
#####
#
SAMPLE PERFORMANCE DATA COMMANDS
#
These are sample performance data commands that can be used to send performance
data output to two text files (one for hosts, another for services). If you
plan on simply writing performance data out to a file, consider using the
host_perfdata_file and service_perfdata_file options in the main config file.
#
#####

define command {

 command_name process-host-perfdata
 command_line /usr/bin/printf "%b" "$LASTHOSTCHECK$\t$HOSTNAME$\t$HOSTSTATE$\t$HOSTATTEMPT$\t$"
}

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^P Replace ^U Uncut Text ^T To Spell ^L Go To Line M-E Redo
```

- Ahora tenemos que editar el fichero con el siguiente comando:

- nano /usr/local/nagios/etc/servers/Linux144.cfg

- Agregamos las siguientes líneas:

- define service{

- use generic-service

- host\_name localhost

```
service_description MySQL connection-time
check_command
check_mysql_health!localhost!3306!all!all!connection-time!
}

■ define service{
use generic-service
host_name localhost
service_description MySQL Open Files
check_command check_mysql_health!localhost!3306!all!all!open-files!
}

■ define service{
use generic-service
host_name localhost
service_description MySQL UP Time
check_command check_mysql_health!localhost!3306!all!all!uptime!
}
```

```
GNU nano 2.9.3 /usr/local/nagios/etc/servers/Linux144.cfg

check_interval 2
retry_interval 2
check_period 24x7
check_freshness 1
contact_groups admins
notification_interval 2
notification_period 24x7
notifications_enabled 1
register 1
}

define service{
use generic-service
host_name clientelinux14-VirtualBox
service_description MySQL connection-time
check_command check_mysql_health!clientelinux14-VirtualBox!5666!usuario!usuario!connection-time!
}

define service{
use generic-service
host_name clientelinux14-VirtualBox
service_description MySQL Open Files
check_command check_mysql_health!clientelinux14-VirtualBox!5666!usuario!usuario!open-files!
}

define service{
use generic-service
host_name clientelinux14-VirtualBox
service_description MySQL UP Time
check_command check_mysql_health!clientelinux14-VirtualBox!5666!usuario!usuario!uptime!
}

-
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^Y Replace ^U Uncut Text ^T To Spell ^L Go To Line M-E Redo
```

- Una vez realizado todos los cambios deberemos reiniciar el servicio de nagios:

- /etc/init.d/nagios restart

```
root@usuario:/usr/local/nagios/etc/servers# service nagios restart
root@usuario:/usr/local/nagios/etc/servers#
```

- Si vamos ahora al navegador y entramos en nagios deberíamos ver esto:

**Nagios®**

**General**

- [Home](#)
- [Documentation](#)

**Current Status**

- [Tactical Overview](#)
- [Map \(Legacy\)](#)
- [Hosts](#)
- [Services](#)
- [Host Groups](#)
- [Summary](#)
- [Grid](#)
- [Service Groups](#)
- [Summary](#)
- [Grid](#)
- [Problems](#)
- [Services \(Unhandled\)](#)

**Current Network Status**

Last Updated: Wed Apr 22 20:23:33 CEST 2020  
Updated every 90 seconds  
Nagios® Core™ 4.4.5 - www.nagios.org  
Logged in as nagiosadmin

[View History For This Host](#)  
[View Notifications For This Host](#)  
[View Service Status Detail For All Hosts](#)

**Host Status Totals**

|             |   |
|-------------|---|
| Up          | 1 |
| Down        | 0 |
| Unreachable | 0 |
| Pending     | 0 |

[All Problems](#) [All Types](#)

|   |   |
|---|---|
| 0 | 1 |
|---|---|

**Service Status Totals**

|          |   |
|----------|---|
| Ok       | 4 |
| Warning  | 0 |
| Unknown  | 0 |
| Critical | 0 |
| Pending  | 0 |

[All Problems](#) [All Types](#)

|   |   |
|---|---|
| 0 | 4 |
|---|---|

**Service Status Details For Host 'clientelinux14-VirtualBox'**

| Host ↕                    | Service ↕             | Status ↕ | Last Check ↕        | Duration ↕    | Attempt ↕ |
|---------------------------|-----------------------|----------|---------------------|---------------|-----------|
| clientelinux14-VirtualBox | MySQL Open Files      | OK       | 04-22-2020 20:18:10 | 0d 0h 6m 32s+ | 1/3       |
|                           | MySQL UP Time         | OK       | 04-22-2020 20:19:20 | 0d 0h 6m 32s+ | 1/3       |
|                           | MySQL connection-time | OK       | 04-22-2020 20:22:28 | 0d 0h 1m 5s   | 1/3       |
|                           | PING                  | OK       | 04-22-2020 20:22:51 | 0d 0h 8m 46s  | 1/2       |

Results 1 - 4 of 4 Matching Services

- Con esto acabamos con la instalación del nagios mysql plugin.

## Capítulo 11

### Crear y añadir mi propio plugin

- En mi caso he creado un plugin de Twitter a partir de un script que nos indica los followers y los tweets del usuario que indiquemos.

#### Paso 1. Creación de los comandos.

- Primero creamos los comandos que vayamos a añadir al script.
  - Para acceder a la web un simple CURL (con un -s para que sea silencioso).
  - Buscamos la línea que contenga la cadena ‘data-nav=>»followers»‘ que es donde están nuestro seguidores.
  - Con un segundo grep escogemos solo los números.
  - En casos de más de 999 twitter nos devuelve el número de seguidores en dos cadenas. Las juntamos con TR.
  - Finalmente eliminamos espacios en blanco.
  - Aquí tenemos la cadena y el resultado:

■ curl -s https://twitter.com/(nombre-usuario) | grep 'data-nav="followers"' |  
grep -E -o "[0-9]{1,9}" | tr '\n' '' | sed "s/ //g"

```
root@usuario:/home/usuario# curl -s https://twitter.com/AngelaGmez | grep 'data-nav="followers"' | grep -E -o "[0-9]{1,9}" | tr '\n' '' | sed "s/ //g"
```

- Ahora si cambiamos los “followers” por “tweets” obtendremos el número de tweets subidos en la cuenta.

- Aquí está el resultado:

■ curl -s https://twitter.com/(nombre-usuario) | grep 'data-nav="tweets"' |  
grep -E -o "[0-9]{1,9}" | tr '\n' '' | sed "s/ //g"

```
root@usuario:/home/usuario# o# curl -s https://twitter.com/AngelaaGmez grep 'dat
a-nav="tweets"' | grep -E -o "[0-9]{1,9}" | tr '\n' '' | sed "s/ //g"
31999810429896500979193722231912319222319114044041741141465872059551995267root@u
```

## Paso 2. Creación y ejecución del script.

- Ahora metemos todo esto en un script:

- nano check\_twitter.sh

■ #!/bin/bash

```
followers=`curl -s https://twitter.com/$1 | grep 'data-nav="followers"' |
grep -E -o "[0-9]{1,9}" | tr '\n' '' | sed "s/ //g")`

tweets=`curl -s https://twitter.com/$1 | grep 'data-nav="tweets"' | grep -E
-o "[0-9]{1,9}" | tr '\n' '' | sed "s/ //g")`

echo "OK: Cuenta @$1 tiene $tweets tweets y $followers followers |

tweets=$tweets followers=$followers"

exit 0
```

- Tenemos que \$1 va a ser el valor (nombre de la cuenta), y que “exit 0” indica a Nagios que el resultado del plugin es siempre OK.

```

GNU nano 2.9.3 check_twitter.sh

#!/bin/bash
followers=$(curl -s https://twitter.com/$1 | grep 'data-nav="followers"' | grep -E -o "[0-9]{1,9}" | tr '\n' ' ' | sed "s/ //g")
tweets=$(curl -s https://twitter.com/$1 | grep 'data-nav="tweets"' | grep -E -o "[0-9]{1,9}" | tr '\n' ' ' | sed "s/ //g")
echo "OK: Cuenta @$1 tiene $tweets tweets y $followers followers | tweets=$tweets followers=$followers"
exit 0

```

^G Get Help ^C Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text  
 ^X Exit ^R Read File ^V Replace ^U Uncut Text ^I To Linter ^S Go To Line M-E Redo M-C Copy Text

- Le damos los permisos necesarios y ejecutamos el script para comprobar que funciona:

- chmod 777 check\_twitter.sh
- ./check\_twitter.sh (user)

■ Nos saldrá una respuesta así (para el usuario AngelaaGmez):

- OK: Cuenta @AngelaaGmez tiene 33368 tweets y 859 followers |  
tweets=33368 followers=859

```

root@usuario:/home/usuario# chmod 777 check_twitter.sh
root@usuario:/home/usuario# ./check_twitter.sh AngelaaGmez
OK: Cuenta @AngelaaGmez tiene 33368 tweets y 859 followers | tweets=33368 followers=859

```

- Probamos con otros users:

- # ./check\_twitter.sh marta\_garfuen
  - OK: Cuenta @marta\_garfuen tiene 2633 tweets y 429 followers |  
tweets=2633 followers=429

- # ./check\_twitter.sh AnaCama78067438
  - OK: Cuenta @AnaCama78067438 tiene 2782 tweets y 53 followers | tweets=2782 followers=53

```
root@usuario:/home/usuario# nano check_twitter.sh
root@usuario:/home/usuario# ./check_twitter.sh marta_garfuen
OK: Cuenta @marta_garfuen tiene 2633 tweets y 429 followers | tweets=2633 followers=429
root@usuario:/home/usuario# ./check_twitter.sh AnaCama78067438
OK: Cuenta @AnaCama78067438 tiene 2782 tweets y 53 followers | tweets=2782 followers=53
root@usuario:/home/usuario# ./check_twitter.sh AngelaaGmez
OK: Cuenta @AngelaaGmez tiene 33368 tweets y 859 followers | tweets=33368 followers=859
```

- Es un script muy sencillo y meramente informativo que solo nos devuelve los seguidores y tweets de una cuenta, y que no tiene más opciones configurables.

### Paso 3. Agregar servicio de Nagios.

- Ahora procederemos a agregar esto como un servicio de Nagios para poder monitorizarlo.
  - Este procedimiento se puede resumir en 3 pasos:
    - Definir ubicación del script a utilizar. Generalmente /usr/lib/nagios/plugins/
    - Añadir el comando que va a utilizar Nagios para llevar a cabo la monitorización. Modificar el fichero .cfg correspondiente. Generalmente /etc/nagios-plugins/config/<fichero>.cfg
    - Definir el servicio en el equipo que se va a monitorizar.
- La estructura que debe tener el nuevo comando es la siguiente:

- define command{

command\_name <nombre\_comando>

command\_line [intérprete] <Ruta completa del script a utilizar>

}

- <nombre\_comando>: Con este nombre se debe llamar a la hora de definir el servicio.
- <Ruta completa del script a utilizar>: Es la ruta del apartado anterior, donde hemos creado el script, en mi caso /home/usuario/check\_twitter.sh.
- [intérprete]: Es opcional, algunas veces hay que especificar explícitamente el intérprete de comandos para ejecutar el script.

```
GNU nano 2.9.3 /usr/local/nagios/etc/objects/commands.cfg

define command {
 command_name check_local_users
 command_line $USER1$/check_users -w 4 -c 5
}

define command {
 command_name check_local_swap
 command_line $USER1$/check_swap -w 40% -c 15%
}

define command {
 command_name check_local_mrtgtraf
 command_line $USER1$/check_mrtgtraf -F $ARG1$ -a $ARG2$ -w $ARG3$ -c $ARG4$ -e $ARG5$
}

define command{
 command_name check_twitter
 command_line /home/usuario/check_twitter.sh
}

#####
NOTE: The following 'check_...' commands are used to monitor services on
both local and remote hosts.

[Wrote 277 lines]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^ Go To Line M-E Redo
```

- Ahora vamos a definir el servicio en el equipo que se va a monitorizar.
  - En cada equipo se debe especificar el servicio que va a ejecutar. Dependiendo del tipo de equipo el fichero .cfg varía.

- La estructura correspondiente es:

- define service{
 

```
use servicio
host_name <nombre_del_host>
service_description <Descripción>
check_command <nombre_comando>!<argumentos_opcionales>
}
}
```

- Check\_command debe coincidir con el nombre del comando del apartado anterior, en mi caso el nombre del comando sería check\_twitter. Podemos incluir parámetros de ejecución separados por un simbolo ! dependiendo de la sintaxis.

```
GNU nano 2.9.3 /usr/local/nagios/etc/servers/Windows139.cfg

define service{
 use generic-service
 host_name clientew2-PC
 service_description Explorer
 check_command check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe
}

Plugin de twitter
define service{
 use generic-service
 host_name clientew2-PC
 service_description TWITTER
 check_command check_twitter
}

#####
END OF FILE
#####
```

**GNU nano 2.9.3**

**/usr/local/nagios/etc/servers/Windows139.cfg**

define service{  
 use generic-service  
 host\_name clientew2-PC  
 service\_description Explorer  
 check\_command check\_nt!PROCSTATE!-d SHOWALL -l Explorer.exe  
}  
}  
  
**# Plugin de twitter**  
define service{  
 use generic-service  
 host\_name clientew2-PC  
 service\_description TWITTER  
 check\_command check\_twitter  
}  
  
#####  
**# END OF FILE**  
#####

^G Get Help ^C Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo  
^X Exit ^R Read File ^V Replace ^U Uncut Text ^I To Spell ^ ^ Go To Line M-E Redo

## Paso 4. Comprobación del funcionamiento.

- Entramos en el navegador y escribimos nuestra IP/Nagios, comprobamos que en el equipo en el que hemos añadido nuestro plugin se está monitoreando y está funcionando correctamente.
  - Esta imagen es del primer día que instalamos el plugin.

The screenshot shows the Nagios web interface at the URL [192.168.1.142/nagios/](http://192.168.1.142/nagios/). The left sidebar has sections for General, Home, Documentation, and Current Status. The Current Status section is expanded, showing links for Tactical Overview, Map (Legacy), Hosts, Services, Host Groups, Service Groups, Problems, and a link to Twitter. The main content area displays the 'Current Network Status' with last updated information and a log entry. It also shows 'Host Status Totals' and 'Service Status Totals'. Below this is a table titled 'Service Status Details For Host 'clientew2-PC''. The table lists services with their status, last check time, duration, attempts, and status information. For example, 'C:\ Drive Space' is OK with a duration of 0d 1h 17m 15s and 1 attempt. The 'Status Information' column contains detailed system usage statistics.

| Host         | Service            | Status | Last Check          | Duration      | Attempt | Status Information                                                                |
|--------------|--------------------|--------|---------------------|---------------|---------|-----------------------------------------------------------------------------------|
| clientew2-PC | C:\ Drive Space    | OK     | 04-27-2020 21:05:35 | 0d 1h 17m 15s | 1/3     | c: - total: 930,28 Gb - used: 396,68 Gb (43%) - free 533,60 Gb (57%)              |
|              | CPU Load           | OK     | 04-27-2020 21:06:50 | 0d 1h 16m 1s  | 1/3     | CPU Load 6% (5 min average)                                                       |
|              | Explorer           | OK     | 04-27-2020 21:10:28 | 0d 1h 12m 22s | 1/3     | explorer.exe: Running                                                             |
|              | Memory Usage       | OK     | 04-27-2020 21:07:15 | 0d 1h 15m 35s | 1/3     | Memory usage: total:15092,00 MB - used: 7667,54 MB (51%) - free: 7424,47 MB (49%) |
|              | NSClient++ Version | OK     | 04-27-2020 21:03:48 | 0d 1h 19m 2s  | 1/3     | NSClient++ 0.4.1.73 2012-12-17                                                    |
|              | PING               | OK     | 04-27-2020 21:12:28 | 0d 1h 18m 26s | 1/2     | PING OK - Packet loss = 0%, RTA = 0.96 ms                                         |
|              | TWITTER            | OK     | 04-27-2020 21:12:13 | 0d 0h 2m 38s  | 1/3     | OK: Cuenta @AngelaGmez tiene 33368 tweets y 859 followers                         |
|              | Uptime             | OK     | 04-27-2020 21:11:41 | 0d 1h 11m 9s  | 1/3     | System Uptime - 12 day(s) 5 hour(s) 6 minute(s)                                   |

- Esta imagen es del segundo día, se ve la diferencia en el número de tweets escritos.

The screenshot shows the Nagios web interface at the URL [192.168.1.142/nagios/](http://192.168.1.142/nagios/). The left sidebar is identical to the previous screenshot. The main content area displays the 'Current Network Status' with last updated information and a log entry. It also shows 'Host Status Totals' and 'Service Status Totals'. Below this is a table titled 'Service Status Details For Host 'clientew2-PC''. The table lists services with their status, last check time, duration, attempts, and status information. For example, 'C:\ Drive Space' is OK with a duration of 0d 0h 15m 21s and 1 attempt. The 'Status Information' column contains detailed system usage statistics, showing a slight change from the first screenshot.

| Host         | Service            | Status | Last Check          | Duration      | Attempt | Status Information                                                                |
|--------------|--------------------|--------|---------------------|---------------|---------|-----------------------------------------------------------------------------------|
| clientew2-PC | C:\ Drive Space    | OK     | 04-28-2020 19:24:47 | 0d 0h 15m 21s | 1/3     | c: - total: 930,28 Gb - used: 396,71 Gb (43%) - free 533,57 Gb (57%)              |
|              | CPU Load           | OK     | 04-28-2020 19:26:04 | 0d 0h 14m 4s  | 1/3     | CPU Load 23% (5 min average)                                                      |
|              | Explorer           | OK     | 04-28-2020 19:23:49 | 0d 0h 16m 19s | 1/3     | explorer.exe: Running                                                             |
|              | Memory Usage       | OK     | 04-28-2020 19:29:06 | 0d 0h 11m 2s  | 1/3     | Memory usage: total:15092,00 MB - used: 8044,12 MB (53%) - free: 7047,88 MB (47%) |
|              | NSClient++ Version | OK     | 04-28-2020 19:20:23 | 0d 0h 9m 45s  | 1/3     | NSClient++ 0.4.1.73 2012-12-17                                                    |
|              | PING               | OK     | 04-28-2020 19:28:59 | 0d 0h 17m 13s | 1/2     | PING OK - Packet loss = 0%, RTA = 0.72 ms                                         |
|              | TWITTER            | OK     | 04-28-2020 19:20:08 | 0d 22h 2m 37s | 1/3     | OK: Cuenta @AngelaGmez tiene 33378 tweets y 859 followers                         |
|              | Uptime             | OK     | 04-28-2020 19:28:50 | 0d 0h 11m 18s | 1/3     | System Uptime - 13 day(s) 3 hour(s) 23 minute(s)                                  |

## Capítulo 12

### Monitorizar impresora

#### Paso 1. Requisitos previos.

- Antes de poder monitorear debemos instalar los paquetes necesarios de snmp. Los paquetes están disponibles en repositorios predeterminados.
  - apt update

```
root@usuario:/usr/local/nagios/etc/objects# apt-get update
Obj:1 http://es.archive.ubuntu.com/ubuntu bionic InRelease
Des:2 http://es.archive.ubuntu.com/ubuntu bionic-updates InRelease [88,7 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu bionic-backports InRelease [74,6 kB]
Des:4 http://es.archive.ubuntu.com/ubuntu bionic-security InRelease [88,7 kB]
Des:5 http://es.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [915 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [1.065 kB]
Des:7 http://es.archive.ubuntu.com/ubuntu bionic-security/main amd64 Packages [692 kB]
Des:8 http://es.archive.ubuntu.com/ubuntu bionic-security/universe amd64 Packages [657 kB]
Descargados 3.582 kB en 4s (962 kB/s)
Leyendo lista de paquetes... Hecho
```

- apt install snmpd snmp libsnmp-dev

```
root@usuario:/usr/local/nagios/etc/objects# apt install snmpd snmp libsnmp-dev
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
snmp ya está en su versión más reciente (5.7.3+dfsg-1.8ubuntu3.3).
fijado snmp como instalado manualmente.
Se instalarán los siguientes paquetes adicionales:
 libpci-dev libsensors4-dev libudev-dev libudev1 libwrap0-dev udev
Paquetes sugeridos:
 snmptrapd
Se instalarán los siguientes paquetes NUEVOS:
 libpci-dev libsensors4-dev libsnmp-dev libudev-dev libwrap0-dev snmpd
Se actualizarán los siguientes paquetes:
 libudev1 udev
2 actualizados, 6 nuevos se instalarán, 0 para eliminar y 28 no actualizados.
Se necesita descargar 2.429 kB de archivos.
Se utilizarán 10,0 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] _
```

- Una vez que se realiza la instalación, procedemos a configurar.

- El archivo de configuración predeterminado es /etc/snmp/snmpd.conf.
- El archivo está muy comentado y sólo haremos algunos cambios.
- Haremos una copia del archivo original antes de continuar.
  - cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak

```
root@usuario:/usr/local/nagios/etc/objects# cp /etc/snmp/snmp.conf /etc/snmp/snmp.conf.bak
root@usuario:/usr/local/nagios/etc/objects# -
```

- Ahora tenemos que reconfigurar los plugins instalados al principio para que nos aparezca check\_hpjd, que es el que nos permitirá monitorear el estado de la impresora.
  - cd /opt/nagios-plugins-2.2.1
  - sudo ./configure --with-nagios-user=nagios --with-nagios-group=nagios --with-openssl
  - sudo make
  - sudo make install
- Usamos los comandos de Nagios para verificar el archivo de instalación y configuración de Nagios.
  - /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

```
Last Modified: 2019-08-20
License: GPL

Website: https://www.nagios.org
Reading configuration data...
 Read main config file okay...
Warning: Duplicate definition found for service 'PING' on host 'cliente-VirtualBox' (config file '/usr/local/nagios/etc/servers/Linux142.cfg', starting on line 14)
 Read object config files okay...

Running pre-flight check on configuration data...

Checking objects...
 Checked 46 services.
 Checked 7 hosts.
 Checked 3 host groups.
 Checked 0 service groups.
 Checked 1 contacts.
 Checked 1 contact groups.
 Checked 28 commands.
 Checked 5 time periods.
 Checked 0 host escalations.
 Checked 0 service escalations.
Checking for circular paths...
 Checked 7 hosts
 Checked 0 service dependencies
 Checked 0 host dependencies
 Checked 5 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors: 0

Things look okay - No serious problems were detected during the pre-flight check
```

- Despues de verificar con éxito, iniciamos el servicio central de Nagios:
  - service nagios start
  - service nagios status

```

root@usuario:/opt/nagios-plugins-2.2.1# service nagios start
root@usuario:/opt/nagios-plugins-2.2.1# service nagios status
● nagios.service - Nagios Core 4.4.5
 Loaded: loaded (/lib/systemd/system/nagios.service; enabled; vendor preset: enabled)
 Active: active (running) since Mon 2020-04-27 19:19:06 CEST; 24min ago
 Docs: https://www.nagios.org/documentation
 Main PID: 3179 (nagios)
 Tasks: 8 (limit: 2318)
 CGroup: /system.slice/nagios.service
 ├─3179 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
 ├─3180 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
 ├─3181 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
 ├─3182 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
 ├─3183 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
 └─3184 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

abr 27 19:43:29 usuario nagios[3179]: wproc: host=clientew-PC; service=PING; contact=nagiosadmin
abr 27 19:43:29 usuario nagios[3179]: wproc: early_timeout=0; exited_ok=1; wait_status=32512; erro
abr 27 19:43:29 usuario nagios[3179]: wproc: stderr line 01: /bin/sh: 1: /bin/mail: not found
abr 27 19:43:29 usuario nagios[3179]: wproc: stderr line 02: /usr/bin/printf: write error: Broken
abr 27 19:43:31 usuario nagios[3179]: SERVICE NOTIFICATION: nagiosadmin;winserver;CPU Load;CRITICAL;
abr 27 19:43:31 usuario nagios[3179]: wproc: NOTIFY job 56 from worker Core Worker 3180 is a non-che
abr 27 19:43:31 usuario nagios[3179]: wproc: host=winserver; service=CPU Load; contact=nagiosadmin
abr 27 19:43:31 usuario nagios[3179]: wproc: early_timeout=0; exited_ok=1; wait_status=32512; erro
abr 27 19:43:31 usuario nagios[3179]: wproc: stderr line 01: /bin/sh: 1: /bin/mail: not found
abr 27 19:43:31 usuario nagios[3179]: wproc: stderr line 02: /usr/bin/printf: write error: Broken
lines 1-26/26 (END)

```

- También configuramos Nagios para que se inicie automáticamente en el arranque del sistema:
  - `sudo systemctl enable nagios`
- Aquí tenemos todos los plugins.

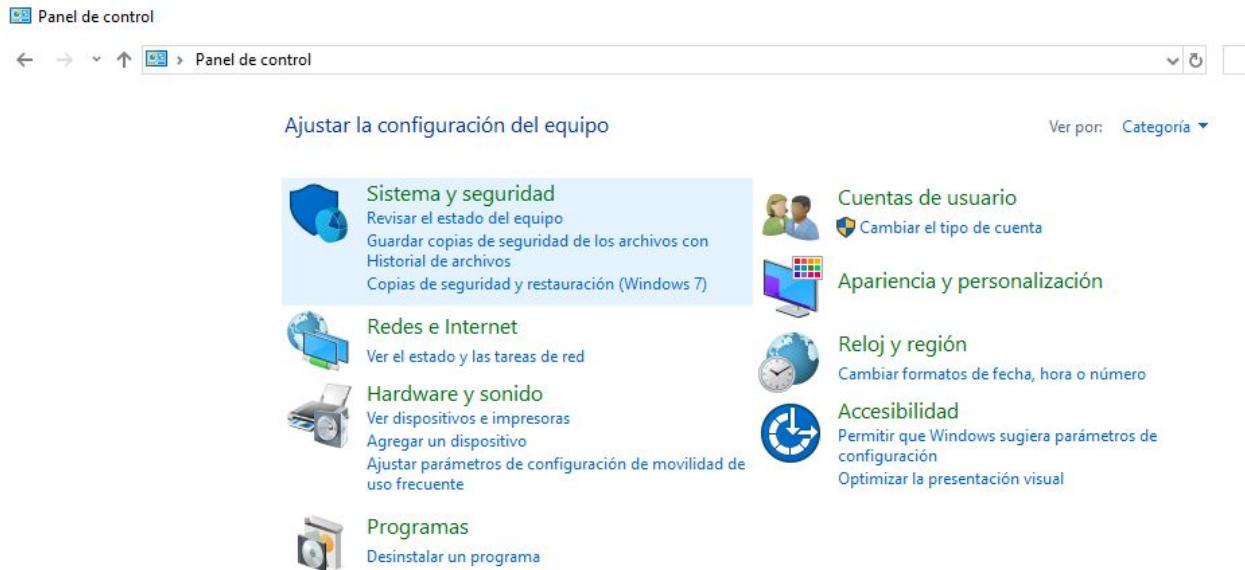
```

root@usuario:/usr/local/nagios/etc/servers# ls /usr/local/nagios/libexec/
check_apt check_hpjd check_mysql check_pop check_udp
check_breeze check_http check_mysql_health check_procs check_ups
check_by_ssh check_icmp check_mysql_query check_real check_uptime
check_clamd check_ide_smart check_nagios check_ntp check_users
check_cluster check_ifoperstatus check_nttp check_ntp_peer check_sensors
check_dhcp check_ifstatus check_nttp check_ntp_time check_wave
check_dig check_imap check_nt check_ntp check_sensors
check_disk check_ircd check_ntp check_ntp_time check_wave
check_disk_smb check_jabber check_nttp check_ntp_time check_sensors
check_dns check_load check_nt check_ntp check_ntp_time
check_dummy check_log check_ntp check_ntp_time check_ntp_time
check_file_age check_mailq check_ntstat check_ntp_time check_ntp_time
check_flexim check_mrtg check_ntp check_ntp_time check_ntp_time
check_ftp check_mrtgtraf check_ntstat check_ntp_time check_ntp_time
root@usuario:/usr/local/nagios/etc/servers#

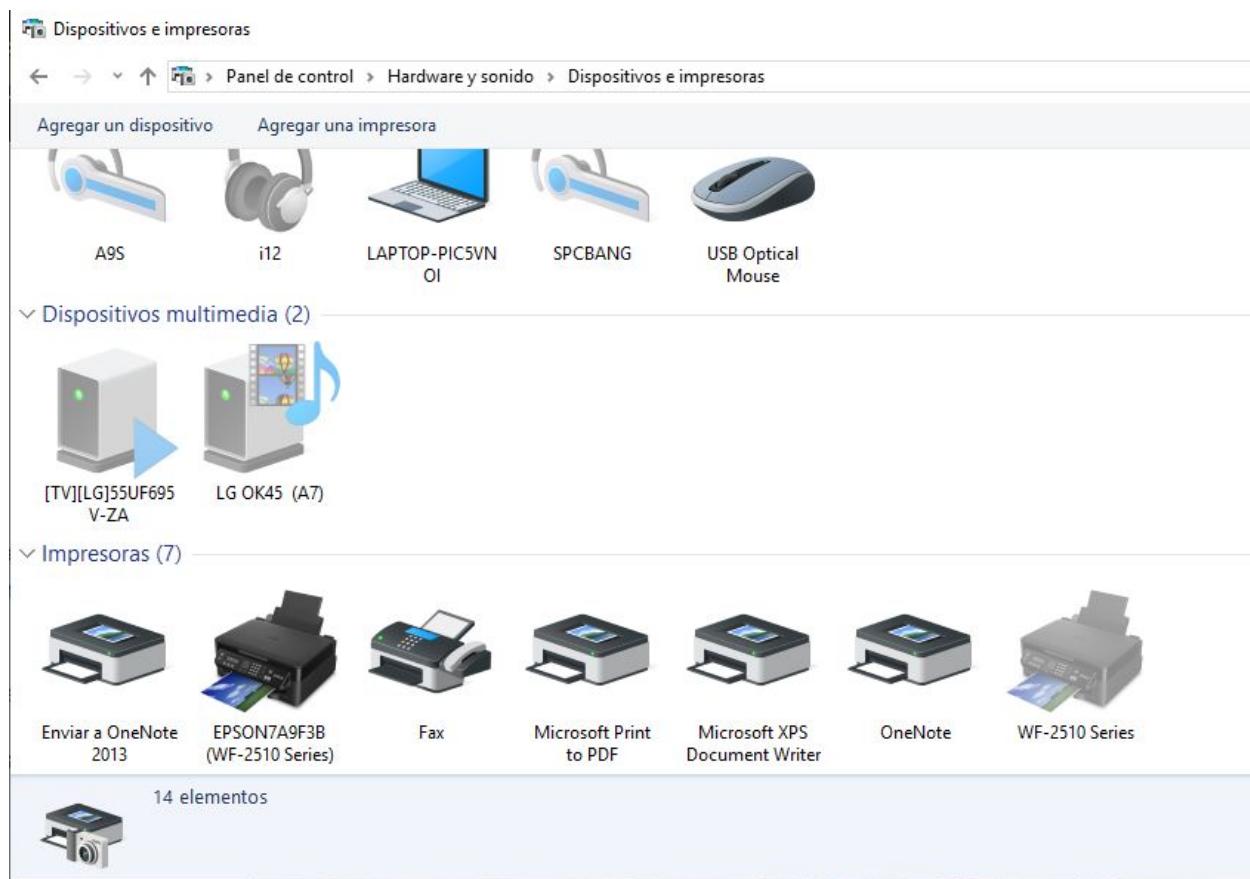
```

## Paso 2. Comprobar IP de la impresora a monitorizar.

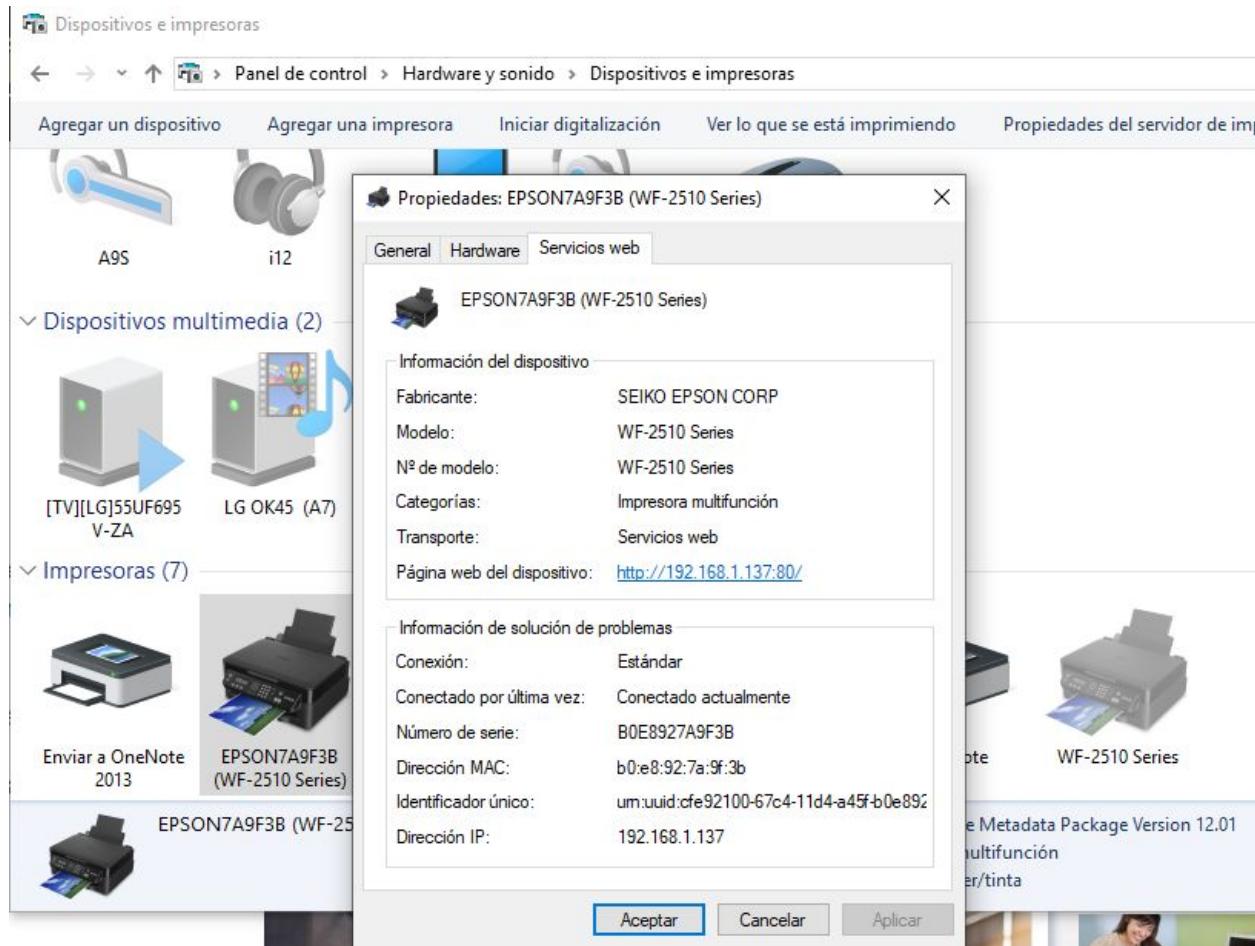
- Entramos en el panel de control de nuestro equipo.



- Nos vamos a ver dispositivos e impresoras.
- Hacemos click con el ratón derecho en la impresora que tengamos conectada y vayamos a monitorizar y entramos en propiedades.



- Por últimos entramos en servicios web y aquí tendremos los datos de nuestra impresora incluida su dirección IP, que necesitaremos más adelante.



### Paso 3. Configuración del servidor.

- El plugin check\_hpjd nos permite monitorear el estado de impresoras que tienen SNMP habilitado. El plugin es capaz de detectar los siguientes estados de la impresora:
  - Papel atascado
  - Sin Papel
  - Impresora fuera de línea
  - Intervención Requerida
  - Toner Bajo

- Memoria Insuficiente
- Puerta Abierta
- Bandeja de salida está llena
- etc.
- Comenzamos editando el archivo de configuración principal de Nagios.
  - nano /usr/local/nagios/etc/nagios.cfg
  - Borramos el asterisco (#) de la siguiente línea del archivo de configuración principal:
    - #cfg\_file=/usr/local/nagios/etc/objects/printer.cfg
  - Guardamos el archivo y salimos.

```

GNU nano 2.9.3 /usr/local/nagios/etc/nagios.cfg Modified

log_file=/usr/local/nagios/var/nagios.log

OBJECT CONFIGURATION FILE(S)
These are the object configuration files in which you define hosts,
host groups, contacts, contact groups, services, etc.
You can split your object definitions across several config files
if you wish (as shown below), or keep them all in a single config file.

You can specify individual object config files as shown below:
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg

Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

Definitions for monitoring a Windows machine
cfg_file=/usr/local/nagios/etc/objects/windows.cfg

Definitions for monitoring a router/switch
cfg_file=/usr/local/nagios/etc/objects/switch.cfg

Definitions for monitoring a network printer
cfg_file=/usr/local/nagios/etc/objects/printer.cfg

You can also tell Nagios to process all config files (with a .cfg
extension) in a particular directory by using the cfg_dir

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^Y Replace ^U Uncut Text ^I To Spell ^L Go To Line M-E Redo

```

- Ahora editamos el archivo printer.cfg.
  - nano /usr/local/nagios/etc/objects/printer.cfg
- Agregamos una nueva definición de equipo para la impresora de red que vamos a monitorear.
  - Podemos simplemente modificar la definición de equipo de ejemplo que nos aparece en el archivo.
  - Cambiamos los campos host\_name, alias, y address a los valores apropiados para la impresora.

```
■ define host{
 use generic-printer ; Inherit default values from a template
 host_name nombre ; The name we're giving to this printer
 alias nombre ; A longer name associated with the printer
 address 192.168.1.137 ; IP address of the printer
 hostgroups allhosts ; Host groups this printer is associated with
}
}
```

```
GNU nano 2.9.3 /usr/local/nagios/etc/objects/printer.cfg

#####
PRINTER.CFG - SAMPLE CONFIG FILE FOR MONITORING A NETWORK PRINTER
#
#
NOTES: This config file assumes that you are using the sample configuration
files that get installed with the Nagios quickstart guide.
#
#####

#####
#
HOST DEFINITIONS
#
#####

Define a host for the printer we'll be monitoring
Change the host_name, alias, and address to fit your situation

define host {
 use generic-printer ; Inherit default values from a template
 host_name EPSON7A9F3B ; The name we're giving to this printer
 alias IMPRESORA EPSON ; A longer name associated with the printer
 address 192.168.1.139 ; IP address of the printer
 hostgroups network-printers ; Host groups this printer is associated with
}

#####

[Read 82 lines]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^X Replace ^U Uncut Text ^T To Spell ^_ Go To Line M-B Redo
```

- A continuación agregamos algunas definiciones de servicio (al mismo archivo de configuración) para monitorear diferentes aspectos de la impresora.

- Agregamos la siguiente definición de servicio para revisar el estatus de la impresora. El servicio utiliza el plugin check\_hpjd para revisar el estatus de la impresora cada 10 minutos por default. La cadena de la comunidad SNMP utilizada para realizar la petición a la impresora es "public" en este ejemplo.

```
■ define service{
 use generic-service
```

```

host_name nombre
service_description Printer Status
check_command check_hpjd!-C public
normal_check_interval 10
retry_check_interval 1
}

```

```

GNU nano 2.9.3 /usr/local/nagios/etc/objects/printer.cfg

#
HOST GROUP DEFINITIONS
#
#####
A hostgroup for network printers
define hostgroup {
 hostgroup_name network-printers ; The name of the hostgroup
 alias Network Printers ; Long name of the group
}

#####
SERVICE DEFINITIONS
#
#####

Create a service for monitoring the status of the printer
Change the host_name to match the name of the host you defined above
If the printer has an SNMP community string other than "public",
change the check_command directive to reflect that

define service {
 use generic-service ; Inherit values from a template
 host_name EPSON7A9F3B ; The name of the host the service is associated with
 service_description Printer Status ; The service description
 check_command check_hpjd!-C public ; The command used to monitor the service
}

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^X Replace ^U Uncut Text ^T To Spell ^L Go To Line M-E Redo

```

- Agregamos la siguiente definición de servicio para realizar un ping a la impresora cada 10 minutos por default. Esto es útil para monitorear RTA, pérdida de paquetes y conectividad en general en la red.

```

■ define service{

 use generic-service

 host_name nombre

 service_description PING

 check_command check_ping!3000.0,80%!5000.0,100%

 normal_check_interval 10

 retry_check_interval 1

}

```

```

GNU nano 2.9.3 /usr/local/nagios/etc/objects/printer.cfg

check_interval 10 ; Check the service every 10 minutes under normal conditions
retry_interval 1 ; Re-check the service every minute until its forced down state

Create a service for "pinging" the printer occasionally.
Useful for monitoring RTA, packet loss, etc.

define service {

 use generic-service
 host_name EPSON7A9F3B
 service_description PING
 check_command check_ping!3000.0,80%!5000.0,100%
 check_interval 10
 retry_interval 1
}

```

^G Get Help ^Q Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo  
 ^X Exit ^R Read File ^N Replace ^U Uncut Text ^T To Spell ^L Go To Line M-E Redo

- Guardamos y cerramos el archivo.

- Reiniciamos el servicio Nagios.

- service nagios restart

```
root@usuario:/usr/local/nagios/etc/objects# service nagios restart
```

#### Paso 4. Comprobar estado y funcionamiento.

- Nos vamos al navegador y entramos en Nagios para comprobar si se está monitoreando correctamente.

The screenshot shows the Nagios web interface with the following sections:

- Current Network Status:** Last Updated: Sat Apr 25 17:34:38 CEST 2020. Nagios Core™ 4.4.5 - www.nagios.org
- Host Status Totals:** Up: 7, Down: 0, Unreachable: 0, Pending: 0. All Problems: 0, All Types: 7.
- Service Status Totals:** Ok: 20, Warning: 0, Unknown: 0, Critical: 26, Pending: 0. All Problems: 26, All Types: 46.
- Host Status Details For All Host Groups:** A table listing 7 hosts:
 

| Host                      | Status | Last Check          | Duration       | Status Information                          |
|---------------------------|--------|---------------------|----------------|---------------------------------------------|
| EPSON7A9F3B               | UP     | 04-25-2020 17:34:21 | 0d 0h 2m 54s   | PING OK - Packet loss = 0%, RTA = 135.83 ms |
| cliente-VirtualBox        | UP     | 04-25-2020 17:31:33 | 0d 12h 36m 1s  | PING OK - Packet loss = 0%, RTA = 0.09 ms   |
| clientelinux14-VirtualBox | UP     | 04-25-2020 17:34:14 | 0d 0h 0m 24s   | PING OK - Packet loss = 0%, RTA = 1.43 ms   |
| clientew-PC               | UP     | 04-25-2020 17:33:14 | 0d 0h 1m 24s   | PING OK - Packet loss = 40%, RTA = 1.17 ms  |
| clientev2-PC              | UP     | 04-25-2020 17:34:28 | 0d 0h 5m 10s   | PING OK - Packet loss = 0%, RTA = 129.23 ms |
| localhost                 | UP     | 04-25-2020 17:33:48 | 1d 23h 25m 14s | PING OK - Packet loss = 0%, RTA = 0.08 ms   |
| winserver                 | UP     | 04-25-2020 17:31:26 | 0d 0h 8m 12s   | PING OK - Packet loss = 0%, RTA = 0.08 ms   |
- Reports:** Availability, Trends (Legacy), Alerts, History, Summary, Histogram (Legacy), Notifications, Event Log.
- System:** Comments, Downtime, Process Info, Performance Info.

**Nagios®**

**General**

- Home
- Documentation

**Current Status**

- Tactical Overview
- Map (Legacy)
- Hosts
- Services
- Host Groups
  - Summary
  - Grid
- Service Groups
  - Summary
  - Grid
- Problems
- Services (Unhandled)
- Hosts (Unhandled)
- Network Outages

Quick Search:

**Reports**

- Availability
- Trends (Legacy)
- Alerts
  - History
  - Summary
  - Histogram (Legacy)
- Notifications
- Event Log

**System**

- Comments
- Downtime
- Process Info

**Host Information**

Last Updated: Sat Apr 25 17:34:58 CEST 2020  
 Updated every 90 seconds  
 Nagios® Core™ 4.4.5 - www.nagios.org  
 Logged in as nagiosadmin

**Host**  
**IMPRESORA EPSON (EPSON7A9F3B)**

Member of network-printers

192.168.1.139

**Host State Information**

| Host Status:                 | UP (for 0d 0h 3m 14s)                                            |
|------------------------------|------------------------------------------------------------------|
| Status Information:          | PING OK - Packet loss = 0%, RTA = 135.83 ms                      |
| Performance Data:            | rta=135.832993ms;3000.000000;5000.000000;0.000000 pl=0%;80;100;0 |
| Current Attempt:             | 1/10 (HARD state)                                                |
| Last Check Time:             | 04-25-2020 17:34:21                                              |
| Check Type:                  | ACTIVE                                                           |
| Check Latency / Duration:    | 0.000 / 4.000 seconds                                            |
| Next Scheduled Active Check: | 04-25-2020 17:39:21                                              |
| Last State Change:           | 04-25-2020 17:31:44                                              |
| Last Notification:           | N/A (notification 0)                                             |
| Is This Host Flapping?       | NO (0.00% state change)                                          |
| In Scheduled Downtime?       | NO                                                               |
| Last Update:                 | 04-25-2020 17:34:57 (0d 0h 0m 1s ago)                            |

**Active Checks:** ENABLED  
**Passive Checks:** ENABLED  
**Obsessing:** ENABLED  
**Notifications:** ENABLED  
**Event Handler:** ENABLED  
**Flap Detection:** ENABLED

**Host Commands**

- Locate host on map
- Disable active checks of this host
- Re-schedule the next check of this host
- Submit passive check result for this host
- Stop accepting passive checks for this host
- Stop obsessing over this host
- Disable notifications for this host
- Send custom host notification
- Schedule downtime for this host
- Schedule downtime for all services on this host
- Disable notifications for all services on this host
- Enable notifications for all services on this host
- Schedule a check of all services on this host
- Disable checks of all services on this host
- Enable checks of all services on this host
- Disable event handler for this host
- Disable flap detection for this host
- Clear flapping state for this host

**Host Comments**

Add a new comment Delete all comments

Entry Time Author Comment Comment ID Persistent Type Expires Actions

This host has no comments associated with it

## Capítulo 13

### Otras opciones del menú de Nagios.

- Una vez tenemos nuestra estructura de red montada y lista para monitorizar, vamos a ver el apartado de reportes del menú de la interfaz web de Nagios.



- Availability o Disponibilidad: Nos muestra un informe de la disponibilidad de según lo que necesitemos.

#### Step 1: Select Report Type

Type:

- Vamos a elegir para el ejemplo "Hostgroup(s)". Elegimos el grupo que deseamos tener el informe, en este caso el de Linux.

### Step 2: Select Hostgroup

Hostgroup(s):

- Configuramos las opciones del reporte:

### Step 3: Select Report Options

Report Period:

If Custom Report Period...

|                         |                                                                     |                                |                                   |
|-------------------------|---------------------------------------------------------------------|--------------------------------|-----------------------------------|
| Start Date (Inclusive): | <input type="text" value="April"/> <input type="button" value="▼"/> | <input type="text" value="1"/> | <input type="text" value="2020"/> |
| End Date (Inclusive):   | <input type="text" value="April"/> <input type="button" value="▼"/> | <input type="text" value="3"/> | <input type="text" value="2020"/> |

Report time Period:

Assume Initial States:

Assume State Retention:

Assume States During Program Downtime:

Include Soft States:

First Assumed Host State:

First Assumed Service State:

Backtracked Archives (To Scan For Initial States):

Output in CSV Format:

- Creamos el reporte:



| Host      | % Time Up           | % Time Down     | % Time Unreachable | % Time Undetermined |
|-----------|---------------------|-----------------|--------------------|---------------------|
| localhost | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%)    | 0.000%              |
| Average   | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%)    | 0.000%              |

### Host State Breakdowns:

| State        | Type / Reason      | Time        | % Total Time | % Known Time |
|--------------|--------------------|-------------|--------------|--------------|
| UP           | Unscheduled        | 7d 0h 0m 0s | 100.000%     | 100.000%     |
|              | Scheduled          | 0d 0h 0m 0s | 0.000%       | 0.000%       |
|              | Total              | 7d 0h 0m 0s | 100.000%     | 100.000%     |
| DOWN         | Unscheduled        | 0d 0h 0m 0s | 0.000%       | 0.000%       |
|              | Scheduled          | 0d 0h 0m 0s | 0.000%       | 0.000%       |
|              | Total              | 0d 0h 0m 0s | 0.000%       | 0.000%       |
| UNREACHABLE  | Unscheduled        | 0d 0h 0m 0s | 0.000%       | 0.000%       |
|              | Scheduled          | 0d 0h 0m 0s | 0.000%       | 0.000%       |
|              | Total              | 0d 0h 0m 0s | 0.000%       | 0.000%       |
| Undetermined | Nagios Not Running | 0d 0h 0m 0s | 0.000%       |              |
|              | Insufficient Data  | 0d 0h 0m 0s | 0.000%       |              |
|              | Total              | 0d 0h 0m 0s | 0.000%       |              |
| All          | Total              | 7d 0h 0m 0s | 100.000%     | 100.000%     |

### State Breakdowns For Host Services:

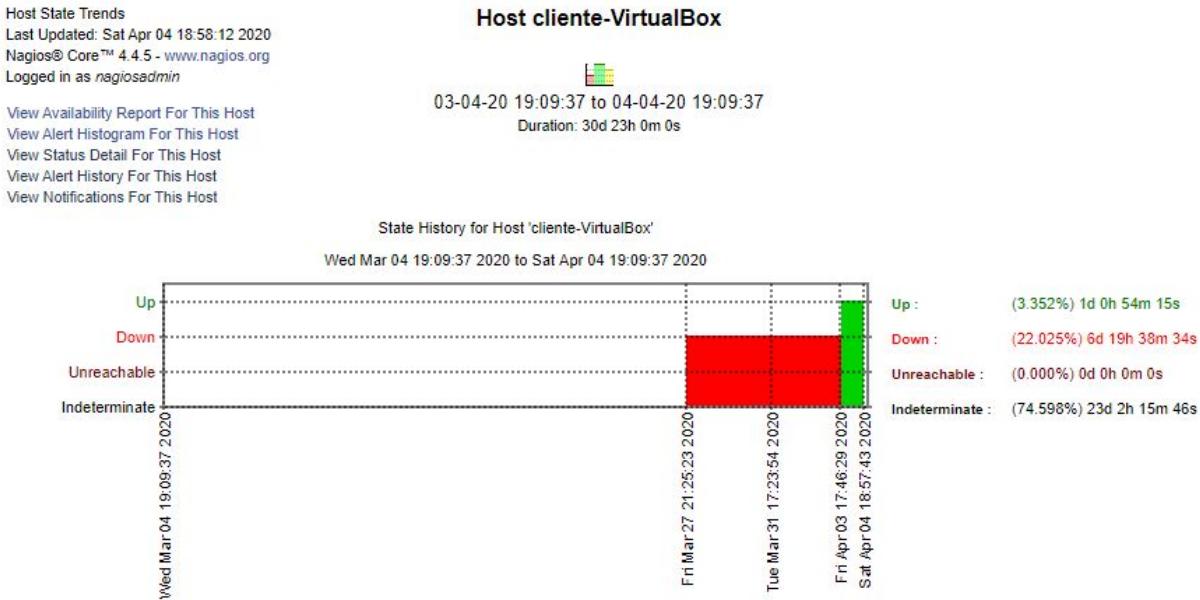
| Service         | % Time OK           | % Time Warning  | % Time Unknown  | % Time Critical | % Time Undetermined |
|-----------------|---------------------|-----------------|-----------------|-----------------|---------------------|
| Current Load    | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000%              |
| Current Users   | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000%              |
| HTTP            | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000%              |
| PING            | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000%              |
| Root Partition  | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000%              |
| SSH             | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000%              |
| Swap Usage      | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000%              |
| Total Processes | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000%              |
| Average         | 100.000% (100.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000% (0.000%) | 0.000%              |

### Host Log Entries:

[ View full log entries ]

| Event Start Time    | Event End Time      | Event Duration | Event/State Type | Event/State Information                    |
|---------------------|---------------------|----------------|------------------|--------------------------------------------|
| 03-21-2020 23:00:00 | 03-28-2020 23:00:00 | 7d 0h 0m 0s+   | HOST UP (HARD)   | First Host State Assumed (Faked Log Entry) |

- Trends o Tendencias: nos lo muestra graficamente.



- Alerts o Alertas:

■ History: nos muestra un listado de alertas por orden cronológico.

**Alert History**  
Last Updated: Fri Apr 3 19:22:18 CEST 2020  
Nagios® Core™ 4.4.5 - www.nagios.org  
Logged in as nagiosadmin

**All Hosts and Services**

Latest Archive      Log File Navigation  
Fri Apr 3 00:00:00 CEST 2020 to Present.  
File: /usr/local/nagios/var/nagios.log

State type options:  
 All state types ▾  
 Hide Flapping Alerts  
 Hide Downtime Alerts  
 Hide Process Messages  
 Older Entries First

abril 03, 2020 19:00

[04-03-2020 19:19:29] HOST ALERT: cliente-PC;DOWN;HARD;10;CRITICAL - Host Unreachable (192.168.1.137)  
[04-03-2020 19:19:01] SERVICE ALERT: cliente-PC;NSClient++ Version:CRITICAL;HARD;3;connect to address 192.168.1.137 and port 12489: No route to host  
[04-03-2020 19:19:01] SERVICE FLAPPING ALERT: cliente-PC;NSClient++ Version:STARTED: Service appears to have started flapping (23.6% change >= 20.0% threshold)  
[04-03-2020 19:18:26] HOST ALERT: cliente-PC;DOWN;SOFT;9;CRITICAL - Host Unreachable (192.168.1.137)  
[04-03-2020 19:17:46] SERVICE ALERT: cliente-PC;Memory Usage:CRITICAL;HARD;3;connect to address 192.168.1.137 and port 12489: No route to host  
[04-03-2020 19:17:46] SERVICE FLAPPING ALERT: cliente-PC;Memory Usage:STARTED: Service appears to have started flapping (23.6% change >= 20.0% threshold)  
[04-03-2020 19:17:23] HOST ALERT: cliente-PC;DOWN;SOFT;8;CRITICAL - Host Unreachable (192.168.1.137)  
[04-03-2020 19:16:41] SERVICE ALERT: cliente-PC;Explorer:CRITICAL;HARD;3;connect to address 192.168.1.137 and port 12489: No route to host  
[04-03-2020 19:16:20] HOST ALERT: cliente-PC;DOWN;SOFT;7;CRITICAL - Host Unreachable (192.168.1.137)  
[04-03-2020 19:15:17] HOST ALERT: cliente-PC;DOWN;SOFT;6;CRITICAL - Host Unreachable (192.168.1.137)  
[04-03-2020 19:15:17] SERVICE ALERT: cliente-PC;CPU Load:CRITICAL;HARD;3;connect to address 192.168.1.137 and port 12489: No route to host  
[04-03-2020 19:15:17] SERVICE FLAPPING ALERT: cliente-PC;CPU Load:STARTED: Service appears to have started flapping (23.7% change >= 20.0% threshold)  
[04-03-2020 19:14:15] HOST ALERT: cliente-PC;DOWN;SOFT;5;CRITICAL - Host Unreachable (192.168.1.137)  
[04-03-2020 19:14:03] SERVICE ALERT: cliente-PC;C:\Drive Space:CRITICAL;HARD;3;connect to address 192.168.1.137 and port 12489: No route to host  
[04-03-2020 19:14:03] SERVICE FLAPPING ALERT: cliente-PC;C:\Drive Space:STARTED: Service appears to have started flapping (23.7% change >= 20.0% threshold)  
[04-03-2020 19:13:12] HOST ALERT: cliente-PC;DOWN;SOFT;4;CRITICAL - Host Unreachable (192.168.1.137)  
[04-03-2020 19:12:09] HOST ALERT: cliente-PC;DOWN;SOFT;3;CRITICAL - Host Unreachable (192.168.1.137)  
[04-03-2020 19:12:03] SERVICE ALERT: cliente-PC;PING:CRITICAL;HARD;2;CRITICAL - Host Unreachable (192.168.1.137)  
[04-03-2020 19:11:30] SERVICE ALERT: cliente-PC;W3SVC:CRITICAL;HARD;3;connect to address 192.168.1.137 and port 12489: No route to host  
[04-03-2020 19:11:30] SERVICE FLAPPING ALERT: cliente-PC;W3SVC:STARTED: Service appears to have started flapping (23.8% change >= 20.0% threshold)  
[04-03-2020 19:11:06] HOST ALERT: cliente-PC;DOWN;SOFT;2;CRITICAL - Host Unreachable (192.168.1.137)  
[04-03-2020 19:10:15] SERVICE ALERT: cliente-PC;Uptime:CRITICAL;HARD;3;connect to address 192.168.1.137 and port 12489: No route to host  
[04-03-2020 19:10:15] SERVICE FLAPPING ALERT: cliente-PC;Uptime:STARTED: Service appears to have started flapping (23.8% change >= 20.0% threshold)

- Summary o Resumen: lo vemos de forma resumida según la configuración que le indiquemos.

**Alert Summary Report**  
 Last Updated: Fri Apr 3 19:23:10 CEST 2020  
 Nagios® Core™ 4.4.5 - www.nagios.org  
 Logged in as nagiosadmin

**Standard Reports:**

Report Type: Top 25 Hard Host Alert Producers ▾

**Custom Report Options:**

Report Type: Most Recent Alerts ▾  
 Report Period: This Year ▾  
 If Custom Report Period...  
 Start Date (Inclusive): April 1 2020  
 End Date (Inclusive): April 3 2020  
 Limit To Hostgroup: \*\* ALL HOSTGROUPS \*\* ▾  
 Limit To Servicegroup: \*\* ALL SERVICEGROUPS \*\* ▾  
 Limit To Host: \*\* ALL HOSTS \*\* ▾  
 Alert Types: Host and Service Alerts ▾  
 State Types: Hard and Soft States ▾  
 Host States: All Host States ▾  
 Service States: All Service States ▾  
 Max List Items: 25

**Alert Summary Report**  
 Last Updated: Sat Apr 4 18:40:31 CEST 2020  
 Nagios® Core™ 4.4.5 - www.nagios.org  
 Logged in as nagiosadmin

**Most Recent Alerts**  
 01-01-2020 00:00:00 to 04-04-2020 18:40:31  
 Duration: 94d 17h 40m 31s

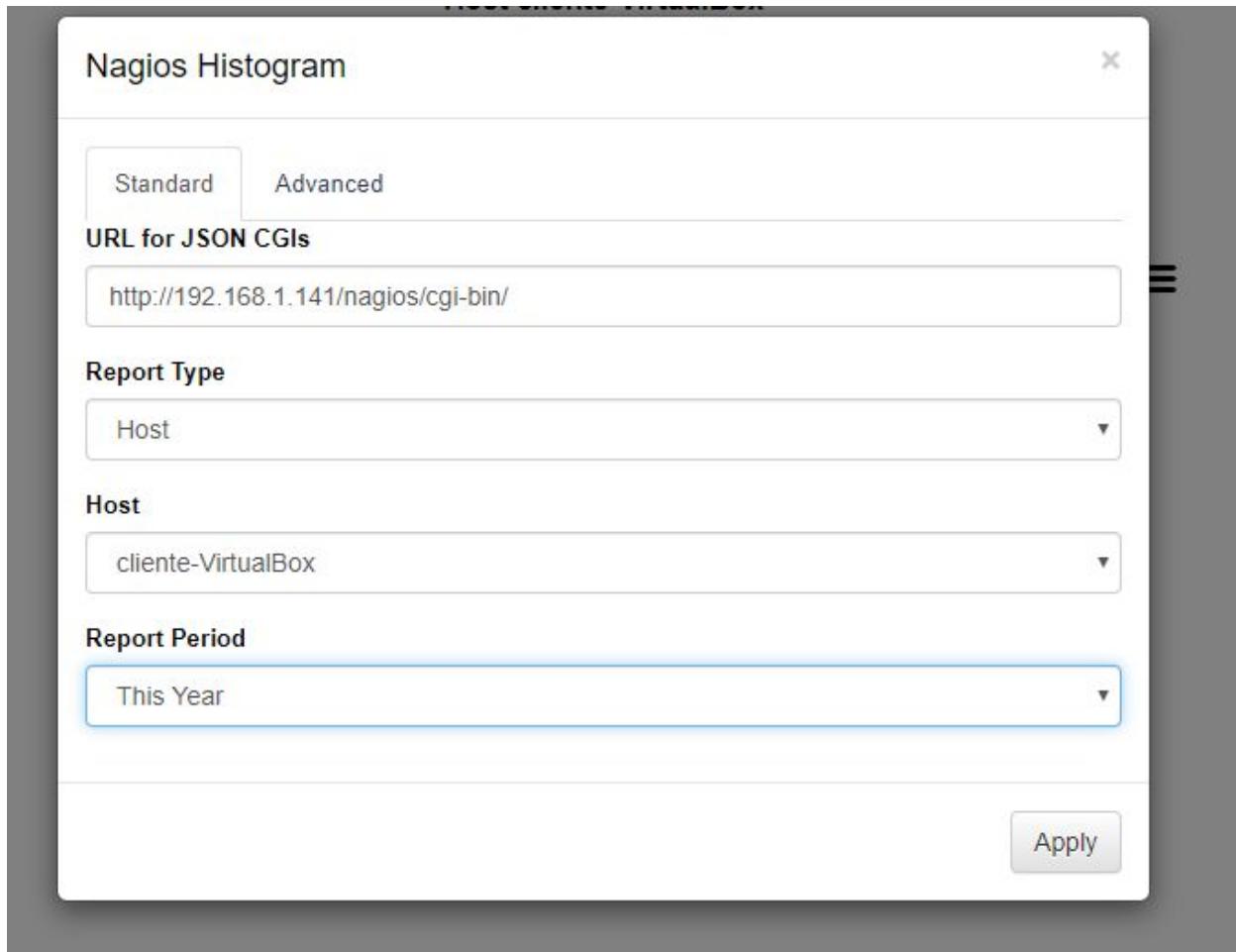
**Report Options Summary:**  
 Alert Types: Host & Service Alerts  
 State Types: Soft & Hard States  
 Host States: Up, Down, Unreachable  
 Service States: Ok, Warning, Unknown, Critical

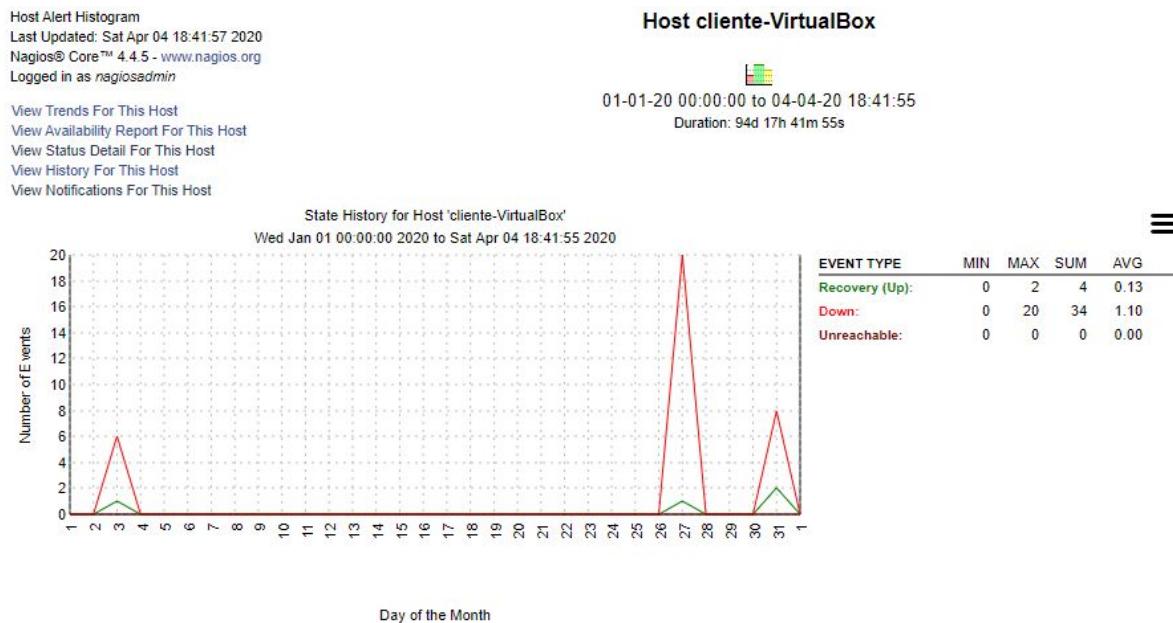
Displaying most recent 25 of 157 total matching alerts

| Time                | Alert Type    | Host               | Service            | State    | State Type | Information                                                       |
|---------------------|---------------|--------------------|--------------------|----------|------------|-------------------------------------------------------------------|
| 04-03-2020 19:19:29 | Host Alert    | clientew-PC        | N/A                | DOWN     | HARD       | CRITICAL - Host Unreachable (192.168.1.137)                       |
| 04-03-2020 19:19:01 | Service Alert | clientew-PC        | NSClient++ Version | CRITICAL | HARD       | connect to address 192.168.1.137 and port 12489: No route to host |
| 04-03-2020 19:18:26 | Host Alert    | clientew-PC        | N/A                | DOWN     | SOFT       | CRITICAL - Host Unreachable (192.168.1.137)                       |
| 04-03-2020 19:17:46 | Service Alert | clientew-PC        | Memory Usage       | CRITICAL | HARD       | connect to address 192.168.1.137 and port 12489: No route to host |
| 04-03-2020 19:17:23 | Host Alert    | clientew-PC        | N/A                | DOWN     | SOFT       | CRITICAL - Host Unreachable (192.168.1.137)                       |
| 04-03-2020 19:16:41 | Service Alert | clientew-PC        | Explorer           | CRITICAL | HARD       | connect to address 192.168.1.137 and port 12489: No route to host |
| 04-03-2020 19:16:26 | Host Alert    | clientew-PC        | N/A                | DOWN     | SOFT       | CRITICAL - Host Unreachable (192.168.1.137)                       |
| 04-03-2020 19:15:17 | Host Alert    | clientew-PC        | N/A                | DOWN     | SOFT       | CRITICAL - Host Unreachable (192.168.1.137)                       |
| 04-03-2020 19:15:17 | Service Alert | clientew-PC        | CPU Load           | CRITICAL | HARD       | connect to address 192.168.1.137 and port 12489: No route to host |
| 04-03-2020 19:14:15 | Host Alert    | clientew-PC        | N/A                | DOWN     | SOFT       | CRITICAL - Host Unreachable (192.168.1.137)                       |
| 04-03-2020 19:14:03 | Service Alert | clientew-PC        | C:\ Drive Space    | CRITICAL | HARD       | connect to address 192.168.1.137 and port 12489: No route to host |
| 04-03-2020 19:13:12 | Host Alert    | clientew-PC        | N/A                | DOWN     | SOFT       | CRITICAL - Host Unreachable (192.168.1.137)                       |
| 04-03-2020 19:12:06 | Host Alert    | clientew-PC        | N/A                | DOWN     | SOFT       | CRITICAL - Host Unreachable (192.168.1.137)                       |
| 04-03-2020 19:12:03 | Service Alert | clientew-PC        | PING               | CRITICAL | HARD       | CRITICAL - Host Unreachable (192.168.1.137)                       |
| 04-03-2020 19:11:30 | Service Alert | clientew-PC        | W3SVC              | CRITICAL | HARD       | connect to address 192.168.1.137 and port 12489: No route to host |
| 04-03-2020 19:11:06 | Host Alert    | clientew-PC        | N/A                | DOWN     | SOFT       | CRITICAL - Host Unreachable (192.168.1.137)                       |
| 04-03-2020 19:10:15 | Service Alert | clientew-PC        | Uptime             | CRITICAL | HARD       | connect to address 192.168.1.137 and port 12489: No route to host |
| 04-03-2020 19:10:03 | Host Alert    | clientew-PC        | N/A                | DOWN     | SOFT       | CRITICAL - Host Unreachable (192.168.1.137)                       |
| 04-03-2020 19:10:00 | Service Alert | clientew-PC        | PING               | CRITICAL | SOFT       | CRITICAL - Plugin timed out                                       |
| 04-03-2020 19:08:58 | Service Alert | clientew-PC        | NSClient++ Version | UNKNOWN  | HARD       | NSClient - ERROR: Invalid password.                               |
| 04-03-2020 19:07:43 | Service Alert | clientew-PC        | Memory Usage       | UNKNOWN  | HARD       | NSClient - ERROR: Invalid password.                               |
| 04-03-2020 19:06:38 | Service Alert | clientew-PC        | Explorer           | WARNING  | HARD       | No data was received from host!                                   |
| 04-03-2020 19:05:14 | Service Alert | clientew-PC        | CPU Load           | UNKNOWN  | HARD       | NSClient - ERROR: Invalid password.                               |
| 04-03-2020 19:04:14 | Service Alert | cliente-VirtualBox | SSH                | OK       | HARD       | SSH OK - OpenSSH_7_6p1 Ubuntu-4ubuntu0.3 (protocol 2.0)           |
| 04-03-2020 19:04:01 | Service Alert | clientew-PC        | C:\ Drive Space    | UNKNOWN  | HARD       | NSClient - ERROR: Invalid password.                               |

- Histogram o Histograma: Podemos ver una grafica historica por "Hosts" o "Servicios".

- Host:





- Servicio:

Nagios Histogram

Standard     Advanced

**URL for JSON CGIs**

**Report Type**

**Host**

**Service**

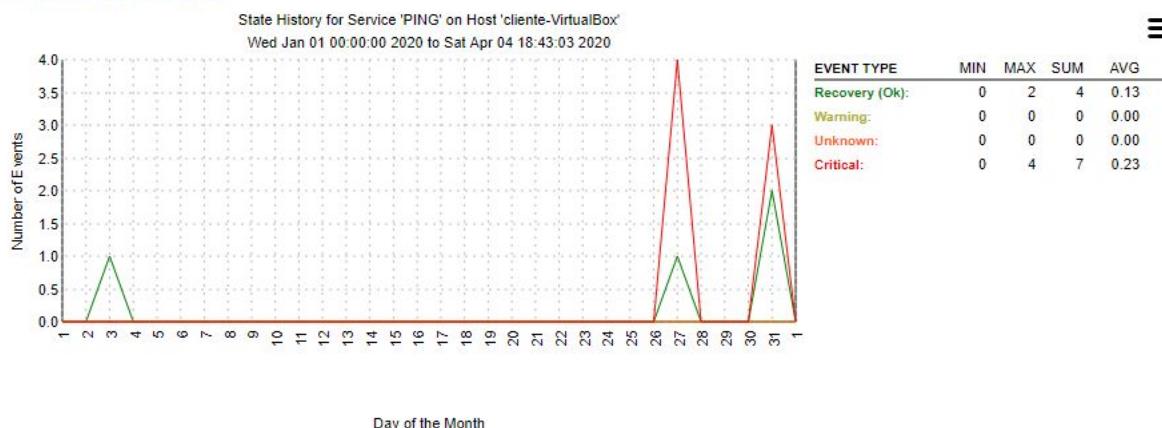
**Report Period**

Service Alert Histogram  
 Last Updated: Sat Apr 04 18:43:05 2020  
 Nagios® Core™ 4.4.5 - www.nagios.org  
 Logged in as nagiosadmin

[View Trends For This Service](#)  
[View Availability Report For This Service](#)  
[View History For This Service](#)  
[View Notifications For This Service](#)

### Service PING on cliente-VirtualBox

01-01-20 00:00:00 to 04-04-20 18:43:03  
 Duration: 94d 17h 43m 3s



- Notifications o Notificaciones: Nos muestra una lista de las notificaciones que se mandan por email u otros medios de todos los dispositivos ordenados cronológicamente.

| Contact Notifications                      |                    |           |                     |             |                         |                                             |
|--------------------------------------------|--------------------|-----------|---------------------|-------------|-------------------------|---------------------------------------------|
| Last Updated: Sat Apr 4 18:44:11 CEST 2020 |                    |           |                     |             |                         |                                             |
| Nagios® Core™ 4.4.5 - www.nagios.org       |                    |           |                     |             |                         |                                             |
| Host                                       | Service            | Type      | Time                | Contact     | Notification Command    | Information                                 |
| clientew-PC                                | N/A                | HOST DOWN | 04-03-2020 19:19:29 | nagiosadmin | notify-host-by-email    | CRITICAL - Host Unreachable (192.168.1.137) |
| winserver                                  | N/A                | HOST DOWN | 04-03-2020 19:18:21 | nagiosadmin | notify-host-by-email    | CRITICAL - Host Unreachable (192.168.1.2)   |
| clientew-PC                                | NSClient++ Version | UNKNOWN   | 04-03-2020 19:08:58 | nagiosadmin | notify-service-by-email | NSClient - ERROR: Invalid password.         |
| clientew-PC                                | Memory Usage       | UNKNOWN   | 04-03-2020 19:07:43 | nagiosadmin | notify-service-by-email | NSClient - ERROR: Invalid password.         |
| clientew-PC                                | Explorer           | WARNING   | 04-03-2020 19:06:38 | nagiosadmin | notify-service-by-email | No data was received from host!             |
| clientew-PC                                | CPU Load           | UNKNOWN   | 04-03-2020 19:05:14 | nagiosadmin | notify-service-by-email | NSClient - ERROR: Invalid password.         |
| clientew-PC                                | C:\ Drive Space    | UNKNOWN   | 04-03-2020 19:04:01 | nagiosadmin | notify-service-by-email | NSClient - ERROR: Invalid password.         |
| clientew-PC                                | W3SVC              | UNKNOWN   | 04-03-2020 19:01:27 | nagiosadmin | notify-service-by-email | NSClient - ERROR: Invalid password.         |
| clientew-PC                                | Uptime             | UNKNOWN   | 04-03-2020 19:00:12 | nagiosadmin | notify-service-by-email | NSClient - ERROR: Invalid password.         |
| clientew-PC                                | N/A                | HOST UP   | 04-03-2020 18:59:57 | nagiosadmin | notify-host-by-email    | PING OK - Packet loss = 0%, RTA = 0.91 ms   |
| clientew-PC                                | N/A                | HOST DOWN | 04-03-2020 18:55:45 | nagiosadmin | notify-host-by-email    | CRITICAL - Host Unreachable (192.168.1.137) |
| winserver                                  | N/A                | HOST DOWN | 04-03-2020 18:48:21 | nagiosadmin | notify-host-by-email    | CRITICAL - Host Unreachable (192.168.1.2)   |

- Event log: Nos muestra el archivo de log que tienen "todos" los servicios que podemos instalar en Linux, pero desde la interfaz Web, en el cual se visualiza mejor, pero que al fin y al cabo lo que vemos son las entradas del archivo de log.

**Current Event Log**  
 Last Updated: Sat Apr 4 18:45:27 CEST 2020  
 Nagios® Core™ 4.4.5 - www.nagios.org  
 Logged in as nagiosadmin

**Latest Archive**

**Log File Navigation**  
 Sat Apr 4 00:00:00 CEST 2020  
 to Present.  
 File: /usr/local/nagios/var/nagios.log

Older Entries First Update

---

**abril 04, 2020 18:00**

---

[i] [04-04-2020 18:39:59] Warning: A system time change of 83752 seconds (0d 23h 15m 52s forwards in time) has been detected. Compensating...

---

**abril 03, 2020 19:00**

---

[i] [04-03-2020 19:19:29] vproc: stderr line 02: /usr/bin/printf: write error: Broken pipe  
 [i] [04-03-2020 19:19:29] vproc: stderr line 01: /bin/sh: 1: /bin/mail: not found  
 [i] [04-03-2020 19:19:29] vproc: early\_timeout=0; exited\_ok=1; wait\_status=32512; error\_code=0;  
 [i] [04-03-2020 19:19:29] vproc: host=clientev-PC; service=(none); contact=nagiosadmin  
 [i] [04-03-2020 19:19:29] vproc: NOTIFY job 25 from worker Core Worker 11745 is a non-check helper but exited with return code 127  
 [!] [04-03-2020 19:19:29] HOST ALERT: clientev-PC;DOWN;HARD;10;CRITICAL - Host Unreachable (192.168.1.137)  
 [!] [04-03-2020 19:19:01] HOST NOTIFICATION: nagiosadmin.clientev-PC;DOWN;notify-host-by-email;CRITICAL - Host Unreachable (192.168.1.137)  
 [!] [04-03-2020 19:19:01] SERVICE ALERT: clientev-PC;NSClient++;Version;CRITICAL;HARD;3:connect to address 192.168.1.137 and port 12489: No route to host  
 [▲] [04-03-2020 19:19:01] SERVICE FLAPPING ALERT: clientev-PC;NSClient++;Version;STARTED: Service appears to have started flapping (23.6% change >= 20.0% threshold)  
 [!] [04-03-2020 19:18:26] HOST ALERT: clientev-PC;DOWN;SOFT;9;CRITICAL - Host Unreachable (192.168.1.137)  
 [i] [04-03-2020 19:18:21] vproc: stderr line 02: /usr/bin/printf: write error: Broken pipe  
 [i] [04-03-2020 19:18:21] vproc: stderr line 01: /bin/sh: 1: /bin/mail: not found  
 [i] [04-03-2020 19:18:21] vproc: early\_timeout=0; exited\_ok=1; wait\_status=32512; error\_code=0;  
 [i] [04-03-2020 19:18:21] vproc: host=winserver; service=(none); contact=nagiosadmin  
 [i] [04-03-2020 19:18:21] vproc: NOTIFY job 22 from worker Core Worker 11742 is a non-check helper but exited with return code 127  
 [!] [04-03-2020 19:18:21] HOST NOTIFICATION: nagiosadmin.winserver;DOWN;notify-host-by-email;CRITICAL - Host Unreachable (192.168.1.2)  
 [!] [04-03-2020 19:17:46] SERVICE ALERT: clientev-PC;Memory Usage;CRITICAL;HARD;3:connect to address 192.168.1.137 and port 12489: No route to host  
 [▲] [04-03-2020 19:17:46] SERVICE FLAPPING ALERT: clientev-PC;Memory Usage;STARTED: Service appears to have started flapping (23.6% change >= 20.0% threshold)  
 [!] [04-03-2020 19:17:23] HOST ALERT: clientev-PC;DOWN;SOFT;8;CRITICAL - Host Unreachable (192.168.1.137)  
 [!] [04-03-2020 19:16:41] SERVICE ALERT: clientev-PC;Explorer;CRITICAL;HARD;3:connect to address 192.168.1.137 and port 12489: No route to host  
 [▲] [04-03-2020 19:16:41] SERVICE FLAPPING ALERT: clientev-PC;Explorer;STARTED: Service appears to have started flapping (23.6% change >= 20.0% threshold)  
 [!] [04-03-2020 19:16:20] HOST ALERT: clientev-PC;DOWN;SOFT;7;CRITICAL - Host Unreachable (192.168.1.137)  
 [!] [04-03-2020 19:15:17] HOST ALERT: clientev-PC;DOWN;SOFT;6;CRITICAL - Host Unreachable (192.168.1.137)  
 [!] [04-03-2020 19:15:17] SERVICE ALERT: clientev-PC;CPU Load;CRITICAL;HARD;3:connect to address 192.168.1.137 and port 12489: No route to host  
 [▲] [04-03-2020 19:15:17] SERVICE FLAPPING ALERT: clientev-PC;CPU Load;STARTED: Service appears to have started flapping (23.7% change >= 20.0% threshold)  
 [!] [04-03-2020 19:14:15] HOST ALERT: clientev-PC;DOWN;SOFT;5;CRITICAL - Host Unreachable (192.168.1.137)

## Capítulo 14

### Nagios Log Server.

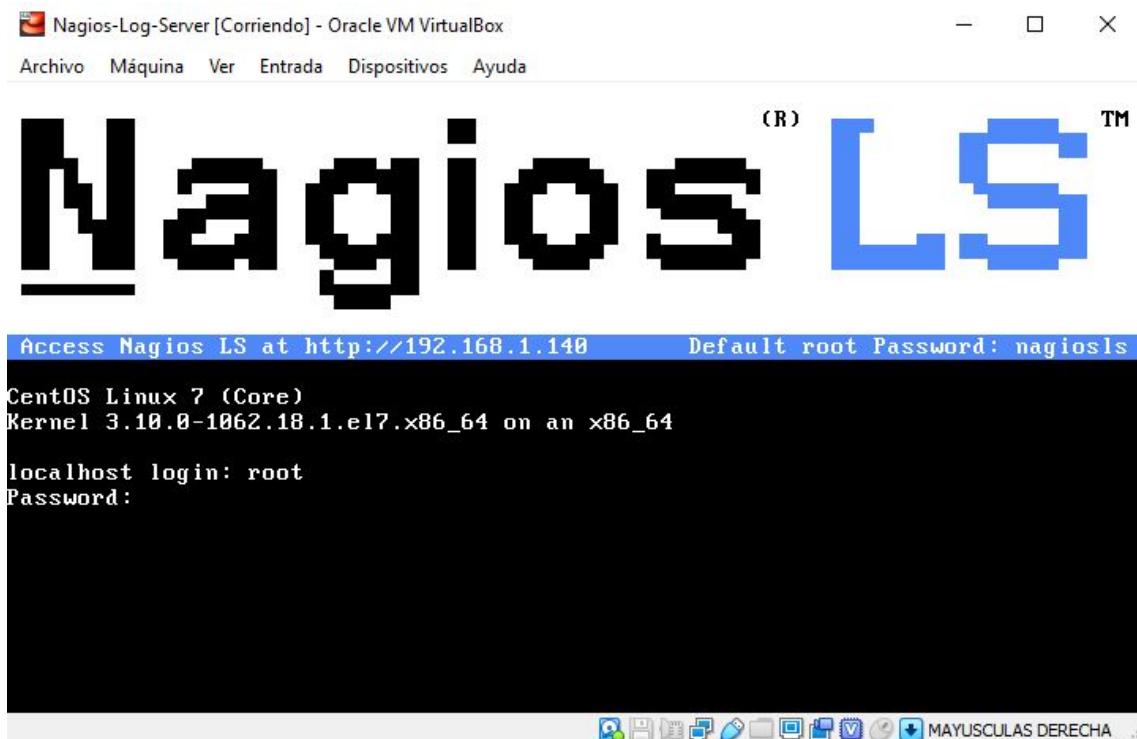
#### Paso 1. Qué es, características.

- Nagios Log Server proporciona a los técnicos la capacidad de buscar y analizar todo tipo de datos en sus logs de una forma rápida y fácil. Nagios Log Server proporciona los siguientes beneficios a los técnicos que lo utilicen:
  - Facilidad de uso: simplifica enormemente el proceso de búsqueda en logs. También se puede configurar alertas para que le notifique cuando se presentan amenazas potenciales, o simplemente filtrar los datos para auditar rápidamente su sistema. Se consigue todos sus datos en un único dashboard, con alta disponibilidad.
  - Escalabilidad: se puede agregar fácilmente instancias adicionales de servidor de logs para el clúster de supervisión. Está diseñado para organizaciones de cualquier tamaño y puede adaptarse con el clic de un botón.
  - Datos en tiempo real: te permite ver los datos de sus logs en tiempo real, proporcionando la capacidad de analizar y resolver los problemas a medida que ocurren rápidamente. Esto mantiene su organización segura, y funcionando sin problemas.
  - Adaptabilidad: tiene una API totalmente accesible que permite una completa personalización para adaptarse a las necesidades de su red. Integrar con soluciones de terceros para una perfecta integración con su infraestructura actual.

- Seguridad de la red: es una solución de primera clase que está perfectamente diseñado para la realización de auditorías de su red.
- Gestión avanzada del usuario: Los administradores pueden agregar, modificar y eliminar usuarios, así como establecer permisos de acceso para que los usuarios sólo pueden modificar los cambios en su propio perfil. Administradores también pueden conceder a determinados usuarios el acceso a la API externa a través de una clave de acceso.

## Paso 2. Elementos vistos en la práctica.

- Nos instalamos la ova que nos dan al descargar en la página oficial de Nagios. Como usuario ponemos root y como contraseña nagiosls.



- Entramos al navegador e introducimos la ip que nos aparece en la máquina, en mi caso 192.168.1.140. Con esto comenzará la instalación.

**Final Installation Steps**

Your're almost done. Setup your instance or connect to existing cluster.

**Install**  
Install a new Nagios Log Server cluster

**Connect**  
Add this as an instance to an existing cluster

---

**License Setup**

Choose a trial license, enter your key, or [get a license now.](#)

Free 30 day trial  I already have a key

**License Key**

---

**Admin Account Setup**

Enter the admin account settings. The default username is nagiosadmin.

|                         |                           |
|-------------------------|---------------------------|
| <b>Username</b>         | nagiosadmin               |
| <b>Full Name</b>        | Nagios Administrator      |
| <b>Password</b>         | *****                     |
| <b>Confirm Password</b> | *****                     |
| <b>Email</b>            | a_angbongom@iestriana.com |
| <b>Language</b>         | Spanish (español)         |
| <b>Timezone</b>         | (UTC+01:00) Madrid        |

**< Back** **Finish Installation >**

- Ahora entraremos con el usuario nagiosadmin y la contraseña del servidor que en mi caso es usuario.

**About Nagios Log Server**  
Nagios Log Server is an enterprise-class log analysis solution that provides organizations with insight into logged errors before problems affect critical business processes. For more information on Nagios Log Server, visit the [Nagios Log Server product page](#).

**Nagios Learning Opportunities**  
Learn about Nagios [training](#) and [certification](#) programs.  
Want to learn about how other experts are utilizing Nagios? Do not miss your chance to attend the next [Nagios World Conference](#).

**Contact Us**  
Have a question or technical problem? Contact us today:

- Para añadir nuestro dispositivo Linux hacemos click en el icono de Linux y usamos estos comandos:

```
root@cliente-VirtualBox:/home/cliente# curl -sS -O http://192.168.1.140/nagioslogserver/scripts/setup-linux.sh
root@cliente-VirtualBox:/home/cliente# bash setup-linux.sh -s 192.168.1.140 -p 5544
Detected rsyslog 8.32.0
Detected rsyslog work directory /var/spool/rsyslog
Destination Log Server: 192.168.1.140:5544
Creating /etc/rsyslog.d/99-nagioslogserver.conf...
getenforce command not found, assuming SELinux is disabled.
rsyslog configuration check passed.
Restarting rsyslog service with 'service'...
Okay.
rsyslog is running with the new configuration.
Visit your Nagios Log Server dashboard to verify that logs are being received.
root@cliente-VirtualBox:/home/cliente#
```

- Verificamos que ha sido agregado:

### verificar los registros entrantes

una vez que haya configurado el remitente del registro, debería comenzar a recibir registros de inmediato. ingrese la dirección IP del remitente para ver si está recibiendo registros de esa ip.

|               |               |                  |
|---------------|---------------|------------------|
| dirección NRD | 192.168.1.144 | <b>verificar</b> |
|---------------|---------------|------------------|

**verificado** existen **12** registros para el anfitrión **192.168.1.144**.

- Vemos que el programa lo está monitoreando.

| campos                        |               |        |                                                                                                                                           |  | 0 a 50 de 250 disponibles para paginación |
|-------------------------------|---------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------|--|-------------------------------------------|
|                               |               |        |                                                                                                                                           |  | Acciones                                  |
| @timestamp                    | host          | type   | message                                                                                                                                   |  |                                           |
| 2020-03-31T19:25:39.000+02:00 | 192.168.1.144 | syslog | Started Cleanup of Temporary Directories.                                                                                                 |  |                                           |
| 2020-03-31T19:25:39.000+02:00 | 192.168.1.144 | syslog | Starting Cleanup of Temporary Directories...                                                                                              |  |                                           |
| 2020-03-31T19:24:47.000+02:00 | 192.168.1.144 | syslog | #31 0x565410de6b40 i resource:///org/gnome/gjs/modules/tweener/tweener.js:365 (0x7f59e06d2cd0 @ 10)                                       |  |                                           |
| 2020-03-31T19:24:47.000+02:00 | 192.168.1.144 | syslog | #26 0x565410de6e90 i resource:///org/gnome/shell/ui/lightbox.js:186 (0x7f59e0438a28 @ 29)                                                 |  |                                           |
| 2020-03-31T19:24:47.000+02:00 | 192.168.1.144 | syslog | #21 0xffed0e2c8c0 b resource:///org/gnome/gjs/modules/_legacy.js:82 (0x7f59e06b5de0 @ 71)                                                 |  |                                           |
| 2020-03-31T19:24:47.000+02:00 | 192.168.1.144 | syslog | #12 0xffed0e27100 b self-hosted:251 (0x7f59e06c4ab0 @ 223)                                                                                |  |                                           |
| 2020-03-31T19:24:47.000+02:00 | 192.168.1.144 | syslog | #7.0x565410de7438 i /usr/share/gnome-shell/extensions/ubuntu-appindicators@ubuntu.com/statusNotifierWatcher.js:219 (0x7f59c43ae5e8 @ 225) |  |                                           |
| 2020-03-31T19:24:47.000+02:00 | 192.168.1.144 | syslog | #3 0xffed0e23be0 b self-hosted:916 (0x7f59e06f12b8 @ 367)                                                                                 |  |                                           |
| 2020-03-31T19:24:47.000+02:00 | 192.168.1.144 | syslog | #35 0x565410de6a30 i resource:///org/gnome/shell/ui/tweener.js:219 (0x7f59e06cf780 @ 15)                                                  |  |                                           |
| 2020-03-31T19:24:47.000+02:00 | 192.168.1.144 | syslog | #30 0x565410de6bb8 i resource:///org/gnome/gjs/modules/tweener/tweener.js:350 (0x7f59e06d2c48 @ 100)                                      |  |                                           |
| 2020-03-31T19:24:47.000+02:00 | 192.168.1.144 | syslog | #23 0xffed0e2dc20 b resource:///org/gnome/gjs/modules/_legacy.js:82 (0x7f59e06b5de0 @ 71)                                                 |  |                                           |
| 2020-03-31T19:24:47.000+02:00 | 192.168.1.144 | syslog | #19 0xffed0e2b560 b resource:///org/gnome/gjs/modules/_legacy.js:82 (0x7f59e06b5de0 @ 71)                                                 |  |                                           |
| 2020-03-31T19:24:47.000+02:00 | 192.168.1.144 | syslog | #12 0xffed0e27100 b self-hosted:251 (0x7f59e06c4ab0 @ 223)                                                                                |  |                                           |

Vistas: mesa / JSON / crudo

| campo                                          | Acciones | Valor                                            |
|------------------------------------------------|----------|--------------------------------------------------|
| <input checked="" type="checkbox"/> @timestamp |          | 2020-03-31T17:30:46.000Z                         |
| <input type="checkbox"/> @version              |          | 1                                                |
| <input type="checkbox"/> _id                   |          | AXExKiB1Q0xjF2HraEHT                             |
| <input type="checkbox"/> _index                |          | logstash-2020.03.31                              |
| <input type="checkbox"/> _type                 |          | syslog                                           |
| <input type="checkbox"/> facility              |          | 3                                                |
| <input type="checkbox"/> facility_label        |          | system                                           |
| <input checked="" type="checkbox"/> host       |          | 192.168.1.144                                    |
| <input type="checkbox"/> logsource             |          | cliente-VirtualBox                               |
| <input checked="" type="checkbox"/> message    |          | Supervising 4 threads of 2 processes of 1 users. |
| <input type="checkbox"/> pid                   |          | 10395                                            |
| <input type="checkbox"/> priority              |          | 31                                               |
| <input type="checkbox"/> program               |          | rkit-daemon                                      |
| <input type="checkbox"/> severity              |          | 7                                                |
| <input type="checkbox"/> severity_label        |          | Debug                                            |
| <input type="checkbox"/> timestamp             |          | Mar 31 19:30:46                                  |
| <input checked="" type="checkbox"/> type       |          | syslog                                           |

- Aquí podemos ver las estadísticas del sistema del Admin.

Nagios® LS

Inicio Dashboards Informes alertando Configurar Ayuda Admin

Registros de búsqueda ... nagiosadmin

+ agregar un origen de registro Identificación del clúster | 151637cd-54fe-453d-8fd6-ba1398:

### informes

registro de auditoría

### Sistema

- estado del clúster
- estado de instancia
- estado del índice
- instantáneas y mantenimiento
- Estado del sistema
- Comandos del subsistema

### administración

- Gestión de usuarios
- gestión de la lista de host
- ldap / integración de anuncios
- monitor de backend (nopa)
- personalizado incluye

### general

- Opciones generales
- Configurar opciones de correo
- Información de la licencia
- Configuración del servidor proxy

servidor de registro nagios 2.1.5 • Actualizaciones automáticas disponibles Acerca de | Legal | Copyright © 2014-2020 empresas nagios, LLC

**estado del clúster**

**Estadísticas de sistema**

|                       |                          |
|-----------------------|--------------------------|
| 5,754 documentos      | 1.7MB tamaño de primaria |
| 1.7MB tamaño total    | 1 instancias de datos    |
| 42 fragmentos totales | 5 índices                |

**salud clúster**

|                              |        |
|------------------------------|--------|
| Estado                       | Yellow |
| caducado?                    | false  |
| # instancias                 | 1      |
| # Instancias de datos        | 1      |
| fragmentos primarios activos | 21     |
| fragmentos activos           | 21     |
| la reubicación de fragmentos | 0      |
| initializar fragmentos       | 0      |
| fragmentos sin asignar       | 21     |

**índices**

| índice              | # docs | tamaño de primaria | # fragmentos | # réplicas | Acciones       |
|---------------------|--------|--------------------|--------------|------------|----------------|
| logstash-2020.03.31 | 3,292  | 925.7KB            | 5            | 1          | Borrar         |
| logstash-2020.03.24 | 2,347  | 537.2KB            | 5            | 1          | Cerrar  Borrar |

- Aquí podemos ver la cantidad de registros.



- Para gestionar los usuarios:

**Nagios® LS**

Inicio Dashboards Informes alertando Configurar Ayuda Admin

Registros de búsqueda ... nagiosadmin

**Gestión de usuarios**

+ crear usuario agregar usuarios de LDAP / AD

| Usuario                            | Email                     | nivel de acceso | Tipo de cuenta | Acceso api | Acciones |
|------------------------------------|---------------------------|-----------------|----------------|------------|----------|
| nagiosadmin (Nagios Administrator) | a_angbongom@iestriana.com | Admin           | local          | Si         |          |

**crear usuario**

por favor rellene todos los campos de la nueva información de los usuarios a continuación. campos con estrellas se requieren

**detalles** **autenticación externa** **Permisos**

**Detalles de usuario**

**nombre completo:**  \*

**Email:**  \*

**Información de la cuenta**

**Usuario:**  \*

**Password:**  \*

**Confirmar contraseña:**  \*

**Idioma:**  ▾

**crear usuario** **Cancelar**

- Para gestionar las alertas:

### crear una alerta

**Nombre de alerta**

**Tipo**

**Query**  ?

**comprobar intervalo**  ?

**periodo retroactivo**  ?

**umbrales**    ?

**Metodos de notificación**  ?

**crear el alerta** **Cancelar**

- Configuración global.

**Configuración global**

administrar las opciones de configuración logstash que se agregarán a todas las instancias. tenga en cuenta que todos los filtros globales aplicadas sucederán antes de que los filtros locales. tener en cuenta el flujo de los datos de registro a través de los filtros al crear filtros globales. [documentación lingüística config vista logstash](#)

guardar    guardar y aplicar    verificar    Vistas ▾

+ agregar un origen de registro    mostrar salidas

+ añadir la entrada ▾    + añadir filtro ▾

**entradas**

ne necesita puertos <1024?

- Activo Syslog (Default)
- Activo Windows Event Log (Default)
- Activo Import Files - Raw (Default)
- Activo Import Files - JSON (Default)

**filtros**

- Activo Apache (Default)
- Activo XI Audit Log

alertas en tiempo real (solo lectura)

filtros      Resultado

## Capítulo 15

### Nagios Network Analyzer.

#### Paso 1. Qué es, características.

- Nagios Network Analyzer le permite ser proactivo en la solución de fallas, detectar comportamiento anormal y amenazas de seguridad, antes de que afecten los procesos críticos del negocio.
- Nagios Network Analyzer proporciona el tráfico de red y la información de la banda ancha para toda la infraestructura de TI, lo que hace que sea más fácil para los usuarios y equipos garantizar que los sistemas, aplicaciones, servicios y procesos del negocio estén funcionando correctamente.
  - Beneficios:
    - Análisis de WAN: El analizador de Red ofrece un análisis profundo de todas las fuentes de tráfico de red y amenazas potenciales de seguridad que permite a los administradores del sistema recopilar rápidamente información de alto nivel en relación a la salud de la red, así como datos para el análisis de la red completa y exhaustiva.
    - Diseño intuitivo: Con una interfaz web potente e intuitiva, Nagios Network Analyzer es fácil de usar; Network Analyzer se integra perfectamente con nuestra solución de monitorización de red Nagios XI, permite la consolidación de alertas y notificaciones, así como el mantenimiento de la red manteniéndola protegida y segura; con el

asistente de Network Analyzer la configuración se encuentra lista con solo unos clics.

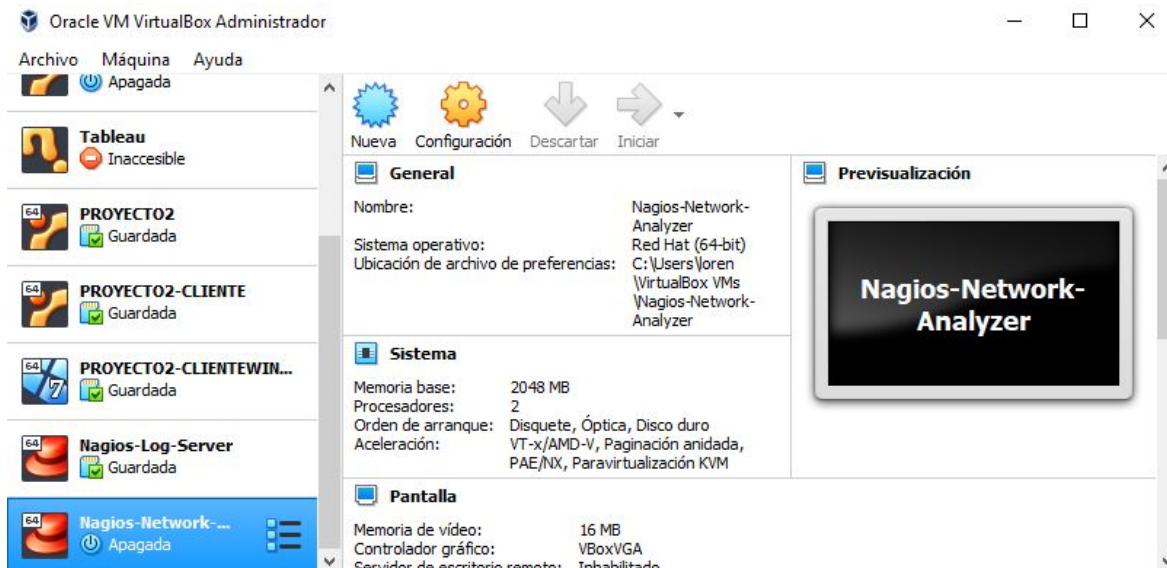
- Claridad en la red: Nagios Network Analyzer proporciona una vista central de su tráfico de red y ancho de banda. Su potente panel de control proporciona una vista del flujo de red o fuentes críticas, métricas del sistema y comportamiento anormal de la red para una rápida evaluación de salud de la red. Los usuarios pueden acceder fácilmente a la información específica sobre IP individuales, puertos de origen, puertos destinos o cualquier combinación de los mismos.
- Análisis profundo: Nagios Network Analyzer proporciona al personal de TI alertas e informes avanzados, altamente granular de su red, generando paquetes de datos que son archivados para su futuro análisis. Cuando se superan los umbrales críticos, se presenta una actividad anormal de la red o se cumplen las restricciones de ancho de banda, Nagios Network Analyzer puede activar alertas que permitan a los administradores actuar de manera inmediata en la resolución de problemas.
- Calculadora de utilización de ancho de banda: Ésta es totalmente personalizable y está incluida. Permite crear informes para resumir la utilización del ancho de banda por la fuente, IP o cualquier combinación que desee el usuario.

- Características:

- Cuadro de instrumentos integral: El tablero de instrumentos proporciona una descripción de alto nivel de las fuentes, los chequeos, los datos de flujo de red y mucho más.
- Fiabilidad y seguridad: Networks Analyzer es capaz de alertar a los usuarios cuando se llevan a cabo actividades sospechosas en la red.
- Vistas avanzadas: Las vistas avanzadas proporcionan ideas rápidas a profundidad sobre el tráfico de red, ancho de banda y la salud general de la red.
- Monitoreo de aplicaciones personalizadas: Consultas individualizadas, vistas e informes que dan la posibilidad de controlar el uso de la red de aplicaciones específicas.
- Vistas especializadas: Mantenga un registro específico del flujo de información en la red y mantenga un historial de su flujo de datos de la red.
- Sistema de alarmas automáticas: Reciba alertas cuando exista una actividad anormal en su red o cuando el uso de banda ancha exceda los umbrales especificados.
- Gestión de usuarios: Capacidades multi- tenancy permiten a los equipos de TI para trabajar juntos de manera eficiente para mantener la red funcionando sin problemas.

## Paso 2. Elementos vistos en la práctica.

- Nos descargamos la ova de la página oficial de Nagios.



- Nos registramos con el usuario root y la contraseña nagiosna.



- Procedemos a llenar los datos convenientes e instalamos.

**Final Installation Steps**

Almost done! Update the license and configure the admin account.

**License Setup**

Choose a trial license, enter your key, or [get a license now](#).

Free 30 Day Trial    I already have a key

License Key:

**Admin Account Setup**

Choose or enter your admin profile and account settings. The default username is nagiosadmin, which you can change.

Username\*:

Password\*:

Confirm Password:

Email:

Address:

Language:

System Timezone:

**Finish Installation >**

- Entramos como nagiosadmin y la contraseña elegida anteriormente.

**Nagios®**  
Network Analyzer™

**Log In**

Installation Complete!

Keep me logged in

**Log In**      [Forgot your password?](#)

- En la página principal podemos ver el tablero, que nos hace una descripción de alto nivel de las fuentes, los chequeos, los datos de flujo de red y mucho más.

The screenshot shows the Nagios Network Analyzer dashboard at the URL 192.168.1.138/nagiosna/. The top navigation bar includes links for Tablero, Fuentes, Grupos de origen, Puntos de vista, Informes, Consultas, Alerta, Ayuda, Administración, and Cerrar sesión. The main content area is divided into several sections:

- Fuentes fijadas (Ver todo):** A table showing two fixed sources: "cliente-VirtualBox" and "clientew-PC". Each entry includes a green checkmark icon, the source name, traffic status ("El tráfico dura 30 minutos"), disk usage ("Uso del disco"), useful life ("Vida útil de los datos"), and flow type ("Tipo de flujo").
- Resumen de alerta:** A section showing alert summaries: "Todas (0)", "De acuerdo (0)", "Advertencia (0)", and "Criticó (0)". It includes fields for "Verificar nombre", "Estado", "Ver mensaje", and "Comportamiento". A note says "No entrar".
- Comportamiento anormal:** A timeline from 18:10 to 19:00 showing abnormal behavior for two sources: "cliente-VirtualBox" and "cliente-VirtualBox". The timeline is highlighted in green.
- Información del estado:** A modal window for "cliente-VirtualBox" at 18:55. It states "La fuente parece estar informando el ancho de banda normal." and lists "Información de marco de tiempo" items: Consulta, Puerto superior fuente parlante, Fuente de conversación superior IP, Puerto superior de destino parlante, and Top Talking Destination IP. The timeline for this source is also highlighted in green.

- Aquí vemos las fuentes que hemos añadido e informes sobre ellas.

The screenshot shows the "Fuentes" (Sources) page of the Nagios Network Analyzer. The top navigation bar is identical to the dashboard. The main content area includes:

- A header "Fuentes" with a "Crear fuente" button and a search bar "Buscar por nombre de fuente" with a magnifying glass icon.
- A note: "Lista completa de todas las fuentes en su sistema. Solo se muestran las fuentes visibles."
- A table listing two sources: "cliente-VirtualBox" and "clientew-PC". Each row includes a green checkmark icon, the source name, traffic status ("El tráfico dura 30 minutos"), disk usage ("Uso del disco"), useful life ("Vida útil de los datos"), flow type ("Tipo de flujo"), port number ("Port"), and actions ("Comportamiento").

The screenshot shows the Network Analyzer interface. At the top, there's a navigation bar with tabs like 'Tablero', 'Fuentes', 'Grupos de origen', 'Puntos de vista', 'Informes', 'Consultas', and 'Alerta'. On the right, it shows the email 'a\_angbongom@estriana.com'. Below the navigation, a breadcrumb trail reads 'Fuentes / Fuente - cliente-VirtualBox / Informes'. The main title is 'Fuente - cliente-VirtualBox'. A status bar indicates the source is 'Corriendo (PID: 9555)' with buttons for 'Detener' and 'Reiniciar'. Below this, there are tabs for 'Resumen', 'Informes' (which is selected), 'Consultas', and 'Calculadora de percentiles'. A search bar says 'Top 5 Talkers By Source IP (Last 24 Hours) \*'. To the right are buttons for 'Sacar un reporte', 'PDF', 'Administrar vistas', 'Editar', and 'Retirar'. The main content area features a large circular chart labeled 'Gráfico circular' and three smaller boxes labeled 'srcip <=> dstip', 'srcip <=> srcport', and 'srcip <=> dstport'. Below this is a section titled 'Top 5 Talkers By Source IP (Last 24 Hours)' with a note about showing the top 5 talkers over the last 24 hours. It includes buttons for 'API externa' and 'Usar a través de HTTP'.

- Para crear fuentes estos son los datos que hay que proporcionar.

## Crear fuente

Cuando agregue una nueva fuente, asegúrese de configurar la fuente para enviar datos de flujo a su dirección IP de instalación NNA en el puerto que especifique a continuación para recibir datos.

The configuration page for creating a new source. It includes the following fields:

- Nombre de la fuente\***: A text input field for the source name, with a note below stating it should be unique and associated with the flow collector device.
- Dirección (es) IP del remitente:** A text input field for the source IP, with a note below stating it's optional and used for internal tracking of sending devices.
- Puerto de escucha\*:** A text input field for the listening port, with a note below stating it must be unique and specified in the NetFlow configuration.
- Tipo de flujo entrante:** A dropdown menu set to 'NetFlow' with a note below explaining its use with specific devices.
- Datos brutos de por vida:** A dropdown menu set to '24 Horas' with a note below explaining the recommended storage period.
- Ajustes avanzados**: A link to advanced settings.
- Checkboxes**: Options to disable abnormal behavior controls and enable advanced settings.
- Buttons**: 'Crear fuente' (Create source) and 'Cancelar' (Cancel).

- En esta parte podemos apreciar los grupos creados y cómo crearlos.

**Nagios®**  
Network Analyzer™

Administración nagiosadmin  
a\_angbongom@lestiana.com

Tablero Fuentes Grupos de origen Puntos de vista Informes Consultas Alerta Ayuda Administración Cerrar sesión

Grupos de origen

## Grupos de origen

Lista completa de grupos fuente en su sistema. Los grupos de origen pueden constar de varias fuentes y actuar como una única fuente para fines de contabilidad de datos y una fuente puede estar en múltiples grupos de origen.

| Nombre del grupo de origen | Fuentes en grupo                                           | Comportamiento         |
|----------------------------|------------------------------------------------------------|------------------------|
| All Sources                | cliente-VirtualBox, clientew-PC                            |                        |
| Cientes                    | cliente-VirtualBox, clientew-PC ( <a href="#">Cambio</a> ) | <a href="#">Borrar</a> |

[Crear grupo de origen](#) Buscar por nombre del grupo de ori

## Crear grupo de origen

Tendrá que agregar uno o más fuente (s) a un grupo de origen. Complete toda la información a continuación.

Nombre del grupo de origen\*:

**Fuentes disponibles**

- cliente-VirtualBox
- clientew-PC

**Fuentes en grupo**

**Datos brutos de por vida:** La misma duración que la fuente con el tiempo de vida de los datos brutos más cortos.

[Crear grupo de origen](#) [Cancelar](#)

- Los informes guardados que podemos ejecutar.

**Nagios®**  
Network Analyzer™

Administración nagiosadmin  
a\_angbongom@iestriana.com

Tablero Fuentes Grupos de origen Puntos de vista **Informes** Consultas Alerta Ayuda Administración Cerrar sesión

Informes

## Informes

Una lista de todos los informes guardados que puede ejecutar. Estos informes se pueden ejecutar en cualquier origen, grupo de origen o vista.

Borrar Crear reporte Buscar por nombre de informe

| Reportar nombre                                              | Comportamiento |
|--------------------------------------------------------------|----------------|
| (Estático) Top 5 Talkers By Source IP (Last 24 Hours)        | correr         |
| (Estático) Top 5 Talkers By Destination IP (Last 24 Hours)   | correr         |
| (Estático) Top 5 Talkers By Source Port (Last 24 Hours)      | correr         |
| (Estático) Top 5 Talkers By Destination Port (Last 24 Hours) | correr         |

- La consultas guardadas que pueden ser ejecutadas, editadas o borradas.

**Nagios®**  
Network Analyzer™

Administración nagiosadmin  
a\_angbongom@iestriana.com

Tablero Fuentes Grupos de origen Puntos de vista Informes Consultas Alerta Ayuda Administración Cerrar sesión

Consultas

## Consultas

Una lista de todas sus consultas guardadas. Puede editarlos, eliminarlos o ejecutarlos en una fuente seleccionada.

Borrar Crear consulta Búsqueda por nombre de consulta

| Nombre de consulta | Descripción                                     | Comportamiento           |
|--------------------|-------------------------------------------------|--------------------------|
| Common Botnets     | Aggregation of the most common ips for botnets. | correr • Editar • Borrar |
| P2P Traffic        | Aggregation of some common P2P traffic ports.   | correr • Editar • Borrar |

- El apartado de administración donde podremos ver varios tipos de información además de gestionar los usuarios.

**Nagios®**  
Network Analyzer™

Administración [nagiosadmin](#)  
[a\\_angbongom@estriana.com](#)

Tablero Fuentes Grupos de origen Puntos de vista Informes Consultas Alerta Ayuda Administración Cerrar sesión

Administración

**CUADROS DE MANDOS**

**Tablero del sistema**

GENERAL  
[Ajustes globales](#)  
[Buscar actualizaciones](#)

AUTENTICACIÓN  
[Gestión de usuarios](#)  
[Integración LDAP / AD](#)

LICENCIA  
[Actualizar licencia](#)

APOYO  
[Respaldo del sistema](#)

## Tablero del sistema

Carga de la CPU del servidor %

UPC

Uso del disco %

Disco

Uso de memoria %

Memoria

Intercambio de uso %

Intercambiar

| Nombre             | Uso  | Estado |
|--------------------|------|--------|
| cliente-VirtualBox | 1.3M |        |
| clientew-PC        | 1.3M |        |

## Capítulo 16

### Total de dispositivos monitorizados

**Nagios®**

**General**

- Home Documentation

**Current Status**

- Tactical Overview
- Map (Legacy)
- Hosts
- Services
- Host Groups
  - Summary
  - Grid
- Service Groups
  - Summary
  - Grid
- Problems
  - Services (Unhandled)
  - Hosts (Unhandled)
  - Network Outages
- Quick Search:

**Reports**

- Availability
- Trends (Legacy)
- Alerts
  - History
  - Summary
  - Histogram (Legacy)

**Host Status Totals**

|              |           |             |         |
|--------------|-----------|-------------|---------|
| Up           | Down      | Unreachable | Pending |
| 7            | 0         | 0           | 0       |
| All Problems | All Types |             |         |
| 0            | 7         |             |         |

**Service Status Totals**

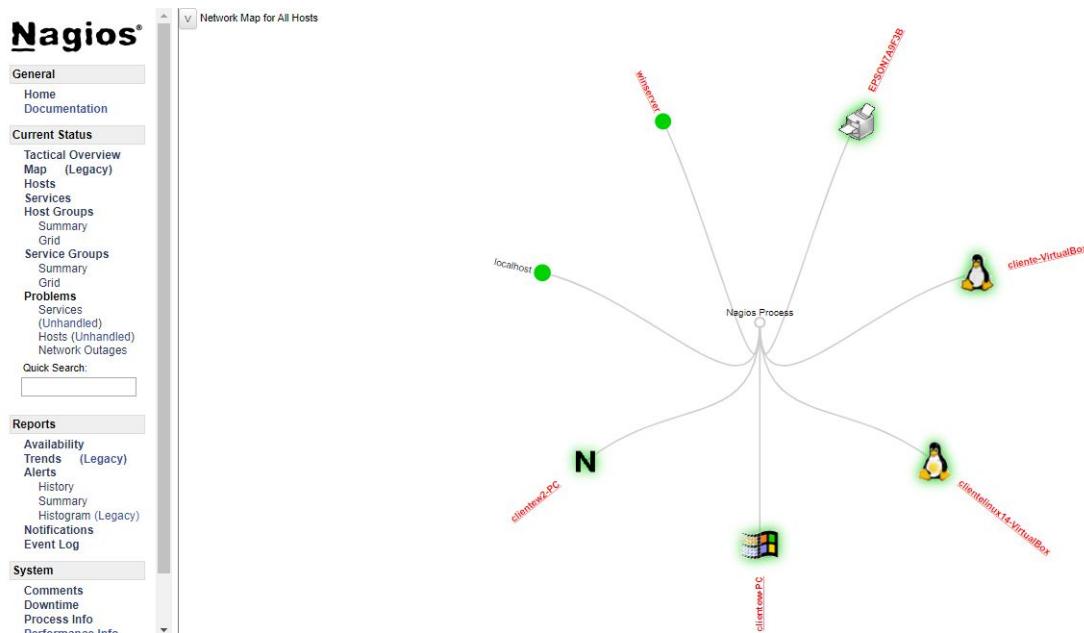
|              |           |         |          |         |
|--------------|-----------|---------|----------|---------|
| Ok           | Warning   | Unknown | Critical | Pending |
| 29           | 2         | 0       | 16       | 0       |
| All Problems | All Types |         |          |         |
| 18           | 47        |         |          |         |

**Host Status Details For All Host Groups**

Limit Results: 100 ▾

| Host                      | Status | Last Check          | Duration      | Status Information                        |
|---------------------------|--------|---------------------|---------------|-------------------------------------------|
| EPSON7A9F3B               | UP     | 04-28-2020 20:02:05 | 0d 0h 31m 21s | PING OK - Packet loss = 0%, RTA = 1.20 ms |
| cliente-VirtualBox        | UP     | 04-28-2020 19:59:43 | 0d 0h 13m 43s | PING OK - Packet loss = 0%, RTA = 0.96 ms |
| clientelinux14-VirtualBox | UP     | 04-28-2020 20:03:08 | 0d 0h 10m 18s | PING OK - Packet loss = 0%, RTA = 1.01 ms |
| clientew-PC               | UP     | 04-28-2020 19:59:46 | 0d 0h 34m 18s | PING OK - Packet loss = 0%, RTA = 1.21 ms |
| clientew2-PC              | N      | 04-28-2020 19:59:08 | 0d 0h 51m 52s | PING OK - Packet loss = 0%, RTA = 0.87 ms |
| localhost                 | UP     | 04-28-2020 20:02:29 | 0d 1h 25m 57s | PING OK - Packet loss = 0%, RTA = 0.09 ms |
| winserver                 | UP     | 04-28-2020 19:59:22 | 0d 1h 34m 22s | PING OK - Packet loss = 0%, RTA = 0.08 ms |

Results 1 - 7 of 7 Matching Hosts



## Lista de referencias

Rahul. (2020). How to Install Nagios 4.4 on Ubuntu 18.04 & 16.04 LTS.

<https://tecatadmin.net/install-nagios-monitoring-server-on-ubuntu/>

Rahul. (2017). How to Monitor Remote Linux Host using Nagios and NRPE.

<https://tecatadmin.net/monitor-remote-linux-host-using-nagios/>

Rahul. (2019). How to Monitor Remote Windows Host using Nagios.

<https://tecatadmin.net/monitor-remote-windows-host-using-nagios/>

Albert Esquís. (2019). Instalación de Nagios Core 4.4.1 en servidor Ubuntu 18.04.

<https://www.esquis.net/instalacion-de-nagios-core-4-4-1-en-servidor-ubuntu-18-04/>

Foxmclaud. (2013). Nagios - Añadir iconos en el mapa.

<http://asircierva.blogspot.com/2013/04/nagios-anadir-iconos-en-el-mapa.html>

(2020). Nagios. <https://es.wikipedia.org/wiki/Nagios>

Xpert. (2020). Nagios Network Analyzer.

<http://www.xpertic.com.mx/monitoreo/nagiosnetworkanalyzer>

Nagios. (2019). Nagios Log Server - Manual Installation Instructions

<https://assets.nagios.com/downloads/nagios-log-server/docs/Manual-Installation-Instructions-For-Nagios-Log-Server.pdf>

Juanlu Ramirez. (2016). Monitorizacion de sistema y redes con Nagios.

<https://www.juanluramirez.com/monitorizacion-sistema-nagios/>

Nagiosvideo. (2017). Configuring Devices & Applications in Nagios Log Server 2.

<https://www.youtube.com/watch?v=jB5CdNCUuPQ>

Nagiosvideo. (2017). Adding a new instance to a Nagios Log Server Cluster.

[https://www.youtube.com/watch?v=guWROkZ05Ag&list=PLN-ryIrpC\\_mBEiOuZ1J9OOBoWF8TmSA3R](https://www.youtube.com/watch?v=guWROkZ05Ag&list=PLN-ryIrpC_mBEiOuZ1J9OOBoWF8TmSA3R)

Nagiosvideo. (2017). Administering Log Server 2 Snapshots & Maintenance.

[https://www.youtube.com/watch?v=oXYZKwsetXo&list=PLN-ryIrpC\\_mBEiOuZ1J9OOBoWF8TmSA3R&index=4](https://www.youtube.com/watch?v=oXYZKwsetXo&list=PLN-ryIrpC_mBEiOuZ1J9OOBoWF8TmSA3R&index=4)

Nagiosvideo. (2017). Monitor Your Log Server Instances - Pro Tip.

[https://www.youtube.com/watch?v=cYUduX5qQTw&list=PLN-ryIrpC\\_mBEiOuZ1J9OOBoWF8TmSA3R&index=5](https://www.youtube.com/watch?v=cYUduX5qQTw&list=PLN-ryIrpC_mBEiOuZ1J9OOBoWF8TmSA3R&index=5)

Jorge. (2017). Configurar alertas de correo en Nagios.

<https://nksistemas.com/configurar-alertas-de-correo-en-nagios/>

Maslinux (2018) CÓMO CONFIGURAR UNA DIRECCIÓN IP ESTÁTICA EN UBUNTU 18.04. <https://maslinux.es/como-configurar-una-direccion-ip-estatica-en-ubuntu-18-04/>

El Respondón (2020) ¿Cómo configurar Dirección IP Estática o Fija en Linux/Ubuntu?

<https://elrespondon.com/como-configurar-direccion-ip-fija-linux-ubuntu/>

Sergio De Luz (2010). Cómo establecer una IP privada fija en Windows 7

<https://www.redeszone.net/windows/ip-privada-fija-en-windows-7/>

Francesc (2017). Error Nagios: CRITICAL Socket timeout after 10 seconds.

<https://www.solvetic.com/topic/5874-error-nagios-critical-socket-timeout-after-10-seconds/>

Kwhogster (2015) NSClient - ERROR: Invalid password.

<https://support.nagios.com/forum/viewtopic.php?t=35386>

Sugupedia (2015) Sistema de monitorización: NAGIOS.

[https://sugus.eii.us.es/sugupedia/index.php/Sistema\\_de\\_monitorizaci%C3%B3n:\\_NAGIOS](https://sugus.eii.us.es/sugupedia/index.php/Sistema_de_monitorizaci%C3%B3n:_NAGIOS)

Javier Orovengua (2014). Añadir Windows al servidor de Monitorización Nagios.

<https://www.linux-party.com/106-nagios/9086-anadir-windows-al-servidor-de-monitorizacion-nagios>

jbruyet (2012). My host statuses are DOWN but check\_ping shows they're up.

<https://support.nagios.com/forum/viewtopic.php?f=7&t=6050>

Aparna (2005). Warning threshold must be float or float triplet!

<https://forums.meulie.net/t/warning-threshold-must-be-float-or-float-triplet/1525/4>

box293 (2015). check\_users not correctly detecting thresholds.

<https://github.com/nagios-plugins/nagios-plugins/issues/81>

Marcos Rodríguez. NAGIOS MYSQL: Monitorizar en Ubuntu 14.04

<https://vivaubuntu.com/nagios-mysql-monitorizar-ubuntu-14-04/>

Reynierpm (2015). MariaDB/MySQL health plugin for Nagios Core?

<https://support.nagios.com/forum/viewtopic.php?f=7&t=34507>

Israel (2009). Monitoreando Impresoras de Red.

<http://nagioses.blogspot.com/2009/03/monitoreando-impresoras.html>

koromicha (2018). Install and Configure SNMP on Ubuntu 18.04 and CentOS 7.

<https://kifarunix.com/install-and-configure-snmp-ubuntu-18-04-and-centos-7/>

Stickboy (2008). check\_hpjd not installed.

<https://forums.meulie.net/t/check-hpjdf-not-installed/3723>

Frank (2014). Construyendo plugins para Nagios Parte 2 de 2 (Twitter).

<https://www.soluciones-im.com/blogs/tecnologia/construyendo-plugins-para-nagios-parte-2-de-2-twitter/>

WikiEtl (2017). Nagios. <https://www.etl.it.uc3m.es/Nagios>