

Monitorización de hosts, servicios e redes: Nagios

ESCENARIO

Máquinas virtuais:

RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado

Rede: 192.168.120.0/24

Máquina virtual A:

Rede: Interna(eth0) + NAT(eth1)

Servidor Web: Apache (apache2)
Servidor Nagios + Plugins Nagios

Máquina virtual B:

Rede: Interna(eth0) + NAT(eth1)

Cliente Web: Navegador (firefox)
Plugins Nagios

Cliente NRPE: nagios-nrpe-plugin

Servidor NRPE: nagios-nrpe-server (5666)

Servidor Web (apache2)

Servidor SSH (openssh-server)

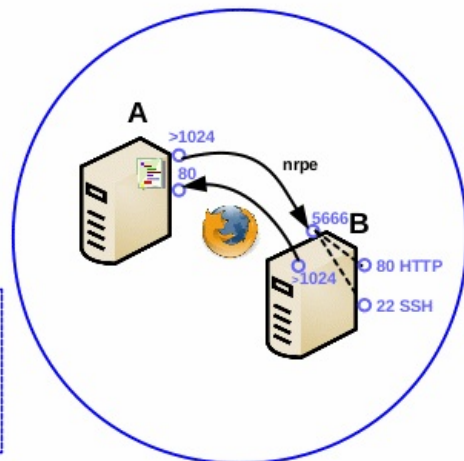
ISO: Kali Live amd64

IP/MS: 192.168.120.100/24

BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

ISO: Kali Live amd64

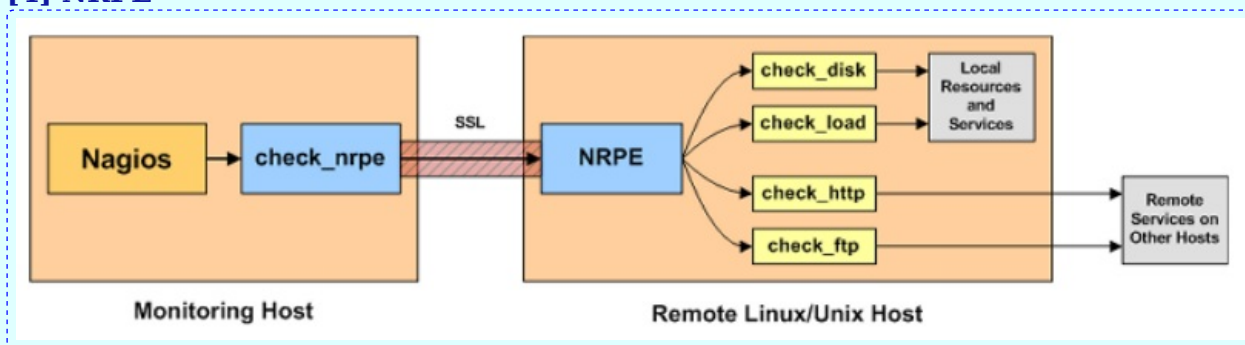
IP/MS: 192.168.120.101/24



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTAS:

- Prerrequisito: [HTTP Basic: Apache](#)
- [\[1\] Linux Monitoring With Nagios](#)
- [\[2\] Documentación Nagios](#)
- [\[3\] Debian Easy Guide Installation](#)
- [\[4\] NRPE](#)



Máquina virtual A: Kali amd64

1. Na contorna gráfica abrir un terminal e executar:

```
kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
```

```
kali@kali:~$ passwd kali #Cambiar o contrasinal do usuario kali. Por como contrasinal abc123. (Olo que o contrasinal ten un caracter punto final).
```

2. Cambiar hostname da máquina virtual A. Por kaliA como hostname:

```
kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
```

```
root@kali:~# echo 'kaliA' > /etc/hostname #Indicar ao sistema o valor do hostname.
```

```
root@kali:~# echo 'kernel.hostname=kaliA' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
```

```
root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
```

```
root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
```

```
kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario kali.
```

3. Configurar a rede:

Na contorna gráfica abrir un terminal e executar:

```
kali@kaliA:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
```

```
kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
```

```
root@kaliA:~# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflito con este demo.
```

```
root@kaliA:~# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar de forma manual a configuración de rede e non ter conflito con este xestor.
```

```
root@kaliA:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo) e interna(eth0).
```

```
root@kaliA:~# ip addr add 192.168.120.100/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.100 e máscara de subrede: 255.255.255.0.
```

```
root@kaliA:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo) e interna(eth0).
```

```
root@kaliA:~# ping -c4 192.168.120.100 #Comprobar mediante o comando ping a conectividade coa interface de rede local eth0
```

Máquina virtual B: Kali amd64

4. Configuración da rede. Na contorna gráfica abrir un terminal e executar:

```
kali@kali:~$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
```

```
kali@kali:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
```

```
root@kali:~# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflito con este demo.
```

```
root@kali:~# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar de forma manual a configuración de rede e non ter conflito con este xestor.
```

```
root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina B as tarxetas de redes: loopback(lo) e interna(eth0).
```

```
root@kali:~# ip addr add 192.168.120.101/24 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 192.168.120.101 e máscara de subrede: 255.255.255.0.
```

```
root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina B as tarxetas de redes: loopback(lo) e interna(eth0).
```

```
root@kali:~# ping -c4 192.168.120.101 #Comprobar mediante o comando ping a conectividade coa interface de rede local eth0
```

```
root@kali:~# ping -c4 192.168.120.100 #Comprobar mediante o comando ping a conectividade coa interface de rede da máquina virtual A
```

```
root@kali:~# echo '192.168.120.100 kaliA' >> /etc/hosts #Engadir no ficheiro /etc/hosts, é dicir, na táboa estática de búsqueda para nomes de host (DNS) o nome kaliA, para que atenda á IP 192.168.120.100
```

```
root@kali:~# ping -c4 kaliA #Comprobar mediante o comando ping a conectividade coa interface de rede da máquina virtual A
```

5. Cambiar hostname da máquina virtual B. Por kaliB como hostname:

```
root@kali:~# echo 'kaliB' > /etc/hostname #Indicar ao sistema o valor do hostname.
```

```
root@kali:~# echo 'kernel.hostname=kaliB' >> /etc/sysctl.conf #Indicar ao kernel o valor do hostname.
```

```
root@kali:~# sysctl -p #Activar o cambio de hostname sen ter que pechar sesión nin reiniciar
```

```
root@kali:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
```

```
kali@kali:~$ exit #Pechar o terminal saíndo da consola local do usuario kali.
```

6. **kaliA → Instalar Nagios (Motor GUI Web + Servidor Nagios):** Realizar o procedemento descrito en [3]. Basicamente:

A. Procedemento instalación nagios-core (Motor GUI Web + Servidor Nagios)

```
kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co
comando sudo (/etc/sudoers, visudo)
root@kaliA# apt-get update
root@kaliA# apt-get install -y autoconf gcc libc6 make wget unzip apache2 apache2-utils
php libgd-dev
root@kaliA# cd /tmp
root@kaliA# wget -O nagioscore.tar.gz
https://github.com/NagiosEnterprises/nagioscore/archive/nagios-4.4.6.tar.gz
root@kaliA# tar xzf nagioscore.tar.gz
root@kaliA# cd /tmp/nagioscore-nagios-4.4.6/
root@kaliA# ./configure --with-httpd-conf=/etc/apache2/sites-enabled
root@kaliA# make all
root@kaliA# make install-groups-users
root@kaliA# usermod -a -G nagios www-data
root@kaliA# make install
root@kaliA# make install-daemoninit
root@kaliA# make install-commandmode
root@kaliA# make install-config
root@kaliA# make install-webconf
root@kaliA# a2enmod rewrite
root@kaliA# a2enmod cgi
root@kaliA# htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
root@kaliA# systemctl restart apache2.service
root@kaliA# systemctl start nagios.service
```

NOTA: No comando htpasswd solicítase un contrasinal para o usuario **nagiosadmin**. Imos pór como contrasinal **abc123**. (Olo que o contrasinal ten un carácter punto final)

Comandos

```
apt-get update
apt-get install -y autoconf gcc libc6 make wget unzip apache2 apache2-utils php libgd-dev
cd /tmp
wget -O nagioscore.tar.gz https://github.com/NagiosEnterprises/nagioscore/archive/nagios-4.4.6.tar.gz
tar xzf nagioscore.tar.gz
cd /tmp/nagioscore-nagios-4.4.6/
./configure --with-httpd-conf=/etc/apache2/sites-enabled
make all
make install-groups-users
usermod -a -G nagios www-data
make install
make install-daemoninit
make install-commandmode
make install-config
make install-webconf
a2enmod rewrite
a2enmod cgi
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
systemctl restart apache2.service
systemctl start nagios.service
```

B. Procedemento instalación nagios-plugins (plugin → permite monitorizar recursos)

```
root@kaliA# apt-get install -y autoconf gcc libc6 libmcrypto-dev make libssl-dev wget bc
gawk dc build-essential snmp libnet-snmp-perl gettext
root@kaliA# cd /tmp
root@kaliA# wget --no-check-certificate -O nagios-plugins.tar.gz
https://github.com/nagios-plugins/nagios-plugins/archive/release-2.3.3.tar.gz
root@kaliA# tar xzf nagios-plugins.tar.gz
root@kaliA# cd /tmp/nagios-plugins-release-2.3.3/
root@kaliA# ./tools/setup
root@kaliA# ./configure
root@kaliA# make
root@kaliA# make install
root@kaliA# systemctl restart nagios.service
root@kaliA# exit
kali@kaliA:~$
```

Comandos

```
apt-get install -y autoconf gcc libc6 libmcrypto-dev make libssl-dev wget bc gawk dc build-essential snmp
libnet-snmp-perl gettext
cd /tmp
wget --no-check-certificate -O nagios-plugins.tar.gz https://github.com/nagios-plugins/nagios-
plugins/archive/release-2.3.3.tar.gz
tar xzf nagios-plugins.tar.gz
cd /tmp/nagios-plugins-release-2.3.3/
./tools/setup
./configure
make
make install
systemctl restart nagios.service
exit
```

Verificar

7. **kaliB → URL <http://kaliA/nagios>**: Lanzar na máquina virtual B (Kali) un navegador e visitar a URL <http://kaliA/nagios>

- Menú lateral esquerdo → Hosts
- Menú lateral esquerdo → Services

NRPE

8. **kaliB → Instalar o servidor nagios NRPE[4]:** Permite executar nagios-plugin nos hosts clientes a monitorizar por Nagios

```
kali@kaliB:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
```

```
root@kaliB:~# apt-get update
root@kaliB:~# apt-get install -y nagios-nrpe-server
root@kaliB:~# sed -i -e
's/allowed_hosts=127.0.0.1,::1/allowed_hosts=127.0.0.1,::1,192.168.120.100/' -e
's/hda1/sda1/g' /etc/nagios/nrpe.cfg
root@kaliB:~# /etc/init.d/nagios-nrpe-server status
root@kaliB:~# /etc/init.d/nagios-nrpe-server start
root@kaliB:~# /etc/init.d/nagios-nrpe-server status
root@kaliB:~# netstat -natp | grep -i nrpe
root@kaliB:~# ps -ef | grep -i [n]rpe
```

9. **kaliA → Instalar cliente NRPE no Servidor Nagios[4]:** Plugin NRPE para poder executar comandos nos clientes Nagios dende o servidor Nagios

```
kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
```

```
root@kaliA# apt-get update
root@kaliA# apt-get install -y nagios-nrpe-plugin
root@kaliA# /usr/lib/nagios/plugins/check_nrpe -H 192.168.120.101
NRPE v3.2.1
root@kaliA# cat > /tmp/command-nrpe.txt <<EOF
##### NRPE #####
define command {
    command_name    check_nrpe
    command_line     $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
}
EOF
root@kaliA# cat /tmp/command-nrpe.txt >>/usr/local/nagios/etc/objects/commands.cfg
root@kaliA# cd /usr/local/nagios/etc/objects/
root@kaliA# cat > kaliB.cfg <<EOF
define host{
    use linux-server
    host_name kaliB
    alias cliente
    address 192.168.120.101
}

define service{
    use generic-service
    host_name kaliB
    service_description CPU Load
    check_command check_nrpe!check_load
}

define service{
    use generic-service
    host_name kaliB
    service_description Current Users
    check_command check_nrpe!check_users
}

define service{
    use generic-service
    host_name kaliB
    service_description /dev/sda1 Free Space
    check_command check_nrpe!check_sda1
}
```

```

define service{
    use generic-service
    host_name kaliB
    service_description Total Processes
    check_command check_nrpe!check_total_procs
}

define service{
    use generic-service
    host_name kaliB
    service_description Zombies Processes
    check_command check_nrpe!check_zombie_procs
}
EOF

```

```

root@kaliA# echo 'cfg_file=/usr/local/nagios/etc/objects/kaliB.cfg' >>
/usr/local/nagios/etc/nagios.cfg
root@kaliA# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
root@kaliA# ln -s /usr/lib/nagios/plugins/check_nrpe /usr/local/nagios/libexec/check_nrpe
root@kaliA# systemctl restart nagios.service
root@kaliA# for i in $(grep check kaliB.cfg | awk -F'|' '{print $NF}' | xargs)
do
/usr/lib/nagios/plugins/check_nrpe -H 192.168.120.101 -c $i
done

```

```

CRITICAL - load average: 0.21, 0.26, 0.26|load1=0.210;0.150;0.300;0;
load5=0.263;0.100;0.250;0; load15=0.263;0.050;0.200;0;
PROCS CRITICAL: 262 processes | procs=262;150;200;0;
USERS OK - 2 users currently logged in |users=2;5;10;0
PROCS OK: 0 processes with STATE = Z | procs=0;5;10;0;
DISK OK - free space: /dev 1871 MB (100% inode=99%);|
/dev=0MB;1496;1683;0;1871

```

Verificar

10. **kaliB → URL <http://kaliA/nagios>:** Actualizar na máquina virtual B (Kali) a página referente á URL <http://kaliA/nagios>

- Menú lateral izquierdo → Hosts
- Menú lateral izquierdo → Services

11. **kaliB** → **Agregar servizos a chequear mediante NRPE[4]:**

```
kali@kaliB:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co
comando sudo (/etc/sudoers, visudo)
root@kaliB:~# echo 'command[check_http]=/usr/lib/nagios/plugins/check_http -H
127.0.0.1 -w 5 -c 10' >> /etc/nagios/nrpe.cfg
root@kaliB:~# echo 'command[check_ssh]=/usr/lib/nagios/plugins/check_ssh -H
127.0.0.1' >> /etc/nagios/nrpe.cfg
root@kaliB:~# /etc/init.d/nagios-nrpe-server restart
root@kaliB:~# /etc/init.d/nagios-nrpe-server status
```

12. **kaliA** → **Chequear os anteriores servizos mediante NRPE no Servidor Nagios[4]:**

```
kali@kaliA:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co
comando sudo (/etc/sudoers, visudo)
root@kaliA# cd /usr/local/nagios/etc/objects/
root@kaliA# cat >> kaliB.cfg <<EOF

define service{
    use generic-service
    host_name kaliB
    service_description Check HTTP Service
    check_command check_nrpe!check_http
}

define service{
    use generic-service
    host_name kaliB
    service_description Check SSH Service
    check_command check_nrpe!check_ssh
}
EOF
root@kaliA# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
root@kaliA# systemctl restart nagios.service
```

Verificar

13. **kaliB** → **URL <http://kaliA/nagios>**: Actualizar na máquina virtual B (Kali) a páxina referente á URL <http://kaliA/nagios>

- Menú lateral esquerdo → Hosts
- Menú lateral esquerdo → Services

14. **kaliB** → **Activar Servidor HTTP (Apache):**

```
kali@kaliB:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando
sudo (/etc/sudoers, visudo)
root@kaliB:~# nc -vz localhost 80 ; [ $(echo $?)-ne 0 ] && /etc/init.d/apache2 start #Verificar se o
servizo HTTP(Apache) está activo. Se non está activo, arráncase
root@kaliB:~# /etc/init.d/apache2 status #Comprobar o estado do servidor HTTP(Apache), agora debe estar
arrancado.
root@kaliB:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
kali@kaliB:~$
```

15. **kaliB** → **Activar Servidor SSH:**

```
kali@kaliB:~$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando
sudo (/etc/sudoers, visudo)
root@kaliB:~# nc -vz localhost 22 ; [ $(echo $?)-ne 0 ] && /etc/init.d/ssh start #Verificar se o
servizo SSH está activo. Se non está activo, arráncase
root@kaliB:~# /etc/init.d/ssh status #Comprobar o estado do servidor SSH, agora debe estar arrancado.
root@kaliB:~# exit #Saír da consola local sudo na que estabamos a traballar para voltar á consola local de kali.
kali@kaliB:~$
```


16. **kaliB** → **URL** <http://kaliA/nagios>: Actualizar na máquina virtual B (Kali) a páxina referente á URL <http://kaliA/nagios>

- Menú lateral esquerdo → Hosts
- Menú lateral esquerdo → Services

Ricardo Feijoo Costa



This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/)