Implantación servidor Nagios en Sistema Operativo Debian 11

Índice de contenidos

1. Instalación de Nagios

Una vez instalado el sistema operativo y configuradas las interfaces de red con IP manual, si se opera desde un equipo Windows se recomienda acceder a la línea de comandos del servidor Debian a través de SSH mediante el software putty (incluso en el caso de servidor en máquina virtual alojada en el propio equipo). También se recomienda el uso del software WinSCP para la transferencia de archivos al servidor.

1.1 Configuraciones previas

Se considera creado previamente en el sistema un usuario nagios y un grupo nagios al que pertenece dicho usuario, aunque es posible hacer esto con los comandos:

useradd nagios

groupadd nagios

usermod -a -G nagios nagios

También se considera que se está accediendo a la máquina con el usuario nagios, y no con root. Por tanto, para configurar el sistema será necesario ejecutar algunos comandos con privilegios de root en la cuenta. Para ello, habrá que instalar el comando sudo (si no lo está por defecto) y añadir el usuario nagios al grupo sudoers:

Cambiar a root conservando el entorno actual: su -

Instalar sudo:

apt update

apt install sudo -y

Añadir usuario nagios a grupo sudo: usermod -aG sudo nagios

Se puede verificar a qué grupos pertenece el usuario con el comando: id nagios

Cambiar de nuevo de root al usuario anterior (nagios): exit

Será necesario volver a hacer login con el usuario nagios para poder usar sudo.

Abrir los puertos http y https en el firewall. Para ello, se instalará la interfaz para iptables UFW:

sudo apt install ufw

Por defecto se permiten las conexiones salientes y se deniegan las entrantes, por ello si se está accediendo en remoto hay que hacer las configuraciones antes de habilitar UFW.

Se habilitan los puertos (SSH debería estar habilitado anteriormente para permitir la conexión remota, pero se indica también porque hay que volverlo a habilitar en UFW):

sudo ufw allow 22,80,443/tcp

(o el puerto configurado para SSH, si no se usa el 22 por defecto)

Habilitar UFW: **sudo ufw enable**

Comprobar el estado y las reglas activas: **sudo ufw status verbose**

Reiniciar el sistema: **sudo systemctl reboot**

1.2. Prerrequisitos

Actualizar repositorios y paquetes: **sudo apt-get update -y**

Para descargar vía web, descomprimir y otras utilidades:

sudo apt-get install wget gettext unzip

Para compilar e instalar paquetes: **sudo apt-get install gcc g++ automake autoconf make**

Instalación de paquetes de dependencias:

Perl: **sudo apt-get install perl libperl-dev libnet-snmp-perl curl net-tools**

SNMP: **sudo apt-get install snmp snmptrapd snmpd snmptt**

sudo apt install apache2 php libapache2-mod-php libssl-dev openssl

1.3. Usuarios y grupos

Añadir usuario apache al grupo nagios: **sudo usermod -a -G nagios www-data**

1.4. Descarga y desenpaquetado de plugins

Ir a la web: sudo y comprobar la última versión. Descargar los ficheros fuente de Nagios, en este caso:

Desde el home del usuario nagios:

wget https://github.com/NagiosEnterprises/nagioscore/releases/download/nagios-4.4.6/nagios-4.4.6.tar.gz

Descomprimir el fichero: **tar -xzvf nagios-4.4.6.tar.gz**

Hacer lo mismo para los ficheros fuente de los plugins de Nagios, disponibles en https://github.com/nagios-plugins/nagios-plugins/releases.

wget https://github.com/nagios-plugins/nagios-plugins/releases/download/release-2.4.0/nagios-plugins-2.4.0.tar.gz

tar -xzvf nagios-plugins-2.4.0.tar.gz

E ídem para los archivos fuente de NRPE, en la URL https://github.com/NagiosEnterprises/nrpe/releases/:

wget https://github.com/NagiosEnterprises/nrpe/releases/download/nrpe-4.0.3/nrpe-4.0.3.tar.gz

tar -xzvf nrpe-4.0.3.tar.gz

1.5. Compilación e instalación

Ir a la carpeta donde se encuentran los ficheros fuente de Nagios, desde el directorio /home/nagios:

cd nagios-4.4.6

./configure

Compilar:

sudo make all

E instalar:

make install

Make install-init

Make install-commandmode

Make install-config

make install-webconf

Habilitar los servicios nagios y apache para que inicien automáticamente en el arranque del sistema:

sudo systemctl enable nagios, apache2

Habilitar la sobreescritura y los módulos CGI de Apache, y reiniciar el servicio:

sudo a2enmod rewrite cgi

sudo systemctl restart apache2

Configurar el usuario y la contraseña para el acceso web:

htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

Iniciamos o reiniciamos los servicios nagios y apache:

sudo systemctl start nagios

sudo systemctl restart apache2

A continuación, compilar e instalar los plugins de nagios. Acceder a la carpeta donde se encuentra el código fuente, desde /home/nagios:

cd nagios-plugins-2.4.0/

./configure

sudo make install

Reiniciar el servicio nagios: **sudo systemctl restart nagios**

Acceder a la carpeta donde se encuentra el código fuente de NRPE, en este caso:

cd ..

cd nrpe-4.0.3/

dpkg -L libssl-dev

Compilar e instalar NRPE[2]:

./configure --with-ssl=/usr/bin/openssl

sudo make check_nrpe

sudo make install-plugin

Crear el comando para que nagios pueda usar el comando NRPE que se acaba de crear. Editar:

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

Y añadir al final de la parte donde se definen los comandos las siguientes líneas:

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

1.6. Configuraciones adicionales

Crear dos comandos para controlar cómodamente la implantación de cambios en el servidor. Desde el directorio /home/nagios, editar el fichero:

nano .bashrc

Y añadir al final las líneas:

alias nagioscheck='/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg'

alias nagiosreload='sudo systemctl restart nagios'

Recargar:

source .bashrc

Con estos comandos creados, cada vez que se haga un cambio en los ficheros de configuración de nagios, se podrá chequear el sistema desde cualquier ubicación ejecutando:

nagioscheck

Y se podrá reiniciar el servicio nagios ejecutando:

nagiosreload

Puede ser útil añadir al sistema un usuario de sólo lectura. Para ello, desde la terminal, ejecutar el comando:

htpasswd -b /usr/local/nagios/etc/htpausswd.users visor visor

Editar el fichero: **sudo nano /usr/local/nagios/etc/cgi.cfg**

Buscar la línea en la que pone: *#authorized_for_read_only=user1,user2*, descomentar y sustituir user1,user2 por visor.

Buscar la línea en la que pone: *authorized_for_all_services=nagiosadmin*, añadir tras nagiosadmin, una coma y visor.

Buscar la línea en la que pone: *authorized_for_all_hosts=nagiosadmin*, añadir tras nagiosadmin, una coma y visor.

nagioscheck

nagiosreload

Tras esto, se podrá acceder a la página de Nagios escribiendo en el navegador: http://IP_del_servidor_Nagios/nagios/ e identificarnos tanto con el usuario nagiosadmin como con el usuario visor, que tendrá acceso limitado.

2. Programación de notificaciones

2.1 Notificaciones por correo electrónico

Instalar php y otras dependencias para notificaciones por correo:

sudo apt install php php-cli php-gd php-curl php-zip php-intl php-mbstring php-xml

Instalar composer de php:

sudo php -r "copy('https://getcomposer.org/installer', 'composer-setup.php');"

sudo php composer-setup.php --install-dir=/usr/local/bin --filename=composer

Descargar e instalar el cliente smtp:

wget https://github.com/boolean-world/smtp-cli/archive/master.zip

sudo unzip -d /opt master.zip

cd /opt/smtp-cli-master

sudo composer install

Crear un archivo config.json y colocar en él los datos de la cuenta de correo que enviará las notificaciones:

{

"host": "smtp.gmail.com", (

"username": "the-senders-email@gmail.com",

"password": "the-password-of-the-account",

"secure": "tls",

"port": 587

}

Si se quiere utilizar outlook en vez de gmail sustituir el host por "smtp-mail.outlook.com" y el "username": "the-senders-email@outlook.com"

Modificar el fichero /usr/local/nagios/etc/objects/commands.cfg para que los comandos notify-host-by-email y notify-service-by-email apunten a /opt/smtp-cli-master/smtp-cli.php. La forma de hacerlo es **remplazando /bin/mail -s por /opt/smtp-cli-master/smtp-cli.php.**

Configurar algún contacto para que utilice los comandos anteriores, en el fichero /usr/local/nagios/etc/objects/contacts.cfg

Un ejemplo de contacto:

```
define contact {

        contact_name                    alerta.nagios
        use                             generic-contact
        alias                           Alertas
        email                           alertanagios01@outlook.es
        host_notifications_enabled      1
        service_notifications_enabled   1
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    w,c,u,r,f,s
        host_notification_options       d,u,r,f,s
        pager                           366265488
        service_notification_commands   notify-service-by-email,notify-service-b>
        host_notification_commands      notify-host-by-email,notify-host-by-tele>
        register 1
}
```

Como información adicional añado los atributos de las directivas de notificación

Atributos de directiva service_notification_options

- w: Notify on WARNING service states
- u: Notify on UNKNOWN service states
- c: Notify on CRITICAL service states
- r: Notify on service RECOVERY (OK states)
- f: Notify when the service starts and stops FLAPPING
- n (none): Do not notify the contact on any type of service notifications

Atributos de directiva host_notification_options

- d: Notify on DOWN host states
- u: Notify on UNREACHABLE host states
- r: Notify on host RECOVERY (UP states)
- f: Notify when the host starts and stops FLAPPING
- s: Send notifications when host or service scheduled downtime starts and ends
- n (none): Do not notify the contact on any type of host notifications.

2.2 Notificaciones PUSH en teléfono móvil

Copiar los ficheros *nath_status.php* y *ServerAlarmNotify.php*, respectivamente a */usr/local/nagios/share* y a */usr/local/nagios/libexec*.[5]

Dar permiso de ejecución a este último, desde la carpeta donde se encuentran las librerías de plugins de nagios, */usr/local/nagios/libexec*:

chmod a+x ServerAlarmNotify.php

Modificar el fichero */usr/local/nagios/etc/objects/commands.cfg* para crear los comandos sm-*host-push-notify* y *sm-service-push-notify*. En las líneas de ambos comandos aparecerá una clave (---) que será distinta para cada aplicación móvil y por tanto será necesario cambiar editando el fichero.

define command {

command_name sm-host-push-notify

command_line $USER1$/ServerAlarmNotify.php $HOSTNAME$ --- HOST $HOSTSTATE$

}

define command {

command_name sm-service-push-notify

command_line $USER1$/ServerAlarmNotify.php $HOSTNAME$ --- SERVICE $SERVICESTATE$

}

Configurar algún contacto para que utilice los comandos anteriores, en el fichero */usr/local/nagios/etc/objects/contacts.cfg*

OpenSSL debe estar instalado por defecto. De lo contrario, instalar:

sudo apt install openssl

Habilitar el módulo SSL de Apache:

sudo a2enmod ssl

sudo a2ensite default-ssl

sudo systemctl restart apache2

Descargar e instalar en el teléfono móvil la aplicación ServerAlarms – Nagios Client en Android e iOS.

Agregar el servidor Nagios completando los campos que se indican. En el campo *PHP SERVER* hay que añadir la línea: https://IP_del_servidor/nagios/

Hacer click en *TEST AND UPDATE*.

Si el servidor se añadió correctamente, ir a Menú -> Settings y pulsar el botón *SHOW KEY*. Se obtendrá la clave que hay que sobrescribir en el fichero commands.cfg, mencionada anteriormente.

2.3 Notificaciones en Telegram

Buscamos el bot BotFather en Telegram y escribimos en su chat /start

Le damos un nombre al bot en mi caso nagios-bot

Y un nombre de usuario: nagiosinntbot

Una vez hecho eso nos devuelve un token de acceso

5275295940:AAGswtcQFQeMs7oZAPQxdzII3HrctqzQJ6w

Donde la id de usuario es 5275295940

Con este link podemos ver información del bot

https://api.telegram.org/bot5275295940:AAGswtcQFQeMs7oZAPQxdzII3HrctqzQJ6w/getUpdates

Con este otro podemos descargarlo en los dispositivos que queremos que lleguen las alertas

https://t.me/nagiosinntbot

2.3.1. Prerrequisitos

Sudo apt install python

pip install twx.botapi

2.3.2 Configuración de Nagios

El primer paso es descargar el script que nos permite enviar las alertas al bot

wget -O /usr/local/bin/nagios_telegram.py
https://raw.githubusercontent.com/pommi/telegram_nagios/master/telegram_nagios.py
chmod 755 /usr/local/bin/nagios_telegram.py

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

define command{
command_name notify-host-by-telegram
command_line /usr/bin/curl -X POST --data chat_id=$CONTACTPAGER$ --data parse_mode="markdown" --data text="%60$HOSTNAME$%60 %0A%0A$NOTIFICATIONTYPE$ %0A%60$HOSTSTATE$%60 %0A%60$HOSTADDRESS$%60 %0A%60$HOSTOUTPUT$%60" https://api.telegram.org/bot5275295940:AAGswtcQFQeMs7oZAPQxdzII3HrctqzQJ6w

/sendMessage
}

define command{
command_name notify-service-by-telegram
command_line /usr/bin/curl -X POST --data chat_id=$CONTACTPAGER$ --data parse_mode="markdown" --data text="%60$HOSTNAME$%60 %0A%0A$NOTIFICATIONTYPE$ %0A%60$SERVICEDESC$%60 %0A%60$HOSTADDRESS$%60 %0A%60$SERVICESTATE$%60 %0A%60$SERVICEOUTPUT$%60" https://api.telegram.org/bot5275295940:AAGswtcQFQeMs7oZAPQxdzII3HrctqzQJ6w/sendMessage
}

/usr/local/nagios/etc/objects/contacts.cfg

#Yo solo estoy utilizando un contacto no un grupo

define contact {
 contact_name alerta.nagios
 pager 366265488
 service_notification_commands notify-service-by-telegram
 host_notification_commands notify-host-by-telegram
}

define contact {
 contact_name Telegram Group Chat
 pager -23456789
 service_notification_commands notify-service-by-telegram
 host_notification_commands notify-host-by-telegram
}

Para rellenar el dato pager tenemos que saber nuestra id de telegram, una forma de saberla es buscar el bot userinfobot. Otra forma de saberlo es enviar algun mensaje al bot y volviendo a mirar este link

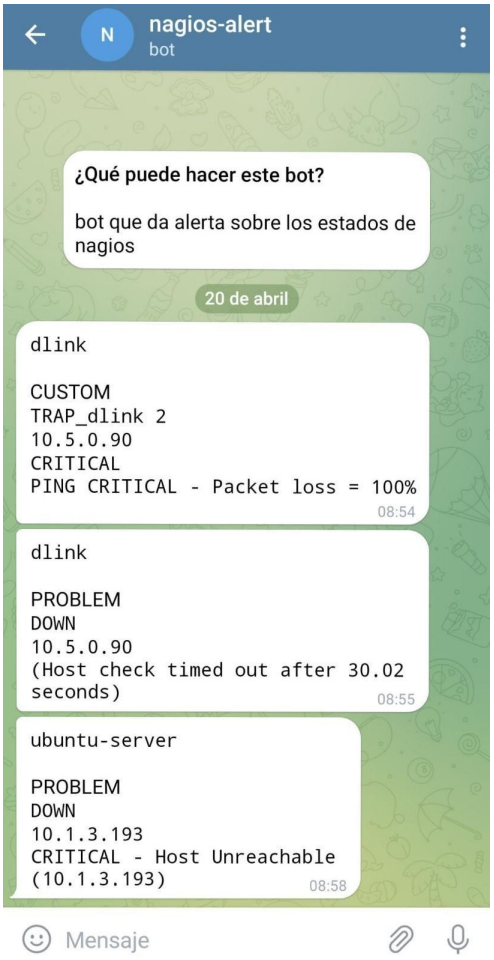
https://api.telegram.org/bot5275295940:AAGswtcQFQeMs7oZAPQxdzII3HrctqzQJ6w/getUpdates

Nos saldrá una nueva sentencia en la que nos indica la id del chat, nombre y algunos datos más.

2.3.3 Comprobar que funciona

Podemos comprobar que recibimos mensajes con el comando

curl -s -X POST https://api.telegram.org/bot5275295940:AAGswtcQFQeMs7oZAPQxdzII3HrctqzQJ6w/sendMessage -d text="mensaje de texto de prueba" -d chat_id= 366265488



3. Monitoreo de dispositivos de red con SNMP

3.1 Instalación de SNMP y sus librerías

Si se ha seguido el manual, el paquete NET-SNMP ya se encuentra instalado. A continuación se instalarán las librerías de NET-SNMP-PERL:

sudo apt-get update

sudo apt-get install -y libnet-snmp-perl libconfig-inifiles-perl libnet-ip-perl libnet-dns-perl libperl-version-perl

Tras esto, se procederá a instalar el traductor de traps snmptt, comenzando por los prerrequisitos:

sudo cpan YAML Getopt::Long File::Basename Time::HiRes Sys::Hostname Text::Balanced Text::ParseWords Sys::Syslog Crypt::DES Digest::MD5 Digest::SHA1 Digest::HMAC List::Util Config::IniFiles SNMP Net::SNMP Net::DNS

A continuación, descargar en /home/nagios y desempaquetar el código fuente de snmptt:

wget https://sourceforge.net/projects/snmptt/files/latest/download/snmptt_1.4.2.tgz

tar -zxvf snmptt_1.4.2.tgz

3.2 Ficheros y configuración necesaria para SNMP

Entrar en el directorio:

cd snmptt_1.4.2/

sudo cp snmptthandler snmptt snmpttconvert snmpttconvertmib /usr/sbin

sudo cp snmptt.ini /etc/snmp

Editar el fichero ***/etc/default/snmpd***

Añadiendo las siguientes líneas al final:

export MIBS=ALL

TRAPDRUN=yes

TRAPDOPTS='-On -Lsd -p /var/run/snmptrapd.pid'

Editar el fichero: **sudo nano /etc/snmp/ snmptt.ini**

Cambiando los parámetros:

net_snmp_perl_enable = 1

dns_enable=1

mibs_environment = ALL

Dar permisos de ejecución: **sudo chmod a+x /etc/snmp/snmptt.ini**

Crear el fichero:

sudo touch /etc/snmp/snmptt.conf

Editar el fichero: **sudo nano /etc/snmp/snmptrapd.conf**

Añadiendo al final las siguientes líneas:

authCommunity log *[community snmp que se utilice]*

traphandle default /usr/sbin/snmptt

disableAuthorization yes

donotlogtraps yes

Editar el fichero: **sudo nano /etc/logrotate.conf**

Añadiendo al final:

/var/log/snmp/snmptt.log /var/log/snmp/snmpttunknown.log

{missingok}

Crear el directorio y los ficheros donde se guardarán los logs de SNMPTT:

sudo mkdir /var/log/snmptt

sudo touch /var/log/snmptt/snmptt.log

sudo touch /var/log/snmptt/snmpttunknown.log

sudo chmod 755 /var/log/snmptt/snmptt.log

sudo chmod 755 /var/log/snmptt/snmpttunknown.log

sudo mkdir /var/spool/snmptt

Añadir al cortafuegos el puerto donde se recibirán los traps:

sudo ufw allow 162/udp

sudo systemctl reboot

Habilitar e iniciar los servicios snmpd y snmptrapd:

sudo systemctl enable snmpd snmptrapd

sudo systemctl start snmpd snmptrapd

3.3. Configuración de TRAPS y añadir dispositivo

Crear el plugin que gestionará la recepción de traps en nagios:

sudo mkdir /usr/local/nagios/libexec/eventhandlers/

sudo nano /usr/local/nagios/libexec/eventhandlers/submit_check_result

Y añadir las líneas:

#!/bin/sh

echocmd="/bin/echo"

CommandFile="/usr/local/nagios/var/rw/nagios.cmd"

datetime=`date +%s`

cmdline="[$datetime] PROCESS_SERVICE_CHECK_RESULT;$1;$2;$3;$4"

`$echocmd $cmdline >> $CommandFile`

Dar permiso de ejecución y cambiar propietario:

sudo chmod a+x /usr/local/nagios/libexec/eventhandlers/submit_check_result

sudo chown nagios:nagios /usr/local/nagios/libexec/eventhandlers/submit_check_result

Siempre que se quiera controlar mediante traps snmp un dispositivo determinado, habrá que copiar los ficheros .mib que nos proporcione el fabricante en el directorio */usr/share/snmp/mibs*. Después, generaremos un fichero con información del trap a partir del .mib, con el comando:

sudo snmpttconvertmib --in=/usr/share/snmp/mibs/nombre_del_fichero.mib --out=/etc/snmp/snmptt.conf.nombre_dispositivo --exec='/usr/local/nagios/libexec/eventhandlers/submit_check_result $r TRAP_nombre_del_servicio 2 "El dispositivo ha generado una alarma $1 $2 $3 $4"'[6]

Donde $r corresponde al nombre del host, 2 sería el estado de la alerta (0=OK, 1=WARNING, 2=CRITICAL) y $1, $2, $3, $4 son parámetros contenidos en el trap. El fichero */etc/snmp/snmptt.conf.nombre_dispositivo* se genera de manera automática y debe modificarse para que se ajuste a lo necesario, según la información que devuelva el trap.

Cada vez que se haga esa operación, habrá que editar el fichero:

sudo nano /etc/snmp/ snmptt.ini

Y añadir al final la línea correspondiente al fichero generado:

[TrapFiles]

snmptt_conf_files = <<END

/etc/snmp/snmptt.conf

/etc/snmp/snmptt.conf.nombre_dispositivo

END

Por último, hay que añadir la definición del servicio trap, como una plantilla:

sudo nano /usr/local/nagios/etc/objects/templates.cfg

define service{

    name trap-service

    use generic-service

    register 0

service_description TRAP_Updates

is_volatile 1

check_command check-host-alive

max_check_attempts 1

check_interval 1

retry_interval 1

active_checks_enabled 0

passive_checks_enabled 1

check_period none

notification_interval 0

contact_groups adminsapt

}

El servicio correspondiente a cada equipo que envíe las traps deberá estar asociado al servicio (en este ejemplo: TRAP_nombre_del_servicio) definido en Nagios:

Añadir en el .cfg del dispositivo

Sudo nano /usr/local/nagios/etc/objects/switch.cfg

define service{

use trap-service

hosts dispositivo1, dispositivo2

service_description TRAP_nombre_del_servicio

}

También hay que descomentar en /usr/local/nagios/etc/nagios.cfg la ruta del fichero .cfg del dispositivo

cfg_file=/usr/local/nagios/etc/objects/switch.cfg

Reiniciar servicios:

sudo systemctl restart snmpd

sudo systemctl restart snmptrapd

nagioscheck

nagiosreload

Para resolver algunas posibles incidencias, es conveniente dar de alta los nombres de los equipos asociados a su IP en el fichero /etc/hosts:

sudo nano /etc/hosts

IP_dispositivo nombre_dispositivo

3.1 Monitoreo de tráfico con check_iftraffic64.pl

Lo descargamos desde la página de nagios y lo añadimos a la siguiente ruta

Cd /usr/local/nagios/libexec

wget https://exchange.nagios.org/components/com_mtree/attachment.php?link_id=4019&cf_id=24

Le otorgamos permisos de ejecución y propietario tanto al plugin como a la carpeta traffic

chmod 755 check_iftraffic64.pl

chown nagios:nagios check_iftraffic64.pl

chmod 755 /usr/local/nagios/libexec/traffic

chown nagios:nagios /usr/local/nagios/libexec/traffic

Definimos el comando

nanoSudo /usr/local/nagios/etc/objects/commands.cfg

```
define command{
        command_name    check_iftraffic
        command_line    $USER1$/check_iftraffic64.pl -H $HOSTADDRESS$ -C public -i $ARG1$ -B -w $ARG2$ -c $ARG3$
}
define command{
        command_name    check_iftraffic_v1
        command_line    $USER1$/check_iftraffic64.pl -v 1 -H $HOSTADDRESS$ -C public -f --32bit -I 100 -u m -i $ARG1$ -B -w $ARG2$ -c $ARG3$
```

}

Definimos el host y servicio en sudo /usr/local/nagios/etc/objects/ap_inntelia

```
#Difinición de host
define host{
use      generic-ap
host_name      ap_inntelia
alias          ap_inntelia interior
address        ip del dispositivo
 }
# Monitor traffic with check_iftraffic64

define service {

   use              trap-service            ; Inherit values from a template
   host_name        ap_inntelia
   service_description    WiFi Traffic
   check_command       check_iftraffic!wifi0!80!95
   contact_groups      alerta_nagios
   check_interval      5
  retry_interval       1
}

define service {

   use              trap-service            ; Inherit values from a template
   hostgroup_name      ap_inntelia
   service_description    Ethernet Traffic
   check_command       check_iftraffic!eth1!80!95
```

contact_groups alerta_nagios

}

Habilitar SNMP en el router o switch

1. Nos metemos en el router y escribimos

Router> enable

2. Nos pide la contraseña de acceso

Password:

3. Router# configure terminal

4. Router(config)# snmp-server

Community public RO (si queremos solo lectura)

Community private RW (si queremos lectura y escritura)

5. Router(config)# exit

6. Router# write memory

4. Monitoreo de servidores y equipos con NRPE

4.1. Instalación del plugin check_nrpe

En el directorio

cd /home/nagios

Descargamos la última versión de NRPE, en este caso 4.0.3

wget https://github.com/NagiosEnterprises/nrpe/releases/download/nrpe-4.0.3/nrpe-4.0.3.tar.gz

tar –xzvf nrpe-4.0.3.tar.gz

Nos movemos al directorio

cd nrpe-4.0.3/

Ejecutamos el script de configuración

sudo ./configure

Instalamos el plugin

Make check_nrpe

Make install-plugin

Abrimos el siguiente fichero y definimos el comando de check_nrpe si no lo está

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

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

4.2. Instalación de la herramienta NRPE en el host remoto

Nos loggeamos como root y escribimos los siguientes comandos

sudo update

sudo apt install -y autoconf automake gcc libc6 libmcrypt-dev make libssl-dev

Dado que NRPE necesita los complementos de Nagios para realizar sus comprobaciones, instálelo de la misma manera que lo hicimos anteriormente. Luego, descargue el código fuente de NRPE y ejecute los pasos en la sección "Instalación del complemento check_nrpe", hasta "Configurar los Makefiles". Una vez que haya completado, ejecute los siguientes comandos:

Instalar los plugins de nagios

wget
https://github.com/nagios-plugins/nagios-plugins/releases/download/release-2.4.0/nagios-plugins-2.4.0.tar.gz

tar -xzvf nagios-plugins-2.4.0.tar.gz
cd nagios-plugins-2.4.0

./configure

Make install

Descargar código fuente

Wget https://github.com/NagiosEnterprises/nrpe/archive/refs/tags/nrpe-4.0.3.tar.gz

Volvemos a repetir instalación del complemento check_nrpe

Wget
https://github.com/NagiosEnterprises/nrpe/releases/download/nrpe-4.0.3/nrpe-4.0.3.tar.gz

tar –xzvf nrpe-4.0.3.tar.gz

Nos movemos al directorio

cd nrpe-4.0.3/

Ejecutamos el script de configuración

sudo ./configure

make check_nrpe
make install-plugin

make all
make install
make install-config
make install-init

Modificamos el archivo nrpe.cfg

sudo nano /usr/local/nagios/etc/nrpe.cfg

La parte de allowed_hosts y server_address la modificamos a

allowed_hosts=127.0.0.1,::1,<Nagios server IP>
server_address=0.0.0.0

Recarganos nrpe

systemctl enable nrpe
systemctl start nrpe

Si escribimos el siguiente comando y nos devuelve la versión significa que nrpe está funcionando

/usr/local/nagios/libexec/check_nrpe -H <Remote host IP>

4.3. Configuración NRPE

Con el comando df –h podemos ver la lista de discos y su niveles de uso

```
nagios@nagios:/usr/local/nagios/etc/servers$ df -h
S.ficheros     Tamaño Usados  Disp Uso% Montado en
udev             1,5G      0  1,5G   0% /dev
tmpfs            299M   1,2M  298M   1% /run
/dev/sda1         19G   6,1G   12G  35% /
tmpfs            1,5G      0  1,5G   0% /dev/shm
tmpfs            5,0M   4,0K  5,0M   1% /run/lock
tmpfs            299M   124K  299M   1% /run/user/1000
```

Podemos añadir un comando para monitorizar el espacio de disco, abrimos el archivo nrpe.cfg

sudo nano /usr/local/nagios/etc/nrpe.cfg

Escribimos al final del documento

command[check_sda1]= /usr/local/nagios/libexec/check_disk –w 20% -c 10% -p /dev/sda1

Con esto conseguimos que si el espacio del disco es menor al 20% nos de una alerta y si el espacio del disco es menor al 10% nos lo indicará con un estado crítico.

systemctl restart nrpe

4.4. Configuración Nagios

Ahora tenemos que indicar al servidor de nagios como recoger las estadísticas.

Editamos el archivo nagios.cfg

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

Encontramos la siguiente línea y la descomentamos

#cfg_dir=/usr/local/nagios/etc/servers

Creamos la carpeta server

mkdir /usr/local/nagios/etc/servers

sudo nano /usr/local/nagios/etc/servers/testserver.cfg

Editamos el archivo

```
define host {
    use                     linux-server
    host_name               <Remote server hostname>
    alias                   <An alias for your server, can contain spaces>
```

```
        address                 <Remote server IP>
        max_check_attempts      5
        check_period            24x7
        notification_interval   30
        notification_period     24x7
}

define service {
        use                             generic-service
        host_name                       <Remote server hostname>
        service_description             CPU load
        check_command                   check_nrpe!check_load
}

define service {
        use                     generic-service
        host_name               <Remote server hostname>
        service_description     /dev/sda1 free space
        check_command           check_nrpe!check_sda1
}
```

systemctl restart nagios

5. Instalación de gráficos estadísticos

5.1. PNP4Nagios

Instalar las dependencias:

sudo apt-get install rrdtool php-gd librrds-perl -y

Descargar y desempaquetar código fuente:

wget
https://downloads.sourceforge.net/project/pnp4nagios/PNP-0.6/pnp4nagios-0.6.26.tar.gz

tar -xzvf pnp4nagios-0.6.26.tar.gz

Acceder al directorio para compilar:

cd pnp4nagios-0.6.26/

./configure --with-httpd-conf=/etc/apache2/sites-enabled --sysconfdir=/etc/pnp4nagios --with-base-url=/pnp4nagios

make all

sudo make fullinstall

Para que se ejecute desde el inicio del sistema:

sudo systemctl enable npcd

sudo systemctl start npcd

Reiniciar apache:

sudo systemctl restart apache2

Renombrar fichero install.php:

sudo mv /usr/local/pnp4nagios/share/install.php /usr/local/pnp4nagios/share/install.php.BKP

A continuación editar el fichero de configuración de Nagios:

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

Añadir al final del fichero las líneas:

process_performance_data=1

service_perfdata_file=/usr/local/pnp4nagios/var/service-perfdata

service_perfdata_file_template=DATATYPE::SERVICEPERFDATA\tTIMET::$TIMET$\tHOSTNAME::$HOSTNAME$\tSERVICEDESC::$SERVICEDESC$\tSERVICEPERFDATA::$SERVICEPERFDATA$\tSERVICECHECKCOMMAND::$SERVICECHECKCOMMAND$\tHOSTSTATE::$HOSTSTATE$\tHOSTSTATETYPE::$HOSTSTATETYPE$\tSERVICESTATE::$SERVICESTATE$\tSERVICESTATETYPE::$SERVICESTATETYPE$

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::$HOSTNAME$\tHOSTPERFDATA::$HOSTPERFDATA$\tHOSTCHECKCOMMAND::$HOSTCHECKCOMMAND$\tHOSTSTATE::$HOSTSTATE$\tHOSTSTATETYPE::$HOSTSTATETYPE$

host_perfdata_file_mode=a

host_perfdata_file_processing_interval=15

host_perfdata_file_processing_command=process-host-perfdata-file

Seguidamente, editar el fichero de comandos de Nagios:

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

Añadiendo:

define command {

command_name process-service-perfdata-file

command_line /bin/mv /usr/local/pnp4nagios/var/service-perfdata /usr/local/pnp4nagios/var/spool/service-perfdata.$TIMET$

}

define command {

command_name process-host-perfdata-file

command_line /bin/mv /usr/local/pnp4nagios/var/host-perfdata /usr/local/pnp4nagios/var/spool/host-perfdata.$TIMET$

}

Editar el fichero de plantillas de Nagios:

sudo nano /usr/local/nagios/etc/objects/templates.cfg

Y añadir:

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=$SERVICEDESC$' class='tips' rel='/pnp4nagios/index.php/popup?host=$HOSTNAME$&srv=$SERVICEDESC$

register 0

}

Desde el mismo directorio del código fuente de pnp4nagios, ejecutar:

sudo cp contrib/ssi/status-header.ssi /usr/local/nagios/share/ssi/

Reiniciar el servicio del npcd:

sudo systemctl restart npcd

nagioscheck

nagiosreload

Activar los gráficos para un host o para un servicio, accediendo a su fichero de configuración correspondiente y añadiendo a la cláusula *use* (en la que se importa la plantilla), la expresión host-pnp para los equipos o srv-pnp para los servicios. Recargar:

nagioscheck

Nagiosreload

Si nos sale el siguiente error

Error Function set_magic_quotes_runtime() is deprecated

Sustituir en input.php

//if (get_magic_quotes_runtime())

Por:

if (function_exists('get_magic_quotes_runtime'))

//set_magic_quotes_runtime(0);

Por:

ini_set('magic_quotes_runtime',0);

//if (get_magic_quotes_gpc())

Por:

if (function_exists('get_magic_quotes_gpc'))

Si no cargan los gráficos, y al hacer click sobre ellos aparece el siguiente problema:

Editar el archivo:

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

Buscar la sección

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

Y cambiarla de esta forma:

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

Apt install php-xml

5.2. Grafana

sudo apt-get install -y adduser libfontconfig1

Descargar el paquete de instalación en su última versión. En este caso, desde /home/nagios:

wget https://dl.grafana.com/enterprise/release/grafana-enterprise_8.4.4_amd64.deb

E instalar:

sudo dpkg -i grafana-enterprise_8.4.4_amd64.deb

Habilitamos desde el arranque del sistema e iniciamos el servicio:

sudo systemctl enable grafana-server

sudo systemctl start grafana-server

Abrir el puerto del firewall que utiliza grafana:

sudo ufw allow 3000/tcp

Instalar los paquetes de fuentes necesarios:

sudo apt install fontconfig freetype* -y

Instalar plugins desde grafana:

sudo grafana-cli plugins install sni-pnp-datasource

Ir al directorio de pnp4nagios:

cd /usr/local/pnp4nagios/share/application/controllers/

Y descargar, desde allí, la api:

wget -O api.php "https://github.com/lingej/pnp-metrics-api/raw/master/application/controller/api.php"

Reiniciar el servicio de Grafana:

sudo systemctl restart grafana-server

Añadir el usuario grafana a la lista de usuarios de nagios:

sudo htpasswd -b /usr/local/nagios/etc/htpasswd.users grafana 123456

Ya está disponible el servidor web de grafana. Acceder a éste mediante *http://IP_del_servidor_Nagios:3000*

Las credenciales por defecto son admin/admin, y tras la identificación, la página solicita el cambio de contraseña a una más segura.

Tras esto, hay que añadir un nuevo datasource de tipo PNP con la URL *http://localhost/pnp4nagios*, autenticación básica y las credenciales que hemos registrado anteriormente, esto es, grafana/123456.

A partir de ahí, ya se puede crear los dashboards y gráficos que se desee desde dentro de la web.

5.3. Nagvis

Instalar dependencias:

sudo apt install php-mbstring php-pdo graphviz librrd-dev libboost-dev libboost-system-dev librrd8 rsync php-sqlite3

Ir a la web http://nagvis.org/downloads y copiar la dirección del enlace de la última versión. Desde /home/nagios, hacer un wget que apunte a dicha dirección para descargar el fichero del código fuente. En este caso:

wget http://nagvis.org/share/nagvis-1.9.30.tar.gz

Sudo apt-get install nagvis

Instalar mk_livestatus. Desde /home/nagios, hacer un wget para descargar la última versión del fichero del código fuente. En este caso:

wget https://download.checkmk.com/checkmk/1.5.0p25/mk-livestatus-1.5.0p25.tar.gz

tar -xzvf mk-livestatus-1.5.0p25.tar.gz

cd mk-livestatus-1.5.0p25

./configure

make

sudo make install

A continuación hay que editar el fichero de configuración de Nagios:

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

Buscar la sección *EVENT BROKER MODULE(S)*, y añadir debajo de ésta:

broker_module=/usr/local/nagios/lib/mk-livestatus/livestatus.o /usr/local/nagios/var/rw/live

Recargar Nagios:

nagioscheck

nagiosreload

Para comprobar que todo funciona, entrar en el directorio */usr/local/nagios/var/rw/* y hacer un *ls* para ver si se ha generado efectivamente el archivo *live*.

Volver al directorio /home nagios para descomprimir los archivos de NagVis e instalar (en este caso no se necesita compilar, sino que viene con un instalador):

cd /home/nagios

tar -xzvf nagvis-1.9.30.tar.gz

cd nagvis-1.9.30/

sudo ./install.sh

Apt install sqlite3

Y responder con la opción por defecto a todas las preguntas que haga el sistema.

Editar el archivo de configuración de nagvis en apache:

sudo nano /etc/httpd/conf.d/nagvis.conf

ó

sudo nano /etc/apache2/conf-available/nagvis.conf

Comentar la línea: *#AllowOverride None*, y añadir justo debajo la línea: *Require all granted*

Descomentar las líneas:

AuthName "NagVis Access"

AuthType Basic

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

Require valid-user

Si existe el directorio de configuración de apache */etc/apache2*, copiar el fichero anterior en el directorio *sites-enabled*, ya que el instalador lo copia por defecto en */etc/httpd*:

sudo cp /etc/httpd/conf.d/nagvis.conf /etc/apache2/sites-enabled/nagvis.conf

ó

sudo cp /etc/apache2/conf-available/nagvis.conf /etc/apache2/sites-enabled/nagvis.conf

Editar el archivo de configuración de nagvis:

sudo nano /usr/local/nagvis/etc/nagvis.ini.php

Descomentar las líneas:

logonmodule=”LogonMixed”

logonenvvar=”REMOTE_USER”

logonenvcreateuser=”1”

Reiniciar apache:

sudo systemctl restart apache2

Comprobar en la interfaz web de Nagvis que se han creado los mismos usuarios de Nagios y eliminar el usuario “admin”.

Si sale error por no encontrar la ruta /var/lib/nagios3/rw/live

Editar el archivo nano /etc/nagvis/nagvis.ini.php

Buscar socket:unix y sustituir la ruta por la ruta del live, en mi caso

/usr/local/nagios/var/rw/live

5.4. MRTG

sudo apt-get install mrtg

Cd /etc/

sudo cp mrtg.cfg mrtg.cfg.bkp

sudo chmod 755 mrtg.cfg

Editar la configuración del fichero /etc/mrtg.cfg, y añadir las líneas debajo de *Global Settings*:

RunAsDaemon: yes

EnableIPv6: no

WorkDir: /var/www/mrtg

Options[_]: bits,growright

WriteExpires: Yes

sudo mkdir /var/www/mrtg

sudo chown -R www-data:www-data /var/www/mrtg

sudo chmod -R 755 /var/www/mrtg

Añadir a /etc/mrtg.cfg la configuración de cada equipo cuyo tráfico se pretenda monitorear mediante el comando (hay que ser root para ejecutarlo):

cfgmaker {community}@{direccionIP} >> /etc/mrtg.cfg

sudo indexmaker /etc/mrtg.cfg > /var/www/mrtg/index.html

sudo nano /etc/apache2/sites-available/mrtg.conf

sudo a2ensite mrtg

sudo systemctl restart apache2

6. Detalles para Nagios

6.1 Cambiar skin de página web

En primer lugar, hacer un backup de la web actual:

tar -czvf backup-pagina.tar.gz /usr/local/nagios/share/

Para descargar el skin, ir a la web https://exchange.nagios.org/, buscar el adecuado y copiar el enlace de la descarga. Tras esto, en la terminal, hacer un wget que apunte a dicho enlace. En este caso:

wget https://github.com/ynlamy/vautour-style/releases/download/v1.7/vautour_style.zip

Descomprimir el archivo en el directorio donde se encuentra la página de nagios:

unzip -d /usr/local/nagios/share/ vautour_style.zip

Y cuando el sistema pregunte, marcar la opción *A* (all) para reemplazar todos los ficheros.

Recargar el sistema, y comprobar que la web ha cambiado:

nagiosreload

6.2 Personalizar logo

En la web, hacer click con botón derecho del ratón sobre el logo y pulsar sobre la opción *inspeccionar* para comprobar la ruta y las dimensiones de la imagen. En este caso, el tamaño es 159 x 25 píxeles y la ubicación es */usr/local/nagios/share/images/interface/logo.gif*. Habrá que redimensionar la nueva imagen deseada para que se asemeje a la actual, y el resultado en pantalla sea óptimo.

Ir a la carpeta y renombrar el fichero actual:

cd /usr/local/nagios/share/images/interface/

sudo mv logo.gif logo.gif.bkp

Subir, a través de cualquier método, como por ejemplo SCP, la nueva imagen a esa carpeta y renombrarla con el mismo nombre que tenía la anterior:

sudo mv ejemplo.png logo.gif

Esperar a que el navegador recargue la caché para que muestre la web con la nueva imagen, o abrir en otro navegador.

También se puede cambiar el icono que aparece en la pestaña de la web, repitiendo el mismo proceso con el archivo /usr/local/nagios/share/images/favicon.ico, de tamaño 32 x 32 píxeles, reemplazándolo por el deseado, y así para cualquier imagen fija que se pretenda renovar.

6.3 Actualización de Nagios

En caso de querer actualizar a la última versión de Nagios, seguir los siguientes pasos:

Descargar la última versión de Nagios Core. Comprobar la última versión yendo a la página https://www.nagios.org/projects/nagios-core/history/4x/, y hacer un wget que apunte a dicha versión. Desde /home/nagios:

wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-x.y.z.tar.gz

Donde habrá que sustituir x, y, z por el número de la versión (por ejemplo, 4.4.6).

Hacer un backup del directorio */usr/local/nagios/share* para guardar la apariencia actual de la web (skin, logos, etc.):

tar -czvf share_backup.tar.gz /usr/local/nagios/share/

Descomprimir el fichero de código de Nagios descargado:

tar -xzvf nagios-x.y.z.tar.gz

Compilar e instalar:

cd nagios-x.y.z.tar.gz

./configure --with-command-group=nagios

sudo make all

sudo make install

Reiniciar el servicio:

sudo systemctl restart nagios

Restaurar el backup sobre el directorio */usr/local/nagios/share.* Desde el directorio donde se haya realizado el backup, por ejemplo, /home/nagios:

tar -xzvf share_backup.tar.gz -C /usr/local/nagios/

Tras esto, se podrá acceder a la página de Nagios escribiendo en el navegador: http://IP_del_servidor_Nagios/nagios/ o https://IP_del_servidor_Nagios/nagios/ y el aspecto de la web deberá ser idéntico al previo a la actualización.