

Pràctica 3

Sessió 5 - Implementar un servei DNS

Alumnes:

Mariona Farré Tapias,

Marc Pérez Guerrero

CARPETA VMS SESSIÓ 5:

https://drive.google.com/drive/folders/1cNf8_6chqDFSIM99ZPPI8gdfzaqZs8Em?usp=sharing

ÍNDEX:

Enunciat	1
Informe pràctica 3 sessió 5:	4
*** Introducció de l'escenari:	4
*** Instal·lació nagios: ***	5
*** Configuració de les altres màquines:	7
*** Configuració del servei nagios:	8
*** Configuració del servei apache:	10
** Configuració del servei de monitoreig per nagios:	11
*** Configuració dels servers:	12
*** Verificacions	17

Enunciat

1- Configurar un servidor i màquines a monitoritzar amb Nagios

- Paràmetres a monitoritzar
 - + Servidor: càrrega, disc dur (partició de root), RAM, disponibilitat dels serveis d'SSH i HTTP (a la pròpia màquina) i del servei de DHCP (a la xarxa on es troba).
 - + Routers: càrrega, RAM, disponibilitat del servei d'SSH.
 - + DNSs: càrrega, RAM, disponibilitat dels serveis d'SSH i DNS (a les pròpies màquines) i del servei de DHCP (a la xarxa on es troben).
 - + Serveis externs: connectivitat i disponibilitat del servidor web declarat al domini seax.public.edu i dels servidors DNS utilitzats com a forwarders a la sessió 3.
- L'usuari i contrasenya de la interfície web del servidor han de ser nagiosadmin/seax2024.
- Noms d'equips a utilitzar: routeracces, routerintern, dns1, dns2, nagiosserver, webserver (www.seax.public.edu)
 - Hosts (entre parèntesis l'adreça IP que se'ls definirà): routeracces (10.1.10.1), routerintern (10.1.10.2), nagios (10.1.10.5), dns1 (10.1.10.3), dns2 (10.1.10.4) i webserver (147.83.2.135).
 - Grups: cal crear-ne 2 (entre parèntesis els membres dels grups): routers (routeracces i routerintern), servidors(nagios, dns1 i dns2)

- Les màquines de l'escenari monitoritzades remotament només ho podran ser des d'aquest servidor Nagios.
- S'ha de comprovar l'estat de cada paràmetre monitoritzat cada minut
- Cal configurar llindars per als paràmetres a monitoritzar de manera que generin avisos en ser superats.
- Cal fer captures per a comprovar que la comunicació entre el servidor i la màquina remota és segura.

2- Protecció del servidor Nagios

- Apliqueu les directrius de seguretat específiques pels servidors definides a la sessió 1 i 2
- Expliqueu com podríeu fer que només fossin accessibles els serveis de Nagios i SSH i, en el cas del servei SSH només des de les adreces IP 10.1.10.11 i 10.1.20.11.
- (Opcional) Implementeu i el punt anterior i verifiqueu el seu funcionament.

3- Verificar el seu bon funcionament

- Implementar un primer escenari de treball amb el servidor amb connexió a Internet i una segona màquina a monitoritzar a la mateixa xarxa:
 - + Monitoritzeu els serveis externs definits al punt anteriors
 - + Es recomana que la màquina a monitoritzar sigui un DNS, per evitar possibles conflictes amb la configuració del tallafocs
- Comprovar que la configuració del servidor és correcta.
- Comprovar que els serveis que fan possible la monitorització funcionen correctament a les dues màquines.
- Comprovar des de la consola del servidor que es poden executar funcions de monitorització en local i en remot.
- Realitzar les captures de xarxa que permetin demostrar que la monitorització es fa en base a una comunicació segura entre servidor i màquina monitoritzada.
- Realitzar alguna prova d'estrès que permeti mostrar que passa quan es supera algun llindar prèviament definit per algun paràmetre monitoritzat.

4- Lliurar els resultats.

Mitjançant Atenea (2 fitxers).

- Redactar l'informe de la pràctica p3_s5_cognom1_nom.txt.
- Realitzar les proves necessàries per justificar els resultats i encapsular els fitxers necessaris en el fitxer p3_s5_cognom1_nom.zip.

Mitjançant Google Drive (màquines virtuals)

- Compartir amb rafael.vidal@upc.edu una carpeta a Google Drive (UPC) amb les VMs dels servidors Nagios i la màquina monitoritzada.

Important:

- L'informe de la pràctica ha de contenir l'enllaç a la carpeta amb les VMs.

- Les VMs han de contenir una còpia de l'informe al directori /root.

5- A títol orientatiu el resultat de la pràctica cal que doni resposta a les següents qüestions:

- Quin programari cal instal·lar a la màquina que actua com a servidor? I a la monitoritzada remotament?
- Quin servei s'utilitza al servidor per fer la monitorització? Com es reinicia o comprova el seu estat?
- Com es pot comprovar que la configuració del servidor es correcta?
- Quin servei s'utilitza a la màquina remota per fer la monitorització? Com es reinicia o comprova el seu estat?
- Què cal configurar al servidor per poder monitoritzar una màquina remota? I a la màquina remota?
- Com controla la màquina monitoritzada qui la pot monitoritzar?
- Com es configura el temps entre comprovacions d'un determinat paràmetre?
- Com garanteix la seguretat (control d'accés i privacitat) en la comunicació entre el servidor i la màquina remota que es monitoritza?
- Com heu configurat la màquina virtual que hostatja el servidor per facilitar l'accés a la seva UI?
- Com es pot verificar des de la línia de comandes que un servidor pot monitoritzar una màquina remota?
- Com es pot verificar des de la línia de comandes que una funcionalitat de monitorització concreta està correctament instal·lada?
- Com es pot verificar des de la línia de comandes que un servidor pot executar una funcionalitat de monitorització concreta en una màquina remota?
- Per una funcionalitat de monitorització concreta, que cal configurar per a poder visualitzar avisos en funció dels valors monitoritzats?
- Per una funcionalitat de monitorització concreta, com es pot passar com argument l'adreça IP de la màquina on s'executarà?
- Com es limiten els accessos als serveis d'una màquina?
- Com es comprova que aquests accessos han estat correctament limitats?

Informe pràctica 3 sessió 5:

*** Introducció de l'escenari:

Per configurar un servidor i màquines a monitoritzar amb Nagios, seguirem aquests passos:

Configuració dels paràmetres a monitoritzar:

Al servidor Nagios, monitoritzarem els següents paràmetres:

Càrrega del sistema.

Espai de disc dur (partició de root).

Utilització de la RAM.

Disponibilitat dels serveis SSH i HTTP a la pròpia màquina.

Disponibilitat del servei DHCP a la xarxa on es troba el servidor.

Als routers, monitoritzarem:

Càrrega del sistema.

Utilització de la RAM.

Disponibilitat del servei SSH.

Als servidors DNS, monitoritzarem:

Càrrega del sistema.

Utilització de la RAM.

Disponibilitat dels serveis SSH i DNS a les pròpies màquines.

Disponibilitat del servei DHCP a la xarxa on es troben els servidors DNS.

També verificarem la connectivitat i disponibilitat del servidor web declarat al domini seax.public.edu i dels servidors DNS utilitzats com a forwarders a la sessió 3.

Configuració dels noms d'equips i adreces IP:

Assignarem els següents noms d'equips i adreces IP:

routeraccs: 10.1.10.1

routerintern: 10.1.10.2

nagiosserver: 10.1.10.5

dns1: 10.1.10.3

dns2: 10.1.10.4

webserver (www.seax.public.edu): 147.83.2.135

Creació de grups:

Crearem dos grups:

routers amb els membres routeraccs i routerintern.

servidors amb els membres nagiosserver, dns1 i dns2.

Restricció de monitorització remota:

Només permetrem la monitorització remota des del servidor Nagios.

Comprovació de paràmetres cada minut:

Configurarem Nagios per comprovar l'estat de cada paràmetre monitoritzat cada minut.

Configuració de llindars d'avisos:

Establim llindars per als paràmetres a monitoritzar de manera que generin avisos quan siguin superats.

Comunicació segura entre el servidor i les màquines remotes:

Realitzarem captures per verificar que la comunicació entre el servidor Nagios i les màquines remotes és segura.

Quant a la protecció del servidor Nagios:

Només permetrem l'accés als serveis Nagios i SSH des de les adreces IP 10.1.10.11 i 10.1.20.11.

Si ho desitgem, podem implementar aquesta restricció i verificar el seu funcionament.

**** Instal·lació nagios:**

En una nova màquina virtual, basada en una màquina base sense cap paquet i instal·lació necessària, configurem la màquina amb una interfície per connectar-se a la xarxa dmz i que la seva ip sigui adreçada per el servei dhcp fet anteriorment.

Es pot obrir la màquina i canviar-li el nom de la màquina per així que es digui nagios i sigui clar quina màquina és quina.

Per fer això canviar el nom en els fitxers : /hostnames i posar: nagios

Una vegada configurada la màquina per instal·lar el servidor nagios s'han de seguir els següents passos:

Actualitzar la llista de paquets disponibles des dels serveis configurats anteriorment:

`apt update`

Instal·lació de paquets essencials per a un servidor web

`apt install -y apache2 libapache2-mod-php php php-gd php-cli gcc make unzip wget`

Explicació de cada paquet instal·lat:

apache2:

Instala el servidor web Apache HTTP. Proporcionar un servidor web per poder servir la interfície web de Nagios o altres aplicacions web.

libapache2-mod-php:

Modifica Apache per permetre l'execució de codi PHP.

Integrar PHP amb Apache, permetent que Apache processi fitxers PHP, necessari per a moltes aplicacions web com la interfície de Nagios.

php:

Instal·la el llenguatge de programació PHP. Proporcionar el llenguatge de script que s'utilitza per a les aplicacions web dinàmiques, incloent la interfície de Nagios.

php-gd:

Instal·la la biblioteca de gràfics GD per a PHP. Permetre la manipulació de gràfics en PHP, necessari per a moltes funcions de reporting i visualització.

php-cli:

Instal·la la interfície de línia de comandes per a PHP. Permetre l'execució de scripts PHP des de la línia de comandes, útil per a scripts de manteniment o automatització.

gcc:

Instal·la el compilador de GNU (GCC). Compilar programari des del codi font, necessari per a instal·lar i construir alguns plugins o eines.

make:

Instal·la l'eina de construcció Make. Automatitzar la compilació de programari, especialment en combinació amb GCC per a compilar plugins o altres eines des del codi font.

unzip:

Instal·la l'eina unzip per descomprimir fitxers. Permetre l'extracció de fitxers comprimits, útil per a descarregar i instal·lar programari empaquetat en fitxers ZIP.

wget:

Instal·la l'eina wget per descarregar fitxers des d'Internet. Permetre la descàrrega de fitxers, com ara paquets o actualitzacions, des de la línia de comandes.

Fitxers d'evidència:

configuració de la màquina: 1-1-instalacio-nagios.txt

*** Configuració de les altres màquines:

Per tenir el servei de nagios en els routers hem de configurar varies coses a les altres màquines del escenari:

Instal·lar els paquets del servei nagios i els seus plugins amb les seves dependències:
apt install -y nagios-nrpe-server nagios-plugins

I després en el fitxer de configuració del servidor nagios en els dos routers configurar les línies:

```
cat /etc/nagios/nrpe.cfg
# NRPE USER
# This determines the effective user that the NRPE daemon should run as.
# You can either supply a username or a UID.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd
```

```
nrpe_user=nagios
```

```
# 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=127.0.0.1,10.1.10.5
```

```
...
# COMMAND TIMEOUT
# This specifies the maximum number of seconds that the NRPE daemon will
# allow plugins to finish executing before killing them off.
```

```
command_timeout=60
```

CONNECTION TIMEOUT

This specifies the maximum number of seconds that the NRPE daemon will
wait for a connection to be established before exiting. This is sometimes
seen where a network problem stops the SSL being established even though
all network sessions are connected. This causes the nrpe daemons to
accumulate, eating system resources. Do not set this too low.

connection_timeout=300

Amb aquestes configuracions, el servidor NRPE està preparat per operar amb seguretat i eficiència, esperant connexions al port 5666, executant-se sota l'usuari i grup nagios. acceptant connexions des de les IPs especificades de 10.1.10.5 , i gestionant adequadament els temps d'espera per a ordres i connexions.

Ara fer un reboot als routers i servidors dns per aplicar els canvis anteriors:
systemctl restart nagios-nrpe-server

Fitxers d'evidència:

configuració de la màquina: 1-2-routeraccés.txt
1-2-routerintern.txt
1-2-dns1.txt

Fitxers involucrats:

- /etc/nagios/nrpe.cfg

Configurar el servei nagios pels routers d'accés i l'intern i els servidors dns.

*** Configuració del servei nagios:

Per configurar correctament el servei de nagios, hem de seguir uns passos específics per segons com vulguem que el servei funcioni i amb quins usuaris i quins serveis i hosts volguem monitoritzar:

Per fer això crear un usuari per nagios, Aquest usuari serà utilitzat per executar el procés de Nagios, aïllant-lo d'altres usuaris i processos per raons de seguretat.

useradd nagios

Afegir l'usuari www-data al grup de nagios, ja que www-data és l'usuari per defecte per al servidor web Apache i així pugui tenir els permisos necessaris per interactuar amb Nagios.

usermod -a -G nagios www-data

Ara en el directori de /tmp descarregar el codi font de nagios:

cd /tmp/

wget

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

Així descarregar el fitxer comprimit amb el codi font de Nagios des de GitHub i obtenir la versió específica de Nagios 4.4.6 per a la seva instal·lació.

Desempaquetar el fitxer comprimit:

```
tar xzf nagios-4.4.6.tar.gz
```

Per després poder compliar i instal·lar nagios des del codi font.

Per configurar el codi font de nagios, Configura el procés de construcció de Nagios, especificant que la configuració HTTPD es troba a /etc/apache2/sites-enabled, preparant el sistema per compilar Nagios amb la configuració necessària per integrar-se amb Apache:

```
cd nagios-4.4.6
```

```
./configure --with-httpd-conf=/etc/apache2/sites-enabled
```

Una vegada configurat compliar tot el codi font de nagios per poder executar el servei:

```
make all
```

(execució molt llarga ja que complia tot el codi font de nagios)

Una vegada tinguem el servei que es pugui executar, hem d'instal·lar i configurar varies coses abans per poder-lo executar correctament:

Crear els grups i usuaris necessaris per Nagios, i així assegurar-se que els usuaris i grups correctes estan configurats per executar Nagios de manera segura.

```
make install-groups-users
```

Repetir l'Afegit de www-data al Grup nagios per garantir que www-data té els permisos necessaris després de la creació dels usuaris i grups per Nagios.

```
usermod -a -G nagios www-data
```

Ara si instal·lar Nagios des del sistema:

```
make install
```

Tenint ara un servei Nagios correctament instal·lat, podem instal·lar altres serveis que necessitem per ser gestionat o tenir una millor aplicació amb la web apache:

Instal·la el script de servei de Nagios perquè pugui ser gestionat per systemd, que permet l'inici automàtic i la gestió de Nagios com un servei del sistema:

```
make install-daemoninit
```

Instal·lar els fitxers de configuració per defecte de Nagios, per tenir una configuració inicial per començar a utilitzar Nagios:

```
make install-commandmode
```

```
make install-config
```

Finalment Instal·lar la Configuració Web d'Apache per Nagios, per tenir la configuració necessària d'Apache per servir la interfície web de Nagios i permetre que Nagios tingui una interfície web accessible mitjançant Apache.

```
make install-webconf
```

Fitxers d'evidència:

configuració de la màquina: 2-configuracio-nagios.txt

***** Configuració del servei apache:**

El servidor Apache, formalment conegut com Apache HTTP Server, és un dels servidors web més utilitzats al món. És un projecte de codi obert gestionat per l'Apache Software Foundation. Apache serveix pàgines web als navegadors dels usuaris en resposta a les seves peticions HTTP. Això inclou la distribució de pàgines HTML, fitxers multimèdia, scripts, i altres continguts web.

Per configurar-lo ho hem anat configurant amb aquestes comandes:

Activar el mòdul rewrite en Apache, és utilitzat per reescriure URL's, el que permet redireccions i altres manipulacions d'URL en temps real. Això és essencial per a moltes aplicacions web que necessiten URL's amigables o redireccions basades en patrons específics.

```
a2enmod rewrite
```

Activa el mòdul `cgi` en Apache, que permet executar scripts CGI (Common Gateway Interface), que són necessaris per a certes aplicacions, com Nagios, que utilitzen scripts CGI per generar dinàmicament pàgines web basades en dades en temps real:

```
a2enmod cgi
```

Crea un fitxer de contrasenyes i afegeix un usuari `nagiosadmin`.

Configura l'autenticació bàsica per protegir la interfície web de Nagios, de manera que només els usuaris autenticats puguin accedir-hi, que en el nostre cas serà l'usuari nagiosadmin.

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

Reinicia el servei Apache

Per aplicar els canvis de configuració realitzats anteriorment, es necessita canviar la configuració del nagios perquè aquest funcioni segons les nostres especificacions

```
systemctl restart apache2
```

Iniciar el servei Apache i Assegurar que Apache està en execució després dels canvis de configuració.

```
systemctl start apache2
```

Configurar Apache per iniciar-se automàticament en arrencar el sistema i garantir que el servei Apache estigui sempre actiu després de reiniciar el servidor.

```
systemctl enable apache2
```

I finalment Mostra l'estat actual del servei Apache per poder verificar que Apache s'està executant correctament i que no hi ha errors.

```
systemctl status apache2
```

Fitxers d'evidència:

configuració de la màquina: 3-configuracio-apache.txt

**** Configuració del servei de monitoreig per nagios:**

Una vegada ja tenim la configuració del servidor de nagios i el servidor apache en la màquina nagios, el que hem de fer és configurar la màquina perquè tingui l'accés a les altres màquines i serveis a l'escenari per poder-li fer un monitoreig des de la web de apache, per això hem anat executant les següents comandes.

En el fitxer nagios.cfg és essencial per al funcionament de Nagios, conté totes les configuracions globals necessàries per al seu funcionament. És important configurar aquest fitxer correctament per assegurar-se que Nagios funcioni de manera òptima i eficient.

Per aquesta pràctica em he deixat que tingui servidors a qui monitoritzar, per això en aquest fitxer hem de descomentar la següent línia:

```
/usr/local/nagios/etc/nagios.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
```

Això permetrà que Nagios carregui totes les configuracions dels servidors que es trobin en aquest directori.

Per poder accedir a dit directori primer s'ha de crear la carpeta:

```
mkdir /usr/local/nagios/etc/servers
```

Ara com en la instal·lació del servidor nagios, hem de instal·lar els plugins necessaris per ja que són les eines essencials per a la monitorització que Nagios, s'utilitzen per comprovar l'estat de diversos serveis i recursos del sistema. Aquest paquet de plugins inclou moltes comprovacions predeterminades per a serveis com HTTP, SMTP, POP3, recursos del sistema com CPU, ús de disc, memòria, i altres components de xarxa i sistema.

```
wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz
```

Descomprimir l'arxiu descarregat:
`tar xzf nagios-plugins-2.3.3.tar.gz`

Entrar en la seva carpeta per poder fer el seu executable:
`cd nagios-plugins-2.3.3`

Abans de complir i treure el seu executable executar:

```
./configure --with-nagios-user=nagios --with-nagios-group=nagios
```

`./configure`: Aquest script s'executa des del directori de les fonts del programari i és part del sistema de construcció autotools.

`--with-nagios-user=nagios`: Aquesta opció especifica que l'usuari del sistema sota el qual s'executarà Nagios serà nagios. Això assegura que tots els fitxers i directoris creats durant la instal·lació tinguin les permissos adequats per aquest usuari.

`--with-nagios-group=nagios`: Aquesta opció especifica que el grup del sistema sota el qual s'executarà Nagios serà nagios. Similar a l'opció de l'usuari, això assegura que els permissos dels fitxers i directoris siguin apropiats per aquest grup.

Ara després d'aquestes comandes si que podem complir el programari dels plugins de nagios:

```
make
```

Finalment instal·lar els plugins en la màquina de nagios:

```
make install
```

Fitxers d'evidència:

configuració de la màquina: 4-configuracio-nagios-monitoreig.txt

Fitxers involucrats:

```
-/usr/local/nagios/etc/nagios.cfg
```

Configuració del funcionament del servidor nagios

*** Configuració dels servers:

Després s'ha de configurar el fitxers dels diferents hosts que el servei nagios té accés, en aquest fitxer haurem d'especificar tots els hosts que volem monitoritzar en aquest escenari:

Definir el servidor nagiosserver i els serveis que s'hi monitoritzen:

```
/usr/local/nagios/etc/servers/nagiosserver.cfg
```

```
define host {  
    use                linux-server  
    host_name          nagiosserver  
    alias              Nagios Server  
    address             10.1.10.5  
    max_check_attempts 5
```

```

    check_period      24x7
    notification_interval 30
    notification_period 24x7
}

define service {
    use          generic-service
    host_name     nagiosserver
    service_description Check Load
    check_command  check_nrpe!check_load
}

define service {
    use          generic-service
    host_name     nagiosserver
    service_description Check Disk
    check_command  check_nrpe!check_disk
}

define service {
    use          generic-service
    host_name     nagiosserver
    service_description Check RAM
    check_command  check_nrpe!check_mem
}

define service {
    use          generic-service
    host_name     nagiosserver
    service_description Check SSH
    check_command  check_ssh
}

define service {
    use          generic-service
    host_name     nagiosserver
    service_description Check HTTP
    check_command  check_http
}

define service {
    use          generic-service
    host_name     nagiosserver
    service_description Check DHCP
    check_command  check_dhcp
}

```

Aquest servei monitoritza:

1. **Check Load (Verificació de la càrrega):**

Monitora la càrrega del sistema per assegurar-se que el servidor no està sobrecarregat.

Línia: `check_nrpe!check_load`

Detectar quan la càrrega del sistema és massa alta, indicant un possible problema de rendiment.

2. **Check Disk (Verificació del disc):**

Monitora l'espai disponible en els discos del servidor.

Línia: `check_nrpe!check_disk`

Assegurar-se que hi ha prou espai en disc per evitar problemes relacionats amb l'emmagatzematge.

3. **Check RAM (Verificació de la memòria RAM):**

Monitora l'ús de la memòria RAM del servidor.

Línia: `check_nrpe!check_mem`

Detectar quan la memòria disponible és baixa, evitant problemes de rendiment per falta de memòria.

4. **Check SSH (Verificació de l'accés SSH):**

Monitora la disponibilitat del servei SSH.

Línia: `check_ssh`

Assegurar-se que el servei SSH està operatiu i permet l'accés remot segur al servidor.

5. **Check HTTP (Verificació del servei HTTP):**

Monitora la disponibilitat del servei web HTTP.

Línia: `check_http`

Assegurar-se que el servidor web està funcionant correctament i és accessible.

6. **Check DHCP (Verificació del servei DHCP):**

Monitora la disponibilitat del servei DHCP.

Línia: `check_dhcp`

Assegurar-se que el servidor DHCP està operatiu i assigna adreces IP correctament.

Configurar també de grups d'amfitrions o hostgroups en Nagios per poder monitoritzar:
`/usr/local/nagios/etc/objects/hostgroups.cfg`

```
define hostgroup {
    hostgroup_name routers
    alias          Routers Group
    members        routeraccs,routerintern
}

define hostgroup {
    hostgroup_name servers
    alias          Servers Group
    members        nagiosserver,dns1,dns2
}
```

Els grups d'amfitrions (hostgroups) en Nagios permeten agrupar diversos amfitrions que comparteixen característiques o funcions similars. Això facilita la gestió i la monitorització, ja que es poden aplicar les mateixes configuracions, notificacions i controls a tots els membres d'un grup. Per exemple nosaltres tenim:

Routers Group: Un grup per monitoritzar tots els routers de la xarxa. Això permet aplicar les mateixes verificacions i notificacions a tots els routers de manera centralitzada.

Servers Group: Un grup per monitoritzar tots els servidors. Això permet gestionar els servidors com una unitat i assegurar-se que tots ells compleixen amb els mateixos estàndards de monitorització.

Editar el fitxer de comandes per poder tenir comandes pròpies per la nostra monitorització, per això al final del document posar les següents línies:

```
/usr/local/nagios/etc/objects/commands.cfg
# Mis comandos

define command {

    command_name    check_nrpe
    command_line    /usr/lib/nagios/plugins/check_nrpe -H $HOSTADDRESS$ -c
$ARG1$
}

define command {

    command_name    check_disk
    command_line    /usr/lib/nagios/plugins/check_nrpe -H $HOSTADDRESS$ -c
check_disk
}

define command {

    command_name    check_load
    command_line    /usr/lib/nagios/plugins/check_nrpe -H $HOSTADDRESS$ -c
check_load
}

define command {

    command_name    check_mem
    command_line    /usr/lib/nagios/plugins/check_nrpe -H $HOSTADDRESS$ -c
check_mem
}
```

Així podem tenir les següents funcions:

check_nrpe:

línia: /usr/lib/nagios/plugins/check_nrpe -H \$HOSTADDRESS\$ -c \$ARG1\$

Aquest comandament utilitza el plugin check_nrpe per executar verificacions remotes en un host especificat per \$HOSTADDRESS\$, amb el comandament especificat per \$ARG1\$.

check_disk:

línia: /usr/lib/nagios/plugins/check_nrpe -H \$HOSTADDRESS\$ -c check_disk

Aquest comandament utilitza check_nrpe per verificar l'espai en disc en el host remot.

check_load:

línia: /usr/lib/nagios/plugins/check_nrpe -H \$HOSTADDRESS\$ -c check_load

Aquest comandament utilitza check_nrpe per verificar la càrrega del sistema en el host remot.

check_mem:

línia: /usr/lib/nagios/plugins/check_nrpe -H \$HOSTADDRESS\$ -c check_mem

Aquest comandament utilitza check_nrpe per verificar la memòria en el host remot.

Després de tota les configuracions verificar que la configuració de nagios ha estat correcte:

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

Si està ben configurat hauria de sortir:

Total Warnings: 0

Total Errors: 0

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

Finalment fer un reinici del servei de Nagios per aplicar els canvis:

`systemctl restart nagios`

I fer un reinici del servei de apache per aplicar els canvis:

`systemctl restart apache2`

Instal·lar altres paquets per

`apt install -y nagios-nrpe-server nagios-plugins`

`apt install -y nagios-nrpe-plugin`

Ara si tot va bé en el túnel fet al final de l'evidència connectat al router intern amb el localhost de la màquina externa, s'hauria de poder veure el servidor nagios funcionant amb la següent url: <http://localhost:8080/nagios/>

Fitxers d'evidència:

configuració de la màquina: 5-configuracio-servers.txt

Fitxers involucrats:

-/usr/local/nagios/etc/servers/nagiosserver.cfg
Configuració del servidor nagios i quin servei monitoreja
- /usr/local/nagios/etc/objects/hostgroups.cfg
Configuració dels grups de hosts en Nagios
- /usr/local/nagios/etc/objects/commands.cfg
Configuració de les comandes en Nagios

*** Verificacions

Les verificacions que podem fer des de terminal són limitades, ja que és una pàgina web i és una interfície visual, però el que podem fer és un wget de la pàgina de nagios i verificar que si que hi ha una web i que aquesta mostra informació per pantalla:

El contingut HTML mostrat demostra que la pàgina d'inici de Nagios s'ha descarregat correctament i inclou la definició d'una pàgina HTML amb frames (marcs) que fa servir per mostrar la interfície web de Nagios. Això indica que el servidor web de Nagios està funcionant correctament i que la pàgina principal és accessible.

La comanda wget ha funcionat correctament perquè:

- s'ha resolt el nom de domini del servidor
- S'ha establert una connexió amb el servidor.
- S'ha rebut una resposta HTTP 200 OK.
- S'ha descarregat el contingut del fitxer especificat.

Això confirma que la instal·lació i configuració del servidor web de Nagios s'han realitzat correctament i que el servidor és accessible via web.

Fitxers d'evidència:

verificació: 6-verificacio-wget-nagios.txt

Fonts d'informació:

Nagios4 Debian : <https://wiki.debian.org/Nagios4>

Debian monitoring amb nagios: <https://www.nagios.com/solutions/debian-monitoring/>

Instalar i configurar nagios a debian12:

<https://reintech.io/blog/installing-configuring-nagios-monitoring-debian>

Els paquets de pluguins de debian:

<https://packages.debian.org/search?keywords=nagios-plugins>

Instalar nagios en debian jessie:

<https://www.ochobitshacenunbyte.com/2015/10/29/instalar-configurar-nagios-debian-jessie/>

Errors en el server forum unix linux:

<https://community.unix.com/t/errors-on-the-nagios-server/383188>