- Quin programari cal instal·lar a la màquina que actua com a servidor? I a la monitoritzada remotament?

Instal·lem a la maquina de server nagios el servidor i els plugins per defecte trobem els passos a les guies d'instal·lació

https://support.nagios.com/kb/article/nagios-core-installing-nagios-core-from-source96.html#Debian 2.

https://support.nagios.com/kb/article/nagios-plugins-installing-nagiosplugins-from-source-569.html

Requisits per alguns del plugins:

https://support.nagios.com/kb/article/nagios-plugins-installing-nagios-plugins-from-source569.html#Debian

A la màquina a monitoritzar sera el client nrpe, seguirem els següents links

Agent nrpe: https://support.nagios.com/kb/article.php?id=515

Plugin check\_nrpe: veure «Install the check\_nrpe Plugin» a «Utilització de l'agent NRPE». https://support.nagios.com/kb/article.php?id=515#Debian

- Quin servei s'utilitza al servidor per fer la monitorització? Com es reinicia o comprova el seu estat?

La monitorització es fa servir nagios, i podem reiniciar el servei amb:

systemctl restart nagios.service

Per comprovar el seu estat, hem d'executar la següent comanda:

systemctl status nagios.service

- Com es pot comprovar que la configuració del servidor es correcta?

podem comprovar l’arxiu de configuració amb aquesta comanda:

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

- Quin servei s'utilitza a la màquina remota per fer la monitorització? Com es reinicia o comprova el seu estat?

La monitorització fa servir el servei agent nrpe

Podem reiniciar l’estat amb:

systemctl restart nrpe.service

Podem comprovar l’estat del servei amb:

systemctl status nrpe.service

- Què cal configurar al servidor per poder monitoritzar una màquina remota? I a la màquina remota?

A la màquina remota cal configurar el fitxer nrpe.cfg

que el trobarem a: etc/nagios/nrpe.cfg

A la maquina servidor hem afegit el usr/local/nagios/etc/nagios.cfg

- Com controla la màquina monitoritzada qui la pot monitoritzar?

En la linea allowed\_hosts, del arxiu /etc/nagios/nrpe.cfg de la maquina a monitoritzar allowed\_hosts=127.0.0.1,10.1.10.5 , permitint així que sigui monitoritzada pel servidor Nagios

- Com es configura el temps entre comprovacions d'un determinat paràmetre?

a l’arxiu : /usr/local/nagios/etc/objects/templates.cfg afegirem les lineas

check\_interval = 1

notification interval = 30

Cada (1) minut es comprova l’estat dels serveis i si troba un error s’enviara una notificació cada 30 minuts, aquest valor pot canviar si creiem que els serveis son mencys o més critics.

Es important aplicar aquests canvis del tempaltes.cfg a l’arxiu de configuracio

- Com garanteix la seguretat (control d'accés i privacitat) en la comunicació entre el servidor i la màquina remota que es monitoritza?

Per assegurar aquesta comunicació, es pot configurar NRPE per utilitzar **SSL/TLS**, que xifra la comunicació entre el servidor Nagios i les màquines a monitoritzar.

a la màquina a monitoritzar apt-get install nagios-nrpe-server nagios-plugins

al servidor nagios farem:

apt-get install nagios-nrpe-plugin

d’aqeusta menera podrem uttiltizar el plugin nrpe que protara SSL/TLS per sobre

haurem de modificar el fitxer de configuració /etc/nagios/nrpe.cfg

i afegirem:

ssl\_enabled=1

ara afegirem en /usr/local/nagios/etc/objects/commands.cfg

define command{

command\_name check\_nrpe

command\_line /usr/local/nagios/libexec/check\_nrpe -H “adreça\_host” -t 30 -c check\_nrpe

}

i haurem de reiniciar el servei:

systemctl restart nagios-nrpe-server

systemctl restart nagios.

Haurem d’activar regles de firewall que permeteixin trafic entre ambdues maquines (servidor i maquina nagios), regles al port 5666 (port que utilitza NRPE)

- Com heu configurat la màquina virtul que hostatja el servidor per facilitar l'accés a la seva UI?

Afegirem una ruta per poder accedir desde el nostre ordinador (windows)

route add 10.1.10.0 255.255.255.240 ip interficie eth-troncal

Ara podrem accedir a traves del navegadora : <http://10.1.10.5/nagios/>

Aqui son visibles els paràmetres a monitoritzar desde el servidor nagios

- Com es pot verificar des de la línia de comandes que un servidor pot monitoritzar una màquina remota?

podem utilizar el plugin Check\_ping per observar el correcte funcionament del servidor nagios i la màquina monitoritzada

/usr/lib/nagios/plugins/check\_ping -H 10.1.10.3 -w 100.0,20% -c 500.0,60%

També es poden utilitzar els plugins sobre altres serveis com http o ssh

- Com es pot verificar des de la línia de comandes que una funcionalitat de monitorització concreta està correctament instal·lada?

Al igual que en el punt anterior podem verificar cada funcionalitat concreta amb

/usr/lib/nagios/plugins/check\_ping -H 10.1.10.3 -w 100.0,20% -c 500.0,60%

canviant el check\_ping pel plugin del servei a verificar.

De la mateixa manera

- Com es pot verificar des de la línia de comandes que un servidor pot executar una funcionalitat de monitorització concreta en una màquina remota?

De la mateixa manera que en els apartats anteriors, els plugins poden determinar si la màquina te capacitats per executar la funcionalitat desitjada:

/usr/lib/nagios/plugins/check\_ping -H 10.1.10.3 -w 100.0,20% -c 500.0,60%

- Per una funcionalitat de monitorització concreta, que cal configurar per a poder visualitzar avisos en funció dels valors monitoritzats?

En l’arxiu /etc/nagios/nrpe.cfg afegirem els valors que s'ajusten a warning o critical segons servei i màquina, en el nostre cas hem escollit 15% per warning , 30 per% per critical, de forma que haurem d’afegir:

command[check\_load]=/usr/lib/nagios/plugins/check\_load -w 0.15,0.15,0.15 -c 0.30,0.30,0.30

degut a que la nostra maquina te una CPU, i 0,15 i 0.30 son els valors del 15 i 30 %

- Per una funcionalitat de monitorització concreta, com es pot passar com argument l'adreça IP de la màquina on s'executarà?

Tal i com hem fet en anteriors apartats, podem utilitzar el paràmetre -H per afegir una IP on es farà la comprovació a executar, és important que aquesta màquina sigui monitorizable per la màquina que esta executant el check.

/usr/lib/nagios/plugins/check\_ssh -H 10.1.10.3

- Com es limiten els accessos als serveis d'una màquina?

Tal i com hem après a sessions anteriors, podem limitar l'accés amb fail2ban sobre el servei ssh, en aquestes altures totes les màquines amb servei ssh, han estat securitzades amb fail2ban per afegir aquesta capa exta de gestió per limitar l'accés a les màquines .

podem instalar fail2ban amb la següent configuració

apt install fail2ban, i seguint les configuracions de la wiki proporcionada a clase, afegint els camps

[sshd]

maxrety = 3

al /fail2ban/config/jail.local i per arrelgar el bug esmentat DEFAULT]:

logtarget = SYSTEMD-JOURNAL

backend = systemd

enabled=true

bantime = 5m

ara per evitar que perdem la configuració al botar la maquina executarem les següents comandes: update-rc.d fail2ban defaults

systemctl restart fail2banservice

service fail2ban start

d’aquesta manera queda configurat el fail2ban.

- Com es comprova que aquests accesos han estat correctament limitats?

En aquesta ruta, /var/log/fail2ban.log trobem el log que guarda l’actitvitat registrada, i per tant els accesos que hi han bloquejats.

Per altre costat hem de veure abans de provar els accessos que el servei fail2ban est aixecat amb: fail2ban-client status