Services & Routing NOS: VyOS

VyOS (https://vyos.io) és un NOS lliure basat en Debian que, a més de proporcionar capacitats de gestió a L2 (i altres funcionalitats de xarxa de L4 o superior, com ara tallafocs -amb Nftables- i VPN -amb Wireguard-) a màquines físiques x86_64 i màquines VirtualBox, KVM i altres, com ja vam veure, on destaca sobre tot és en la gestió de rutes L3 mitjançant línia de comandes gràcies a incorporar per defecte la suite FRR (https://frrouting.org) amb tota la seva funcionalitat.

1.-PREVI) Configura la màquina VirtualBox "VyOS1" que vas utilitzar als anteriors exercicis de "switching" per a què ara tingui tres tarjes de xarxa en els següents modes i tot seguit arrenca-la:

* Tarja *eth0* (primera pestanya): mode "adaptador pont"
* Tarja *eth1* (segona pestanya): mode "xarxa interna" anomenada "Xarxa1"
* Tarja *eth2* (tercera pestanya): mode "xarxa interna" anomenada "Xarxa2"

a) Fes que la tarja en mode "adaptador pont" d'aquest sistema agafi una IP per DHCP. Això ho pots fer així:

configure
set interfaces ethernet eth0 address dhcp
set interfaces ethernet eth0 description "Una tarja" <-- Opcional
commit
save

NOTA: Existeix una forma més curta d'escriure la configuració d'un tarja de xarxa (i en general, de no haver de repetir múltiples vegades els mateixos elements de diferents opcions que tenen a veure amb un mateix objecte) fent servir la comanda *edit* Per exemple, la configuració anterior es podria haver escrit de forma abreujada així:

configure
edit interfaces ethernet eth0
set address dhcp
set description "Una tarja"
commit
save

aII) Comprova quina ha sigut l'adreça IP/màscara que ha obtingut la tarja *eth0* amb la comanda *run show interfaces* i la porta d'enllaç assignada (identificada com "0.0.0.0/0") amb la comanda ***run show ip route*** (també ho pots fer, respectivament, amb les comandes natives de Linux *ip -c a* i *ip -c r*). ¿Què mostra la comanda *run show dhcp client leases* ?

b) Executa *ping 8.8.8.8* ¿Funciona? Executa *traceroute 8.8.8.8* ¿Funciona? ¿I *mtr 8.8.8.8* (o equivalentment, *monitor traceroute 8.8.8.8*) ?

NOTA: Observa, amb el tabulador, que totes les comandes anteriors admeten, en lloc d'una IP, indicar una MAC o un nom DNS. La comanda *ping*, a més, admet paràmetres com *count nº* (per limitar el nº de pings), *interface ethX* (per indicar la tarja a usar per enviar i rebre els paquets), *ttl nº* (per indicar el TTL dels paquets), *flood* (per activar el mode "flood") ...

c) Comprova que la comanda *ping www.hola.com* no funciona; això és perquè encara no s'ha establert cap servidor DNS al sistema VyOS (aquesta informació no es té en compte tot i ser present en la resposta DHCP obtinguda). Estableix-lo executant la comanda *set system name-server 8.8.8.8* i tot seguit, després d'haver fet *commit* i *save* i de comprovar amb *show system name-server* (o *run show configuration*) que ja està fet, prova de nou la comanda *ping www.hola.com* ¿Què passa ara?

NOTA: En realitat, sí que es té en compte però s'associa només com a dada assignada a la tarja de xarxa en particular però no s'aplica la configuració al sistema. Per fer-ho, cal executar la comanda *set system name-server eth0*

d) Fes que una tarja en mode "no connectat" (com "eth1") tingui una IP fixa. Això ho pots fer executant:

configure
set interfaces ethernet eth1 address 172.19.1.2/16
commit
run show interfaces

NOTA: Més endavant veurem com assignar una porta d'enllaç per defecte manualment a una interfície concreta
NOTA: Recorda que si es vol desfer una ordre *set*, s'ha de canviar aquesta paraula per *delete* a la mateixa comanda. Per exemple, per esborrar la direcció IP fixa de la tarja eth1 anterior caldria executar *delete interfaces ethernet eth1 address x.x.x.x/y*. I que també existeix la paraula *edit* modificar un determinat ítem ja existent.
NOTA: Es poden veure els diferents "commits" realitzats al llarg del temps amb la comanda *show system commit* i els detalls d'un commit concret dels llistats (suposarem el nº 3) amb la comanda *show system commit diff 3*

e) Observant la sortida de la comanda (executada al mode operacional) *show configuration* ¿quina és la direcció MAC de *eth0*? Si ara observes la sortida de la comanda (també del mode operacional) *show configuration commands* , ¿quina creus que és la comanda que serveix per canviar aquesta direcció MAC?

f) ¿Què mostra la comanda (executada al mode operacional) *show protocols static arp (*o equivalentment, *show arp*)? En aquest sentit, ¿per a què serveix la comanda (executada al mode de configuració): *set system ip arp table-size 4096* ?

2.-a) Activa el servidor SSH que porta incorpora el VyOS executant (en el mode de configuració) les comandes *set service ssh; commit* i tot seguit comprova que tinguis el port 22 obert executant a la màquina VyOS la comanda *ss -tln*. Comprova a continuació que hi pots entrar des de la màquina real amb la comanda *ssh vyos@ip.tarja.mode.pont* Deshabilita finalment el servidor SSH de VyOS amb la comanda *delete service ssh ; commit* i comprova que ara ja no tens el port 22 obert i que no pots entrar des de la màquina real.

NOTA: Pots configurar més coses del servidor amb diverses opcions que apareixen tabulant després de *set service ssh ...* , com per exemple el port d'escolta -per defecte el 22-, amb el paràmetre *port nº* o l'adreça IP específica per on escoltar, amb el paràmetre *listen-address x.x.x.x* , entre molts d'altres. En tot cas, aquesta configuració es pugui establir fora de la per defecte es podrà consultant amb la comanda (del mode de configuració) *show service ssh*
NOTA: Per aturar el servidor SSH (i en general, tots els servidors que es posin en marxa amb l'ordre *set*) només cal canviar aquesta paraula per *delete* . Per exemple, així: *delete service ssh; commit*.
NOTA: Activar el servei SSH en un switch (amb SVI) o un "router" és una de les tasques que se sol fer el més aviat possible per poder accedir-hi al seu terminal de configuració remotament de forma còmoda sense haver de connectar-s'hi a través del port sèrie de forma local.

b) ¿Per a què serveixen cadascuna de les següents comandes? (no cal que les facis)

configure
set service dhcp-server shared-network-name unPool subnet 172.19.0.0/16 subnet-id 1
set service dhcp-server shared-network-name unPool subnet 172.19.0.0/16 range UnRang start 172.19.1.2
set service dhcp-server shared-network-name unPool subnet 172.19.0.0/16 range UnRang stop 172.19.1.100
set service dhcp-server shared-network-name unPool subnet 172.19.0.0/16 option default-router 172.19.1.1
set service dhcp-server shared-network-name unPool subnet 172.19.0.0/16 option name-server 172.19.1.1
commit

NOTA: Altres opcions interessants de *set service dhcp-server shared-network-name unPool subnet x.x.x.x/x* són, per exemple, *option domain-name "domini.com"*, *lease nº*, *exclude una.IP.del.Rang*, etc. D'altra banda, opcions interessants de *set service dhcp-server* en general són *listen-address x.x.x.x* o *listen-interface ethX*
NOTA: Un cop posat en marxa el servidor DHCP, comandes interessants per comprovar el seu correcte funcionament són *show service dhcp-server* així com *show dhcp server leases* i *show dhcp server statistics*
NOTA: Per aturar el servidor DHCP (i en general, tots els servidors que es posin en marxa amb l'ordre *set*) només cal canviar aquesta paraula per *delete* . Per exemple, així: *delete service dhcp-server; commit*. No obstant, fent-ho així, quan el volguessis tornar a habilitar hauries de tornar a executar totes les comandes *set service ...* un altre cop; si això no ho vols fer, pots deshabilitar-lo mantenint la configuració guardada per un futur si el vols tornar a habilitar amb la comanda *set service dhcp-server disable*

c) ¿Per a què serveixen cadascuna les següents comandes? (pots consultar la documentació corresponent a https://docs.vyos.io/en/latest/configuration/service/dns.html ; no cal que les facis)

configure
set service dns forwarding listen-address 172.19.1.2
set service dns forwarding name-server 8.8.8.8 o bé *set service dns forwarding system*
set service dns forwarding domain xeill.net name-server 192.168.15.10
set service dns forwarding allow-from 172.19.0.0/16
commit

NOTA: Una altra opció interessant de *set service dns forwarding ...* és *cache-size nº*
NOTA: VyOS no ofereix cap implementació de servidor DNS autoritatiu

El protocol NTP serveix per sincronitzar l'hora entre màquines. Per defecte, VyOS ja té funcionant un dimoni NTP que se sincronitza amb els servidors NTP oficial de VyOS, però aquests servidors poden canviar-se, així (sempre que tinguem la resolució de noms funcionant...si no, en lloc d'indicar el nom DNS del servidor NTP desitjat hauríem d'indicar la seva adreça IP):

configure
set service ntp server 0.pool.ntp.org [prefer]
commit

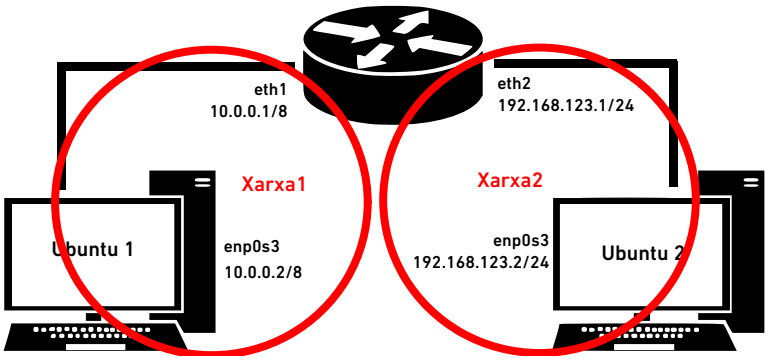
En tot cas, un sistema VyOS pot funcionar, un cop sincronitzat, com a servidor NTP al seu torn de les diferents màquines de la seva pròpia xarxa local, simplement indicant de quines adreces IP acceptarà peticions de sincronització (les quals poden ser de clients individuals, tipus 1.2.3.4 o bé de xarxes senceres, tipus 1.2.3.0/24), així:

configure
set service ntp allow-client address x.x.x.x[/y]
commit

NOTA: Altres opcions interessants de *set service ntp* són *listen-address x.x.x.x* o *interface ethX* , per restringir l'escolta de clients només a la IP o tarja de xarxa indicada, respectivament

d) ¿Què mostra la comanda (en mode operacional) *show ntp [system]*?

3.- PREVI) Configura les màquines "Ubuntu1" i "Ubuntu2" que vas utilitzar als anteriors exercicis de "switching" per a què ara tinguin ambdues una sola tarja de xarxa en mode "xarxa interna", la primera de les quals estarà ubicada en l'anomenada "Xarxa1" i la segona en "Xarxa2". Inicia aquestes dues màquines i a partir d'aquí fes els següents exercicis (l'esquema de xarxa que hi ha establert físicament és el mostrat al diagrama següent...les adreces IP les configurarem a continuació):



a) Estableix la configuració IP del sistema VyOS, així...:

configure
set interfaces ethernet eth1 address 10.0.0.1/8
set interfaces ethernet eth2 address 192.168.123.1/24
commit

... la del sistema "Ubuntu1" així (és molt important establir la màquina VyOS com la seva porta d'enllaç!)...:

sudo ip address add 10.0.0.2/8 dev enp0s3
sudo ip route add default via 10.0.0.1

... i la del sistema "Ubuntu2" així (és molt important establir la màquina VyOS com la seva porta d'enllaç!)...:

sudo ip address add 192.168.123.2/24 dev enp0s3
sudo ip route add default via 192.168.123.1

¿Què et mostra la comanda (del mode operacional de VyOS) *show ip route* ? ¿Pots fer ping entre "Ubuntu1" i "Ubuntu2" (o viceversa)?

b) La capacitat intrínseca d'un router de "transferir" paquets entrants per alguna de les seves tarjes (ubicada en una xarxa determinada) cap a una altra tarja (ubicada en una altra xarxa diferent) es diu "IP Forwarding" i ja ve activada per defecte a sistema VyOS, tal com mostra la comanda *show ip forwarding* (en el mode operacional). Comprova-ho

bII) Manté en marxa el "ping" entre "Ubuntu1" i "Ubuntu2" i llavors executa al mode de configuració del sistema "VyOS" la següent comanda: *set system ip disable-forwarding; commit* ¿Què li passa al "ping"? ¿Per què? Finalment, atura la màquina VyOS

NOTA: Als sistemes Linux "normals" passa justament al revès, que l'"IP-Forward" està deshabilitat per defecte (ja que normalment un sistema d'escriptori no farà tasques d'encaminament) però es pot habilitar si es necessita. Concretament, es pot fer de forma temporal executant (com a root) la comanda *sysctl net.ipv4.ip_forward=1 (p*er desactivar-lo només caldria canviar l'"1" per un "0") o de forma permanent assignant el valor "1" a la línia "net.ipv4.ip_forward=" del fitxer "/etc/sysctl.conf" i reiniciant el sistema.

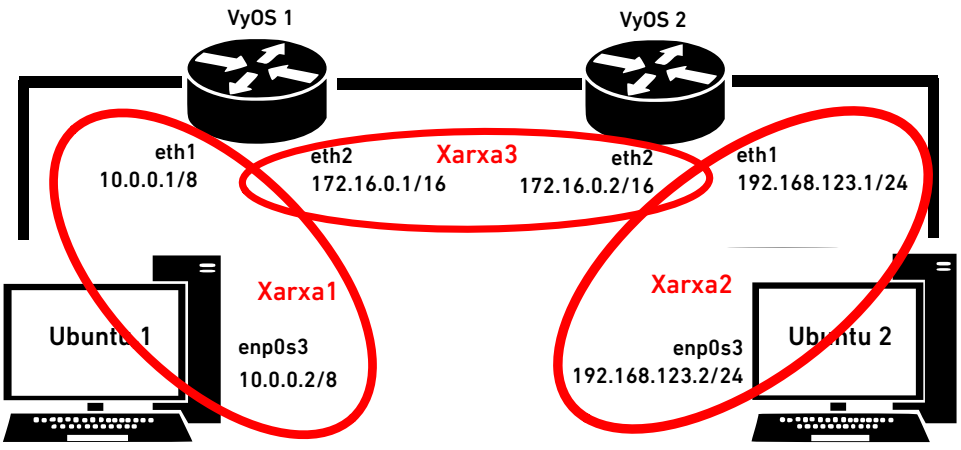
Al proper exercici estudiarem diverses tècniques de "routing" que permeten encaminar els paquets d'una xarxa a una altra no connectades directament en el mateix encaminador. Concretament, veurem les següents tècniques: encaminament estàtic, utilitzant el protocol RIPv2, utilitzant el protocol OSPFv3 i utilitzant el protocol BGPv4. Per realitzar aquesta tasca, el sistema VyOS disposa d'un servei anomenat "vyos-router", que ja funciona per defecte (*systemctl status vyos-router ; sytemctl cat vyos-router*) que no és res més que el programa FRR ja preconfigurat.

4.-. PREVI) En aquest exercici implementarem el següent diagrama de xarxa. Per fer-ho, continuarem utilitzant les mateixes màquines de l'exercici anterior però:

*A la màquina "VyOS1" canviarem la configuració de la seva tarja *eth2* per a què ara, tot i continuant en mode "xarxa interna", pertanyi a la xarxa anomenada "Xarxa3"

*Afegirem una nova màquina, "VyOS2" (pots reaprotifar la que ja vas utilitzar als anteriors exercicis de "switching"), la qual ara haurà de tenir tres tarjes de xarxa en els següents modes :

* Tarja *eth0* (primera pestanya): mode "adaptador pont"
* Tarja *eth1* (segona pestanya): mode "xarxa interna" anomenada "Xarxa2"
* Tarja *eth2* (tercera pestanya): mode "xarxa interna" anomenada "Xarxa3"



a) Arrenca el sistema "VyOS1" i estableix la seva configuració IP, així...:

configure
set interfaces ethernet eth1 address 10.0.0.1/8
set interfaces ethernet eth2 address 172.16.0.1/16
commit
save

...la del sistema "VyOs2" (que també hauràs d'arrencar, òbviament), així...:

configure
set interfaces ethernet eth1 address 192.168.123.1/24
set interfaces ethernet eth2 address 172.16.0.2/16
commit
save

... la del sistema "Ubuntu1" igual que a l'exercici anterior, així ...:

sudo ip address add 10.0.0.2/8 dev enp0s3
sudo ip route add default via 10.0.0.1

... i la del sistema "Ubuntu2" igual que a l'exercici anterior, així ...:

sudo ip address add 192.168.123.2/24 dev enp0s3
sudo ip route add default via 192.168.123.1

* ¿Pots fer ping entre "Ubuntu1" i "Ubuntu2" (o viceversa)? La resposta ha de ser no i has de trobar el per què en la sortida de la comanda del mode operational *show ip route* executada a ambdues màquines VyOS

---

b) Cal afegir una ruta estàtica al sistema "VyOS1" per a què pugui anar a la xarxa 192.168.123.0/24 utilitzant com a "salt" la IP 172.16.0.2, executa i una altra ruta estàtica al sistema "VyOS2" per a què pugui anar a la xarxa 10.0.0.0/8 utilitzant com a "salt" la IP 172.16.0.1. És a dir:

*Executa les següents comandes a "VyOS1"...:

configure
set protocols static route 192.168.123.0/24 next-hop 172.16.0.2
commit

*...i executa les següents comandes a "VyOS2":

configure
set protocols static route 10.0.0.0/8 next-hop 172.16.0.1
commit

bII) Comprova que s'ha afegit la ruta adient (a la tarja que toca!) executant de nou (al mode operacional) *show ip route* i també amb la comanda (al mode de configuració) *show protocols* a les dues màquines VyOS ¿Pots fer ping entre "Ubuntu1" i "Ubuntu2" (o viceversa) finalment?

bIII) ¿Què significaria indicar "0.0.0.0/0" a l'ordre *set protocols static route 0.0.0.0/0 next-hop 1.1.1.100* **?**

---

c) Esborra la ruta estàtica establerta a l'apartat anterior executant a ambdues màquines VyOS les comandes *delete protocols static; commit* Per curiositat, pots provar de tornar a fer un ping entre les màquines "Ubuntu1" i "Ubuntu2" per comprovar que ja no funciona

cII) Per defecte, VyOS ja té activats els protocols d'enrutament RIP, OSPF i BGP a més de l'encaminament estàtic (entre altres); això ho pots confirmar executant (al mode operacional) la comanda *show system routing-daemons* Comprova-ho.

cIII) Ara implementarem en cada router el protocol RIP. D'aquesta manera, la resta de routers de la xarxa seran notificats de les xarxes a les què el router en qüestió hi està directament connectat (i per tant, les xarxes a les què s'hi podrà arribar a través d'ell). És a dir:

*Executa les següents comandes a "VyOS1"...:

configure
set protocols rip network 10.0.0.0/8
set protocols rip network 172.16.0.0/16
commit

*...i executa les següents comandes a "VyOS2":

configure
set protocols rip network 172.16.0.0/16
set protocols rip network 192.168.123.0/24
commit

cIV) Comprova que s'ha afegit la ruta adient amb *run show ip route* i *show protocols* a les dues màquines VyOS ¿Què mostra la comanda *run show ip rip*?¿Pots fer ping entre "Ubuntu1" i "Ubuntu2" (o viceversa)?

---

d) Esborra la configuració de RIP realitzada a l'apartat anterior executant a ambdues màquines VyOS les comandes *delete protocols rip; commit* Per curiositat, pots provar de tornar a fer un ping entre les màquines "Ubuntu1" i "Ubuntu2" per comprovar que ja no funciona

dII) Ara implementarem en cada router el protocol OSPF. D'aquesta manera, a l'igual que passava amb el protocol RIP, la resta de routers de la xarxa seran notificats de les xarxes a les què el router en qüestió hi està directament connectat (i per tant, les xarxes a les què s'hi podrà arribar a través d'ell). És a dir:

*Executa les següents comandes a "VyOS1"...:

configure
set protocols ospf area 0 network 10.0.0.0/8
set protocols ospf area 0 network 172.16.0.0/16
commit

*...i executa les següents comandes a "VyOS2":

configure
set protocols ospf area 0 network 172.16.0.0/16
set protocols ospf area 0 network 192.168.123.0/24
commit

NOTA: Si es volgués no publicar via OSPF la xarxa connectada a una determinada tarja de xarxa (per exemple, eth0), es podria executar *set protocols ospf passive-interface eth0* En general, després de set protocols ospf hi ha molts paràmetres (route-id, default-information originate always ,...)que permeten configurar el seu comportament de forma molt prima

dIII) Comprova que s'ha afegit (després d'uns segons) la ruta adient amb *run show ip route* i *show protocols* a les dues màquines VyOS ¿Què mostra la comanda *run show ip ospf [neighbor|route]*? ¿Pots fer ping entre "Ubuntu1" i "Ubuntu2" (o viceversa)?

---

e) Esborra la configuració de OSPF realitzada a l'apartat anterior executant a ambdues màquines VyOS les comandes *delete protocols ospf; commit* Per curiositat, pots provar de tornar a fer un ping entre les màquines "Ubuntu1" i "Ubuntu2" per comprovar que ja no funciona

eII) Ara implementarem en cada router el protocol BGP. En aquest cas, en ser un protocol de "vora exterior", no es notifiquen les xarxes de forma indiscriminada sinó se n'informa als veïns amb els quals es vol tenir comunicació. És a dir, el sistema "VyOS1" haurà de notificar explícitament al sistema "VyOS2" de la possibilitat d'arribar a la seva xarxa pròpia 10.0.0.0/8 i, d'altra banda, el sistema "VyOS2" haurà de notificar explícitament al sistema "VyOS1" de la possibilitat d'arribar a la seva xarxa pròpia 192.168.123.0/24. És a dir:

*Executa les següents comandes a "VyOS1"...:

configure
set protocols bgp system-as 1234 <--El nº és l'ASN propi (assignat per l'IANA, se suposa)
set protocols bgp parameters router-id 172.16.0.1 <--Opcional: indica la IP "de cara" al veí
set protocols bgp neighbor 172.16.0.2 remote-as 5678 <--Identifica al veí
set protocols bgp neighbor 172.16.0.2 address-family ipv4-unicast <--Indica el tipus d'IPs que es rebrà del veí
set protocols bgp address-family ipv4-unicast network 10.0.0.0/8 <--Informa al veí de la xarxa pròpia interna
commit

*...i executa les següents comandes a "VyOS2":

configure
set protocols bgp system-as 5678
set protocols bgp parameters router-id 172.16.0.2
set protocols bgp neighbor 172.16.0.1 remote-as 1234
set protocols bgp neighbor 172.16.0.1 address-family ipv4-unicast
set protocols bgp address-family ipv4-unicast network 192.168.123.0/24
commit

NOTA: Una alternativa al darrera comanda, per no haver d'indicar vàries comandes diferents si n'hi ha vàries xarxes internes a publicar, és publicar-les totes de cop amb una sola comanda: *set protocols bgp address-family ipv4-unicast redistribute connected*
NOTA: A diferència del que passa amb una instal·lació estàndard de FRRouting, als sistemes VyOS el valor "ebgp-requires-policy" està deshabilitat per defecte (per compatibilitat amb versions de VyOS anteriors). Si es volgués activar caldria executar la comanda *set protocols bgp parameters ebgp-requires-policy*

eIII) Comprova que s'ha afegit la ruta adient amb *run show ip route* i *show protocols* a les dues màquines VyOS ¿Què mostra la comanda *run show ip bgp [neighbors|summary]*? ¿Pots fer ping entre "Ubuntu1" i "Ubuntu2" (o viceversa)?

5.-a) ¿A quina comanda de Linux equival la comanda (en mode operacional) *monitor traffic interface eth0*?

NOTA: El paràmetre *filter* de la comanda *monitor traffic interface ethX* accepta qualsevol expressió BPF escrita entre cometes (per exemple: "port 25" o "port 161 and udp"). El paràmetre *save* permet guardar el tràfic esnifat en un fitxer

b) ¿A quina comanda de Linux equival la comanda (en mode operacional) *monitor bandwith interface eth0*?

NOTA: Pots pulsar "d" per obtenir informació més detallada o "i" per informació addicional. Per sortir pulsa "q" i "y"

c) ¿A quina comanda de Linux equival les comandes (en mode operacional) *monitor bandwith-test accept* i *monitor bandwith-test initiate*?

d) ¿A quina comanda de Linux equival *monitor command "una_comanda_operacional_qualsevol"*?

e) ¿A quina comanda de Linux equival la comanda *monitor log* ?

6.-a) ¿Què explica aquest enllaç: https://docs.vyos.io/en/latest/automation/command-scripting.html? ¿I aquest altre (més avançat): https://docs.vyos.io/es/latest/automation/vyos-pyvyos.html?

b) ¿Què explica aquest enllaç: https://docs.vyos.io/en/latest/configuration/container i quines possibilitats creus que pot aportar aquesta funcionalitat de VyOS (un exemple el podem trobar aquí: https://blog.showipintbri.com/blog/suricata-vyos) ?

c) ¿Què explica aquest enllaç: https://docs.vyos.io/en/latest/configuration/service/https.html conjuntament amb aquest: https://docs.vyos.io/en/latest/automation/vyos-api.html ?