**Linux Advanced.**

**1.2 Remote Access via PuTTY**

Access via een bepaalde tool vanop de client. Serversystemen staan vaak in de omgeving met klimaatcontrole en achter slot en grendel. De beheer gebeurt meestal vanop de aftand via Remote Access via Terminal, er is geen GUI. We gebruiken commandline tools om op afstand in te loggen, bestanden te kopiëren en commando’s te gaan uitvoeren. De meeste tools bevatten SSH (Secure Shell). Er bestaan ook andere tools als scp (veilig kopiëren over netwerk), sftp (bestanden interactief en veilig kopiëren) berichten worden versleuteld. Andere oudere tool Telnet-geen encryptie.

Onder SSH hebben een client en een server.

**$sudo su** – root access geven

**#dnf list installed | grep ssh** – kijken wat geïnstalleerd is, en lijst de pakketten op die ssh bevatten

**#dnf install -y openssh-server of openssh – client** – indien de het niet geïnstalleerd is

Als openssh service op uw Linux distro staat dat wil niet zeggen dat die op de achtergrond opstart het kan zijn dat je die manueel moet opstarten.

**# systemctl ststus sshd.service** – kan je zien of ssh aan het draaien is,

**# system start sshd.service** – start je deze manueel.

**# systemctl enable sshd.service** – om daemon automatisch te laten draaien bij het opstarten.

Vanop de client verbinding maken met een server (via PuTTY)

**# ip a** – om een ip te achterhalen vb 10.0.2.15

**# lsof -i -P-n | grep sshd** – om een poort te achterhalen dus om te zien of de poort op LISTEN staat

Poortdoorverwijzingregel toevoegen: 1) vm uitzetten, 2) instellingen van vm, 3) Netwerk, 4) Geavanceerd, 5) Poortdoorwijzing daarna voeg je een regel toe.

Indien je problemen hebt met Poort 22: Root# cat /etc/ssh/sshd\_config of vim /etc/ssh/sshd\_config of nano /etc/ssh/sshd\_config

Ssh sessie openen via andere Linux client: root# ssh remoteuser@remote-ip-address

Indien je extra beveiliging wilt zodat root zich niet kan inloggen vanop de afstand: root# grep PermitRootLogin /etc/ssh/sshd\_config dan zie bij PermitRootLogin yes staan, dus via root# vim /etc/ssh/sshd\_config verander die Yes naar No.

Daarna ssh sessie herstarten: root# systemctl restartsshd.service

**1.3 Remote Access Xming**

Grafische applicatie runnen moeten we Xming gebruiken op onze fysieke toestel. Xming downloaden en installeren: [https://sourceforge.net/projects/xming/](https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqbm56QjQtZ2NKcng5bnJEc1JPY0RPTlVFbWV0d3xBQ3Jtc0tsMFN5bTI4bndzTVNHRjljT0liYlJaQ2MyQ1FELUxnaTFTUEZrb245QUh4OGw4S0x5OUFEX01uUV92LVI0aGFjMXMyOVk3VUVRVGRmMjltTlY4emtmb25oeXMzeWJHanZsUEtxMkZEWHRjd3pVYlRhYw&q=https%3A%2F%2Fsourceforge.net%2Fprojects%2Fxming%2F)

root# grep X11Forwarding /etc/ssh/sshd\_config

X11Forwarding moet op Yes staan. Indien dit niet zo is kan je deze aanpassen door # vim of nano /etc/ssh/sshd\_config

In PuTTY geef je de naam van een host, daarna ga je naar SSH vervolgens Auth en daarna X11 en daar X11 forwarding aanvinken.

Indien het niet lukt op gedit op te starten via X11 probeer dan eerst uit te loggen op uw vm.

**1.4 Remote Access via client VM**

We gaan onze VM eerst klonen: Volle kloon, Huidige staat oernemen -> MAC-adres Policy: Genereren nieuwe MAC-adressen voor alle netwerkadapters. In Oracle VM VirtualBox ga je naar: Bestand -> Voorkeuren -> Netwerk -> nieuw NatNetwerk toevogen -> Ok

Twee VM aan een NatNetwerk koppelen: selecteer eerte vm: Netwerken -> Netwerkadapter ingeschakeld aanvinken -> Gekoppeld aan: NAT-netwerk -> dan kies je NAT-netwerk die je hebt aangemaakt. Dan doe je exact hetzelfde bij de tweede VM.

Maak op voorhand snapshots

Controleer de IP adressen in beide VM’s

Gaa naar Terminal in VM1 en start de ssh-connectie: ssh username@ip-adres.

Om PuTTY ook te laten connecteren, VB anders instellen: Voorkeuren -> Netwerken -> dubbel klikken op NatNetwork -> Portdoorverwijzing -> nieuwe poort toevogen -> poort 22 voor ssh-connectie

**1.5 Remote bestanden kopieren via scp en rsync.**

Scp dient om bestanden tussen de systemen uit te wisselen op een veilige manier

Zorg dat je altijd connected bent.

**#vim /home/tom/testbestand**

**#cat /home/tom/testbestand**

Hallo, Tom

#scp /home/tom/testbestand [tom@10.0.2.15:/tmp](mailto:tom@10.0.2.15:/tmp)

Dus het commando is: scp /path/to/local/file remoteuser@remote-ipaddress:/path/to/remote/file

Scp remoteuser@remote-ipaddress: /path/to/remote/file /path/to/local/file

Om heel de map te kopiëren: scp -r /home/tom/ [tom@10.0.2.15:/tmp](mailto:tom@10.0.2.15:/tmp)

Rsync is beter in het maken van Backups( als je backups wilt kopiëren gebruik je beter rsync) want de scp commando laat attributen zoals permissies en zo verloren gaan.

Rsync -a recursief arkive

Rsync -v verpoost

Rsync -l kopieren van symbolische links ---- dus rsync -avl /home/tom [tom@10..2.15:/tmp](mailto:tom@10..2.15:/tmp) om backup te kopiëren.

Als je wilt dat de inhoud van twee directory hetzelfde is rsync -avl –delete

**1.6 Interactief kopiëren via sftp**

Indien je niet op voorhand waat wat je allemaal wilt gaan kopieren vanop afstand.

Sftp [tom@10.0.2.15](mailto:tom@10.0.2.15) in mijn vm1 om te kopieren naar mijn vm2

Sftp> ls of lls

Sftp> put /home/tom als ik een file wil versturen.

Bij gewoon ftp wordt alle data gewoon als pure tekst doorgestuurd dus niet geincripteerd

**1.7 Key-based passwordloze authenticatie**

**Ssh-keygen** om sleutels aan te maken

**#ls /home/tom/.ssh** om te zien of deze key er is

**#ssh-copy-id -i ~/.ssh/id\_rsa.pub tom@** -om de public key te kopieren naar een vm2

Dit werkt ook voor sftp en scp

**1.8 System logging**

Rsyslog – in moderne RedHat lereases ler-vert rsyslog boodschappen die worden verzamelt en opgeslegen system d journal.

Jounalctl om boodschappen te bekijken

Rsyslogd aanvaard boodschappen van ander programma’s die op dezelfde computer liggen en schrijft die weg naar de juiste logbestenden. Dus zorgt ervoor de we centraal de logbestanden kunnen beheren. Log boodschappen zijn standaard niet geincrepteerd.

Deze boodschappen komen in submappen terecht

Cat /etc/rsyslog.conf om te zien wat er in zit

Sudo dnf install rsyslog om rsyslog te installeren

Vim /etc/rsyslog.conf – om te openen in vim en aanpassingen doen. Voornamelijk gaan we in Rules werken.

**# vim /var/log/messages**  om te zien wat er in die submappen staat

/var/log/messages is een heel belagrijk via deze logfile kunnen we gemakkelijk krack pogingen zien en detecteren.

**1.9 Schijfruimte en diskverbruik**

Df  om schijfruimte te controlleren

Df -h  om in leesbaar formaat te zien.

Df -T om te zien van welke typen er zijn

Df -t en de naam van mijn type bv df -t tmpfs

Df -x tmpfs alles behalve tmpfs

Du om disk verbruik te zien

Du -h human readiable

Find  kan ik mijn bestandsverbruik zien in verschillende criteria

**# find / -xdev -user tom -print | xargs ls -lds > /tmp/tom** ik zoek in mijn root naar bestanden van tom en die bestanden ga ik printen en die bestanden ga ik tonen als longlisting en kopieren naar een bestand /tmp/tom

**#find / -xdev -size +100M | xargs ls-lds > /tmp/size**  zo zien we welke bestanden groter zijn dan 100M

**2.1 Netwerkbeheer via NetworkManager**

NetworkManager

Standaard staat internet verbinding af omdat het veilig is offline te starten dan meteen online uw system om te starten

Bedraad (Wired)

Draadloos (Wireless)

VPN

Bij het opstarnet van een computer word automatisch verbinding gemaakt met DHCP server de computer krijgt automatisch een IP adres

Ip addr show enp0s3  om een ip adress te zien

We kunnen zelf routes instellen. Als je een bepaald ip adres wilt verbinden zal de computer routing table doorzoeken en bepaalde pad kiezen. Het versturen van die gegevens zal gebeuren via pakketjes.

Lo interface- dat zijn pakketjes die bedoeld zijn voor lokaal systeem. Dus die worden lokaal verzonden en niet door de internet en worden rechtstreeks naar NIC verstuurd.

route -n  huidige routes controleren

Routes zelf instellen  ga naar NetworkManager  wired settings en klik op + teken ipv4 en route instellen en bij het adres geven we het subnet adres in waar dat we routen naar gaan maken.

Gateway geeft toegang tot een nieuwe route.

route -n om een nieuwe route te controleren.  en kan je zien dat die ook toegevoegd is.

**2.1 Netwerkbeheer**

ip a zie je alle interfaces opgelijst zijn

ip addr show hetzelfde commando

ip addr show +de naam van ip die je wilt zien

lo is alles wat local is

Als we geen virtual bridge willen gebruiken dan moeten we die gaan uitzetten:

sudo su

**# systemctl disable libvirtd**

En daarna reboot.

Ifconfig enp0s3 om informatie van dit netwerk te zien(toont meer dan ip addr show commando)

RX-received-ontvangen

TX-transmitted-verzonden

Ping – om van vm1 naar een vm2 te pingen (CTRL+C om pingen te stoppen)

Als je de route van het begin tot einde wilt controleren: traceroute -I ( dit is een hoofdletter I en l-niet kleine L)

Hostname of hostnamectl set-hostname –static “Nieuwhostname” en dan op enter als je het wilt veranderen.

Dnsdomainname -A  om een domain naam op te lijsten

**2.3 Netwerkbeheer Proxy Server instellen**

Proxy Server  De http aanvragen gaan naar de proxy server en die gaat die dan doorsturen naar een internet. Op de Proxy zelf kunnen we ook instellen naar welke website dat we wel en niet kunnen surfen.

Manier 1: via NetworkManagerNetworkProxy

Manier2: via Brouwserabout:preferences of via preferences in een menuNetwork Settings helemaal onderaan  Settingsen kies manueel en stel die daar in.

De poort is geassocieerd met de Proxy Server (standaard is de poort 3128) het kan zijn dat op de Proxy Server een andere poort voorzien is.

Als je bepaalde localhost gegevens of ingeeft bij No Proxy for: gaan die communicaties nooit plaats vinden via Proxy. Die worden gescheiden door ; .

**2.4 Netwerkbeheer via nmtui. (command line tool)**

Via root access

**#nmtui**  komen we in grafische interface terecht, kan handig zijn voor basis instellingen van netwerken.

**2.5 Ethernet channel bonding meerdere NIC’s (=meerdere NIC gaan koppelen aan een IP-adress)**

Waarom? 1. High availability hoge beschikbaarheid. Indine een NIC het begeeft kunnnen nog altijd terug vallen op andere NIC.

2. Performance: een NIC te veel netwerk verkeer krijgt dan kunnen we de workload verspreiden over meerdere NIC.

nmcl commando  Root acces nodig

1. VM uitzetten
2. Selecteer eerste VM in VirtualboxInstellingen
3. Netwerk  adapter een is aangevinkt
4. Adapter 2 inschakelen aansluiten op NAT-netwerk en dan op OK
5. VM starten

Terminal:

#nmcli connection show - om connecties te zien

Sudo su  nmcli connection delete id +denaamvanid ( Hiermee gaan we de connecties verwijderen)

#nmcli connection add type bond con-name +denaamvanbond ifname bond0 mode active-backup (om een nieuwe connectie toe te voegen)

Instellingen van deze connectie aanpassen: ip adress, gateway en dns (#nmcli connection modify (name) ipv4-addresses +ipadres gw4 +ipadress ipv4.dns “……..”

Manueele connectie ( nmcli connection modify mybond0 ipv4.method manuel)

Slives toevoegen

**#nmcli connection add type bond-slave con-name +naam-eth0 ifname enp0s3(slaves) master bond0(master)**

Bond connecties aanzetten : **#nmcli connection up mybond0**

**#nmcli connection show**

Bond slaves opzetten **(#nmcli con up mybond0-+denaam)**

Verbindingen in file checken **( ls /etc/sysconfig/netwrok-scripts)**

**network-scripts# ip addr show**

**network-scripts# cat /proc/net/bonding/bond0** (meer info over bond0)

**network-scripts# ifenslave -c bond +denaamvanslave** (om een andere slave te activeren)

**network-scripts# ifdown mybond0-eth0** (om slave uit te zetten)

**network-scripts# ifdown mybond0** (om bond uit te zetten)

**2.6 Netwerconfiguratiebestanden**

Configuratiebestanden aanpassen (via script of manueel)

Rechtstreeks aanpassen network manager service uitzetten**: # systemctl stop NetworkManager**

**#systemctl start NetworkManager** – om te starten

**#systemctl disable NetworkManager** (zodat deze niet opstart samen met de pc)

**#systemctl enable NetworkManager** (zodat deze opnieuw te laten starten met de pc)

Kijken in welke map Netwerkroutes en netwerkinterfaces aanpassen **(#ls /etc/sysconfig/network-scripts)**

Netwerk configuratie aanpassen: #cat /etc/sysconfig/network-scripts

**network-scripts]# +commando** om te zien wat er in die map zit.

In vim of nano kunnen we de gegevens van bond aanpassen.

**# ifconfig** – de status van netwerken

Routes instellen: **# cd /etc/sysconfig/network-scripts**

Network-scripts**]# vim route-mybond0** (routes instellen)  we komen in vim terecht en hier vullen we onze routes in bv: adresses, netmask, gateway.

Network-scripts]#route -n (om te kijken of deze ingesteld is maar eerst NetworkManager opzetten **#systemctl stop NetworkManager** of systemctl start NetworkManager: suso su )

Network-scripts]#cat /etc/hostname (hostname wordt in dee map bewaard.)

Network-scripts]#vim /etc/hostname (om de hostname te veranderen en daarna reboot)

Nog een belangrijke map #cat /etc/hosts (kan je gebruiken om hostnamen aan de adressen te koppelen in een kleine netwerk of aliasen creëren.)

**#vim /etc/hosts** (om een andere vm toe te voegen bv maar daarna reboot)

DNS servers of zoekdomainen wil instellen: # cat /etc/resolv.conf (daar zitten dns servers die werken in volgorde, maar we kunnen deze ook aanpassen via vim)

**#host redhat.com** (om te controlleren of dns servers juist zijn ingesteld)

**#dig redhat.com** ( geeft meer uitleg dan host commando)

**3.1 Services Inleiding**

Services worden vaak geïmplementeerd als een daemon-process op de achtergrond.

**3.2 Initialisatie daemon**

Het process waar al de processen gaan volgen.

**#init 0 (**dan wilt mijn computer afsluiten)

**#systemd** (voor systemd initialisatie)

PID 0 voor Linux kernel

PID 1 voor init/systemd

PID 0 is de parent van de init/systemd

Init of systemd die starten processen ook op die zodanig zijn ingesteld dat ze bij het booten mee moeten opstarten.

Oude init systemen waren niet gemaakt om met veel services te gaan omgaan. Ze waren vooral gebaseerd op statische hardware omgeving (SysViNit)

**#ps -e | head** (om te zien met welke init system we werken) maar er is ook backward compatible.

**3.3 Klassieke init daemons**

Het kan zijn dat we soms met oudere systemen gaan werken. Systemd is gebaseerd op de oude init daemons.

Init en SysViNit zijn klassieke init daemons

Init – haalt zijn configuratie info uit /etc/ttytab maar tegenwoordig ook uit /etc/inittab

Standaard gezien werken we met runlevel 5. Runlevel is een nummer dat gaat bepalen welke services gaan starten en welke gaan stoppen. Runlevels 2 tot 5 mag je gebruiken om als default runlevel te gaan instellen. Als je toch 6 gaat instellen dan gaat de computer herstarten.

**#init 0 pc uitzetten**

**#init 6 pc rebooten**

**#init 3** (als ik wil troubleshooten en mijn grafische omgeving uitzetten)

**#runlevel** (om te zien welke level er gebruikt wordt. N = nonexistant)

Alle symbolische linken staan in de map init.d die worden gerunt als je op een runlevel komt.

K: staat voor kill bij scripts

S: staat voor start bij de scripts

**3.4 Systemd theaorie**

Systemd initialisatie daemon gaat de klassike initiatie daemon zoals SysVinit of init gaan vervangen. Systemd is sneller omdat deze de services parallel kan opstarten maar in plaats van runlevels zoals bij init gaan we bij systemd targets gebruiken. Kan ook units beheeren, de service unit beheerd de daemons op de server en de target is een soort groepering van units.

**$ systemctl list-units | grep .service** (om mijn lijst met services op te lijsten)

**$ systemctl list-units | grep .target (**om mijn lijst met targets op te lijsten)

**$systemctl list-init-files –type=service** (om configuratie bestanden te bekeken van service units)

Enabled = aan, disabled = uit, static = statisch aan (standaard gezien enabled is maar kan nooit disabled worden.)

**$man systemd (** om meer te weten over systemd)

**3.5 Systemd beckwards compatibility met SysVinit**

Target unit configuratie bestanden symolisch gelinkt zijn aan de eigenlijke target unit configuratie systemd

**$ls -l /lib/systemd/system/runlevel\*.target**

**3.6 Systemd Services starten en stoppen**

Status van services checken: **$systemctl list-unit-files --type=services**

**$systemctl list-unit-files --type=services | grep enabled** ( alleen enabled oplijsten)

**$systemctl list-unit-files –type=service | grep -v disable** (alles wat niet disabled is.)

**$systemctl status sshd.service** (om na te gaan of individuele services gaan runnen

**$systemctls condrestart naamvandeservice.service** (Conditionele restart= restart enkel en alleen als de service actief is.)

Reload= herladen van de configuratiebestanden maar de service zelf blijft runnen.

**3.7 Systemd Services enablen en disablen**

**$systemctl enable of disable**

Het enable of disable enkel het effect heeft bij het booten dus de services gaan actief blijven.

Is handig voor een service die altijd werkzaam zou moeten blijven.

**#systemctl mask NetworkManager.service** ( we zeggen dan NetworkManager nooit gerunt gaat worden)

**#systemctl unmask NetworkManager.service** (we zetten deze terug op)

**3.8 Default target units instellen**

Targets -persistant runlevels = een groep van services die gaan starten bij het booten

**#ls -l /etc/systemd/system/default.target** om symbolische link te zien.

**#systemctl set-default multi-user.target** (bv) ( om een default target aan te maken)

**4.1 Installatie Apache webserver**

Populairste webserver is tegenwoordig Apache. Opensourse webserver, aangepaste versie van httpd daemon. De config files vinden we terug in het map /etc/httpd en alle webpaginas komen in /var/www/html teracht.

Bij Ubuntu is het apache2 en niet httpd.

De webpagina inlezen: dan gaat hij standard zoeken naar index.html of index.php

Installatie van Apache: **#dnf download httpd**

Oplijsten: **#ls httpd\***

Inhoud bekijken:**#rmp -qip httpd** en dan op tab drukken, deze wordt automatisch aangevuld

inhoud:**#rmp -qcp httpd** en dan op tab drukken, deze wordt automatisch aangevuld

**#dnf install httpd** om te installeren

Webserver opstarten **#systemctl start httpd**

Webserer status: **# systemctl status httpd**

**4.2 Apache en de firewall**

Firewall moet als eerste geïnstalleerd worden

**#dnf install firewalld**

**#dnf firewall-config -y** (om grafische omgeving van de firewall te installeren)

Webserver afzetten: **#systemctl stop httpd**

Firewall opstarten: **#systemctl start firewalld**

Firewall opstarten tijdens booten: **#systemctl enable firewalld**

Anders is onze webserver niet beveiligd

Toestand van het firewall opvragen: **#firewall-cmd --state**

Zones van netwerkkaarten achterhalen: **#firewall-cmd --get-active-zones**

Zone public gebruiken voor de poorten: **#firewall-cmd --zone=public –permanent - -add-service=http**

**#firewall-cmd --zone=public –permanent - -add-service=https**

**#firewall-cmd --reload**

Controle : **#netstat -tupln | grep httpd**

**#systemctl start httpd**

**#netstat -tupln | grep httpd**

Om poorten te verwijderen: **#firewall-cmd --zone=public –permanent - -remove-service=http**

**4.3 Eerste webpagina**

**#cd /var/www/html**

**#ls ( het mapje is voorlopig leeg)**

**#vim index.html**

**#systemctl start httpd**

**#systemctl status httpd**

**4.4 Bestandspermissies en eigenaarschap**

Webserver proberen te beveiligen via bestandspermissies en eigenaarschap. Een httpt daemon als gebruiker Apache heeft en de groep is ook apache.

/var/www/html we willen dat onze httpt server deze inhoud kan lezen daarom moeten we aantal permissies gaan instellen.

We kunnen standaard niet inloggen als user apache.

Op bestanden willen we read permissies hebben ofwel voor de other user of voor de apache user en voor de mappen willen we execute permissies.

**#chown -R apache: apache /var/www/html** (Eigenaarschap instellen)

**#chmod -R u+r,g+r /var/www/html** (Bestandspermissies instellen)

**#cd /var/www/html** (Execute rechten op de mappen)

**#chmod u+X \*** (Execute rechten op de mappen)

**4.5 httpd configuratiebestanden**

**#cd /etc/httpd**

**#ls -l**

**#/etc/thhpd/cong/httpd.conf** (dit is ons hoofdconfiguratie bestand)

Die opsplitsing zorgt ervoor dat alles zo modulair mogelijk gebeurt.

**4.6 Meerdere websites via virtual hosts**

In principe hebben we maar een fysieke machine nodig alle die domainnamen gaan hetzelfde IP adress van de server hebben.

We gaan twee configuratie bestanden toevoegen aan apache.

Eerst gaan we een configuratie bestand opstellen voor onze eerste website.

**httpd]#vim /etc/httpd/conf.d/example.org.conf**

In Vim maken we dit bestand aan.

<VirtualHost \*:80> dit sterretje kunnen we vervangen door een ip adress

ServerAdmin [webmaster@example.org](mailto:webmaster@example.org)

ServerName [www.example.org](http://www.example.org)

ServerAlias web.example.org ( is optioneel, kunnen we ook weglaten)

DocumentRoot /var/www/html/example.org/ (submap voor onze website)

DirectoryIndex index.php index.html index.htm ( geeft aan naar welke bestand gaan we zoeken als we op de webserver gaan surfen)

</VirtualHost>

Tweede configuratie bestand is redelijk hetzelfde als de eerste.

**httpd]#cat /etc/httpd/conf.d/example.org.conf** (om alles te controleren)

**httpd]#ls /var/www/html**

Niuwe map aanmaken voor elke virtual host hierin.

**httpd]#mkdir /var/www/html/example.org**

**httpd]#mkdir /var/www/html/example2.org**

**httpd]#ls /var/www/html** ( om te kijken of de mappen zijn aangemaakt)

example.org hierin kan ik index file aanmaken dus mijn eerste website aanmaken

**httpd]# cd /var/www/html/example.org** (html code inzetten)

**[root@localhost example.org]#**

**[root@localhost example.org]#pwd** (om te zien of ik in de juiste map zit.)

**[root@localhost example.org]#vim index.html**

Afbeelding met tekst

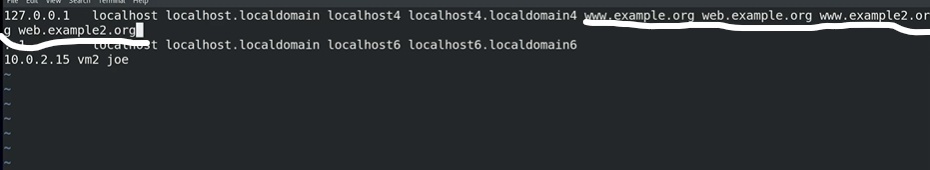
Automatisch gegenereerde beschrijving

**[root@localhost example.org]#vim /var/www/html/example2.org/index.html** (om een tweede file aantemaken voor website twee)

Namen aan onze server toevoegen dat kunnen we op twee manieren doen: 1 via DNS zien we later

2 via /etc/hosts

**[root@localhost example.org]# vim /etc/hosts**



Configuratie test van apache runnen

**[root@localhost example.org]# apachectl configtest (**als we Syntax OK terug krijgen dan weten we dan onze configuratie bestanden geen syntaxis fouten hebben)

Configuratie bestanden terug herladen:

**[root@localhost example.org]# apachectl graceful of systemctl reload httpd**

**[root@localhost example.org]#systemctl restart httpd** (om deze opnieuw te laten starten)

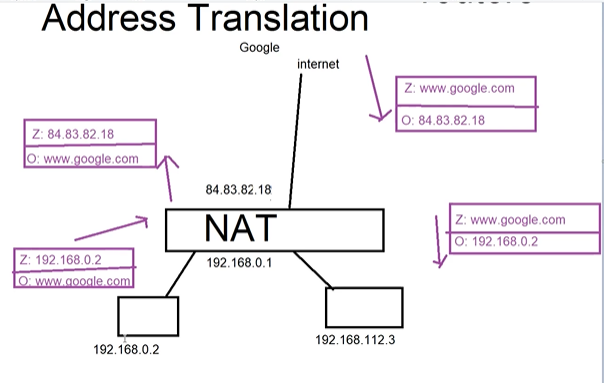
Daarna testen in de brouwser.

**6.1 NAT (Network Address Translation)**

Wordt ook IP masquraiting genoemd (adressinformatie van de data pakketjes gaan aanpassen)

We kunnen verschillende netwerken met elkaar gaan verbinden, wordt vooral gebruikt in routers.

Bij het verzenden van een pakket gaat het interne ip adres vertaald worden naar het externe ip adres. We hebben dus eigenlijk maar een ip adres op het internet nodig voor meerdere onderliggende toestellen dankzij onze NAT.

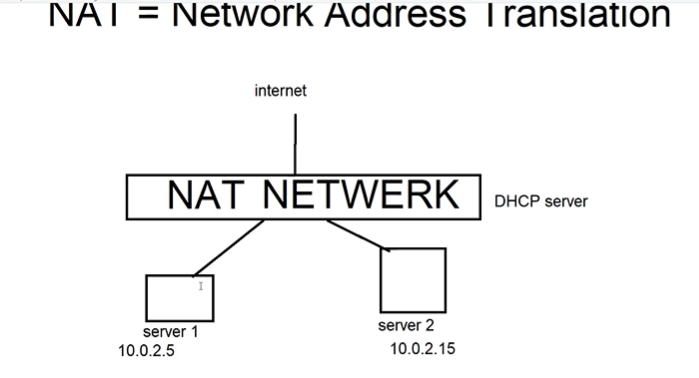


**6.2 NAT-network (Network Address Translation)**

Virtuele machines controleren op NAT netwerk

In een NAT-netwerk zit ook DHCP Server ingebouwd

ip addr show of ip a (om de IP adressen te zien)



**6.3 Intern netwerk en NAT naar buiten.**

Eerst twee machines uitzetten.

Netwerken van virtualbox instellen. VM1(Network🡪adapter 1 op intern netwerk, adapter 2 op NAT)

VM2(Network🡪adaperter 1 op intern netwerk) en daarna beide machines terug aanzetten. Maar adapter twee uitzetten want we gaan intern verbinden.

Onze machines gaat klagen dat ze geen IP adres hebben maar dat komt omdat ons intern netwerk van virtual box is een virtuele switch is die geen ip nummers of ip adressen gaat uitdelen.

We gaan deze manueel doen.

Controleer daarna of deze twee VM met elkaar kunnen communiceren via Ping.

Clean Install doen van eerste server zodat we later geen problemen krijgen.

We kunnen niet pingen vanaf VM2 omdat in de VM1 de twee netwerkkaarten niet met elkaar verbonden zijn. Dus we moeten masqurating gaan instellen.

**6.4 Beide netwerkkaarten koppelen op VM1.**

Firewall omgeving opkuisen en bepalen welke interfaces de externe en de interne is. De externe interface is de interface waarmee we naar het internet gaan connecteren.

**$sudo su**

Farewall instellingen aanpassen:

Externe zone instellen :

**#firewall-cmd - -change-interface=NAAM - -zone=external**

**#firewall-cmd - -list-all - -zone=external** (om te controleren of ons firewall goed geïnstalleerd is of ze effectief op external staan)

**#systemctl firewalld** (indien firewall d niet aan het runnen is)

**#systemctl enable firewalld** ( indien deze niet actief is, deze wordt dan bij het booten opgestart)

**# firewall-cmd - -change-interface=NAAM - -zone=external - -permanent** (om de wijzigingen permanent door te voeren)

**#firewall-cmd - -complete-reload** (herladen van firewall)

Interne zone instellen:

**# firewall-cmd - -change-interface=NAAM - -zone=internal**

**# firewall-cmd - -change-interface=NAAM - -zone=internal - -permanent**

**# firewall-cmd - -set-default-zone=internal** (standaard zone op internal)

**# firewall-cmd - -list-all - -zone=internal** (controle)

Firewall opnieuw herladen:

**# firewall-cmd - -complete-reload**

Poorten open zetten of gaatjes prikken in de firewall

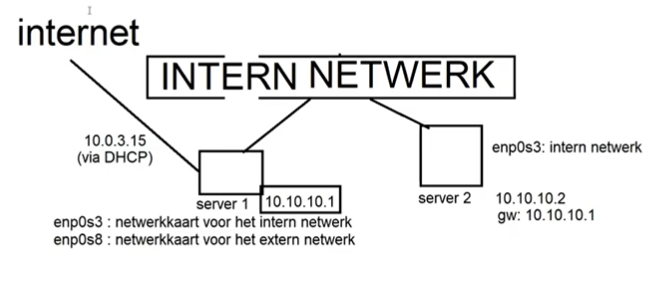
**#firewall-cmd - -zone=internal - -add-service=dns - -permanent** (dns server toevoegen voor internel zone)

**# firewall-cmd - -complete-reload**

**# firewall-cmd - -list-all - -zone=internal** (controleren of dns toegevoegd is)

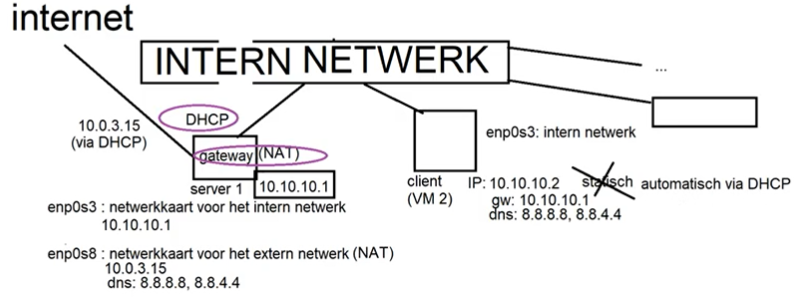
Controleer Wired settings op beide server en kijk of je kan pingen naar google. De gateway voor Server 2 is het IP adres van de Server 1.

Voorbeeld:



**7.1 DHCP**

DHCP-(Dynamic Host Configuration Protocol) = zorgt ervoor dat onze client computer IP adres automatisch kan krijgen via een DHCP Server.



**7.2 DHCP installeren en configureren**

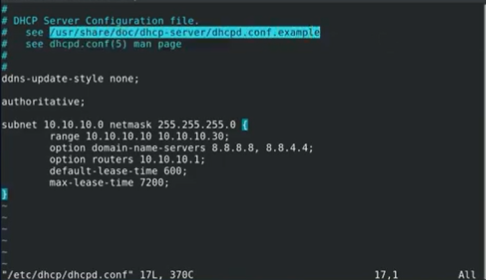
**$sudo su**

**#dnf install dhcp-server** (op CentOS)

DHCP server configureren

**#ls /etc/dhcp/** (om te zien wat er in staat)

**#vim /etc/dhcp/dhcpd.conf**



**# cat /etc/dhcp/dhcpd.conf** ( om te zien of deze aangepast is)

**#systemctl start dhcpd** (om dhcp server op te starten)

**#systemctl enable dhcpd** (zodat deze automatisch opgestart wordt bij het booten)

**#systemctl status dhcpd**

**#ping** [**www.google.com**](http://www.google.com)

We gaan ook kijken of we kunnen surfen op het internet.

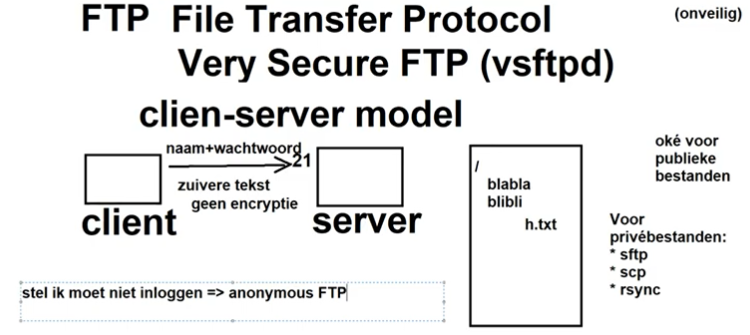
**8.1 FTP**

(=File Transfer Protocol)-een protocol die gebruikt wordt om bestanden te delen in en over een netwerk. Maar deze is redelijk onveilig want wordt uitgewisseld zonder encryptie.

Wordt vooral binnen een veilig LAN netwerk gebruikt.

Very Secure FTP (vsftpd) daemon- wordt tegenwoordig gebruikt op Linux.

Poort 21 wordt standaard gebruikt.



**8.2 Active FTP vs Passive FTP**

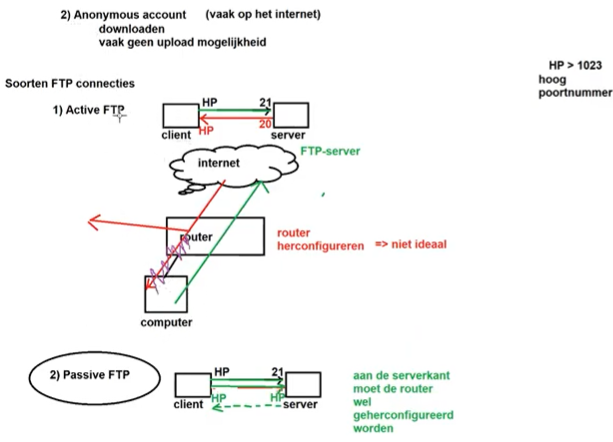
Inloggen voor ftp kan op twee manieren:

1.Standaard Linux gebruikersnaam en wachtwoord

We kunnen Downloaden en uploaden

2.Anonymous account (vaak op het internet), maar er zijn beperkingen we kunnen enkel downloaden maar uploaden is vaak onmogelijk.

Er zijn twee soorten FTP connecties:



**8.3 FTP clients command-line**

**$sudo dnf install ftp**

**$ftp** [**ftp.belnet.be**](ftp://ftp.belnet.be)

Username: anonymous

Password: willekeuring email adres

**ftp>**

**ftp>exit**

Het downloaden gebeurt in de map waarin we ons bevinden.

**$sudo dnf istall lftp**

**$lftp** [**anonymous@ftp.belnet.be**](mailto:anonymous@ftp.belnet.be)

Alles wordt duidelijker met kleurtjes getoond.

**8.4 FTP clients GUI**

Filezilla op Linux gebruiken is moeilijker want deze is bedoeld voor Debian Linux.

We gaan deze eerst downloaden.

**$cd Downloads/**

**Downloads]$ls**

**Downloads]$bunzip2 FileZilla\_3.53.1\_x86\_64-linux-gny.tar.bz2**

**Downloads]$tar xvf FileZilla\_3.53.1\_x86\_64-linux-gny.tar.bz2**

**Downloads]$ls**

**Downloads]$cd FileZilla3/**

**FileZilla]$ls**

**FileZilla]$cd bin**

**bin]$ls**

**bin]$./filezilla**

**8.5 Very Secure FTP server installeren**

**$sudo su**

**#dnf install vsftpd**

**#rpm -qi vsftpd** (informatie over vsftpd)

**#rpm -ql vsftpd** (alle bestanden die in deze pakket zitten)

8.6 FTP server configureren en starten

**#vim /etc/vsftpd/vsftpd.conf**

**#systemctl status vsftpd**

**#systemctl start vsftpd**

**#systemctl enable vsftpd**

**#netstat -tulpn | grep vsftpd**

Anonymous gebruikers gaan in de /var/ftp terecht komen.

**8.7 FTP server beveiligen**

Beveiliging via Firewall

**#dnf install firewall-config**

**#firewall-config**

Could not connect: Connection refused- het kan zijn dat we dit melding krijgen.

Dan gaan naar Firewall zoeken via zoekbalk. Firewall configuration: Bij zones gaan we ftp aanvinken voor external en internal. Daarna de configuratie op permanent zetten. Daarna gaan we naar option en gaan we firewall reloaden.

**#setenforce 0** ( we zetten onze SELinux uit)

**#senenforce1** (om deze terug aan te zetten)

Het is aan te raden om external ftp uit te zetten aangezien we niet echt veilig bezig zijn na het uitzetten SELinux.

**#cd /var/ftp**

**ftp]#chmod o-r hallo.txt** (others hebben geen read permissie)

Als we onze vsftp.conf file aanpassen is het belangrijk dat we onze server altijd herstarten. Voor vsftp werkt reload niet enkel restart.

(dat ftp user de shell van de server niet kunnen gebruiken dus enkel de ftp server)

**ftp]#vim /etc/shells** (hier voegen we eentje bij: /sbin/nologin)

**ftp]#useadd bob -s /sbin/nologin**

Deze user (bob) kan inloggen enkel op ftp server.

**8.8 FTP server op VM1 en FTP client VM2**

Eerst testen of onze twee VM’s met elkaar verbonden zijn.

**#systemctl status vsftpd**

VM2

**#vim /etc/shells** ( we gaan nog een regel toevoegen: /sbin/nologin)

**#ftp 10.10.10.1**( we gebruiken ons eigen ip adres)

Anonymous user zou kunnen schrijven op het interne netwerk:

Vm1

**$sudo su**

**#rpm -qc vsftpd** (onfiguratie file aanpassen)

**#vim /etc/vsftpd/vsftpd.conf** 🡪#anon\_upload\_enable=yes🡪anon\_upload\_enable=yes

**#anon\_mkdir\_write\_enable=yes**🡪 anon\_mkdir\_write\_enable=yes

**#systemctl restart vsftpd**

**#chown ftp ftp:ftp /var/ftp/pub/upload** (de ftp moet de owner zijn van dit mapje)

Belangrijke slides FTP

**9.1 SELinux (Security Enhanced Linux)**

SELinux is een uitbreiding van Linux kernel en die kan zorgen voor een betere beveiliging van uw systeem. Het is dus een extra beveiliging laag rond onze Linux kernel.

SELinux grijpt in in verschillende plaatsen: netwerpoorten, applicaties, locaties in het filesysteem.

SELinux afzetten: om te zien of de probleem die opduikt is aan SELinux ligt.

**#setenforce 0** (SELinux afzetten, tijdelijk doen🡪minder veilig)

**#setenforce 1** (SELinux aanzetten)

SELinux kan zich in drie verschillende modi bevinden: Enforcing (staat aan), Permissive (waarschuwingen printen in de vorm van logs), Disabled (uitgeschakeld).

**$cat /etc/syscpnfig/selinux** (hier vinden we de modi terug)

**~]#ls -Z** (meer info zien met betrekking tot SELinux-voor bestanden)

**~]#ps -Z** (meer info zien met betrekking tot SELinux-voor processen)

**~]#netstat -Z** (kijken naar de netwerkpoorten)

**~]#mkdir test**

**~]#ls**

**~]#ls -Zd test** (om informatie daarvan weer te geven)

**~]#ls -Za** (alles oplijsten van home directory ook de verborgen bestanden)

**9.2 SELinux Webserver types**

**#dnf isntall httpd**

**#rm -rf /var/www/html/\*** (indien html directory volstaat)

httpd\_sys\_content\_t (alle webcontent moet van dat type zijn als deze files niet van dat type is dan kan de httpd server daarmee niet omgaan, dus de bestanden van andere types kan de httpd server niet tonen)

**#systemctl start httpd** ( om de webserver te starten)

**#ls -Zaux | grep httpd** (alle processen opsommen en grep doen op httpd)

Conclusie: Afhankelijk van waar we een bestand of een map gaan aanmaken daar krijgen we een bepaalde SELinux type toegewezen.

**9.3 SELinux types fouten opsporen**

**#ls**

**#cd /var/www/html**

**html]#ls**

**html]#rm index.html**

**html]#ls**

**html]#exit**

**$cd ~**

**$pwd**

**$vim index.html** (Dit is een test. 🡪wq)

**$ls -Z** (type)

**$ls -Z index.html**

**$sudo mv index.html /var/www/html** (bestand moven)

**$cd /var/www/html**

**html]#ls -Z**

We gaan naar een webbrowser🡪 localhost (FORBIDDEN: You don’t have permission to access this resource.)

Oplossing:

**html]$sudo su**

**html]#setenforce 0** (dan werkt het wel, dus het licht aan SELinux)

**html]#setenforce 1**

**html]#cd /var/log/audit** (kijken in log boeken)

**audit]#ls**

**audit]#ls**

**audit]#tail audit.log** (laatste tekst van bestand bekijken)

**audit]#dnf install setroubleshoot**

**audit]#reboot** of **init 6**

**audit]#cd /var/log/audit**

**audit]#ls**

**audit]#journalctl -f** (om logs te bekijken)

**audit]#setsebool -P httpd\_read\_user\_content 1** (voor oplossing)

**audit]#setsebool -P httpd\_read\_user\_content 0**

**audit]#systemctl restart httpd**

Nu gaan we kijken op webbrowser en het werkt.

**audit]#getsebool -a**

**audit]#getsebool -a | grep httpd** (httpd\_read\_user\_content - -> off)

**9.4 SELinux types correct veranderen**

“Je moet starten van een clean install dus de DHCP server”

Type van het file correct gaan aanpassen

**$sudo su**

**#cd /var/www/html**

**html]#ls**

**html]#ls -Z**

**html]#chcon -t httpd\_sys\_content\_t index.html** (manier1)

**html]#ls -Z** (type is veranderd)

**html]#restorecon -vR /var/www** (we gaan die index.html file en alles wat er in zit relabelen) (manier 2)

**9.5 SELinux Booleans instellen**

-P maakt een wijziging permanent.

**html]#cd /var/log/audit**

**audit]#journalctl -f**

**audit]#getsebool -a | grep httpd** (httpd\_read\_user\_content - -> off)

**audit]#setsebool -P httpd\_read\_user\_content 1** (httpd\_read\_user\_content - -> on)

**audit]#less /var/lib/selinux/targeted/active/booleans.local** (om te zien wat er gewijzigd werd)

**10.1 IPTables**

(We maken gebruik van snapshot vanaf DHCP installatie)

Iptables is een commando die gebruikt wordt om pakketten te blokkeren:

-Filteren op basis van een MAC-adres (Datalinklaag)

-Filteren op IP-header velden (Netwerklaag)

-Filteren op TCP/UDP headers (Transportlaag)

-Poortnummers

-Applicatielaag

IPTables zit ingebouwd in Linux kernel

Op kernel niveau wordt netfilter gebruikt om pakketten te filteren.

**$sudo su**

**#systeemctl status firewalld**

#om de firewall te gaan gebruiken kunnen we gebruik maken van **firewall-cmd** commando of **firewall-config** gebruiken.

**#dnf install firewall-config** (installeren indien deze niet aanwezig is)

**#firewall-cmd - -get-default-zone** (om te zien welke zone dit is)

**#systemctl stop firewalld**

**#systemctl disable firewalld**

**#dnf install iptables-services iptables-utils** (IPTables installeren)

**#systemctl start iptables**

**#systemctl enable iptables**

**#systemctl status iptables**

We gaan geen gebruik maken van een system-config-firewall, we maken direct het gebruik van iptables.

Bekijk ook de slides.

**10.2 IPTables tables,chains, rules**

Begrippen om te kennen:

-Tables = een tabel🡪iets om pakketten op een bepaalde manier te verwerken. Er zijn 5 tal tabellen maar we gaan er maar twee geuiken:

1) filter (standaard tabel) => binnenkomende en uitgaande pakketten filteren of toestaan.

2)NAT (network address translation) om IP-adressen te vertalen

Chains horen bij een table;

Voor filter:

* INPUT (wanneer een pakket binnenkomt)
* OUTPUT (wanneer een pakket naar buiten gaat)
* FORWARD (wanneer pakket wordt doorgestuurd; routers)
* kan ook eigen chains maken (custom chains)

Voor NAT:

* PREROUTING
* OUTPUT
* POSTROUTING

Rules toevoegen aan een bepaalde chain:

* Pakketen acceptern met ACCEPT
* Paketten rejecten met REJECT
* Paketten droppen met DROP
* Of doorvewijzen naar een custom chain

Bekijk de slides

**10.3 IPTables voorbeeld**

Twee machines moeten met elkaar kunnen communiceren

**#ifconfig** (om IP-adres te achterhalen)

**#iptables -L** (huidige chain van de filter tabel)

We zien “policy ACCEPT” staan dat is een globale instelling voor heel de chain. Eerst worden de rules gecheckt en dan pas geldt de policy. Dus die regels overschreven de globale policy.

**#iptables -L -n** (voor numeriek)

**#iptables -L -v** ( voor meer informatie)

Zelf iptables instellen

**#iptables -F** (eerst alle regels verwijderen)

**#iptables -t filter-P INPUT DROP**

**10.4 IPTables custom chain maken**

**#iptables -N nieuwe chain** (bij filters)

**#iptables -L**

**#iptables -t nat -N nieuwechain** (bij nat)

**#iptables -X** (bij filters staandaard ) (aangemaakte chain verwijderen)

**10.5 IPTables rules instellen**

**#iptables -F** (om alle regels te verwijderen)

**#iptables -X** (om zelf gemaakte chains te verwijderen)

**#iptables -L** ( om te controleren)

**#iptables -P INPUT ACCEPT** ( als we alles willen accepteren)

**#iptables -A INPUT -s ipadressvdsource -p icmp -j DROP** (alle pakketten die van dit ip adres binnen komen dus de ping pakketten laten we droppen)

**#iptables -D INPUT 1** ( om de regel die we hebben toegevoegd te verwijderen)

Bekijk ook de slides

**10.6 IPTables Ping flooding tegengaan.**

Ping flooding = met behulp van het icmp protocol kunnen we de ene computer naar de andere computer gaan pingen.

Filtertabel is de default tabel.

Aantal ping bepalen:

**#iptables – F**

**#iptables -X**

**#iptables -P INPUT DROP**

**#iptables -A INPUT -p icmpv-m limit - -limit 1 -j ACCEPT** (een regel toekennen: we gaan maar een pakketje per seconde accepteren.)

Bekijk ook de slides

**10.7 IPtables zelfaangevraagde pakketten toelaten**

Starten vanaf een lege tabel.

**#iptables -P** (de policy)

**#iptables -A INPUT -m state - -state RELATED, ESTABLISHED -j ACCEPT** (alles wat ik zelf heb aangevraagd toelaten)

**10.8 IPTables opslaan, NAT, NFTables**

**#less /etc/sysconfig/iptables**

**#iptables-save > /etc/sysconfig/iptables**

**#iptables -t nat -A POSTROUTING -o** denaamvdinterface **-j MASQUERADE** (voor NAT)

Bekijk ook de slides ook netfilter.org

**11.1 Samba voorbereiding**

**Samba op zich is heel traag dus heb geduld en je moet paar keer restarten. Samba vraagt tijd.**

We vertrekken van DHCP opstelling.

Samba is een opensource software pakket en bestaat uit verschillende applicaties. Samba maakt gebruikt van het SMB (Server Message Block)-protocol.

Samba probeert Windows Network Neighbourhood na te botsen op Linux. Op die manier kunnen verschillende machines die SMB-protocol ondersteunen met elkaar communiceren over het netwerk.

**$ifconfig** (om de ip adres te controleren)

**#systemctl status dhcpd** (we controleren of de dhcp server opstaat)

De namen van de VM’s veranderen:

**#hostnamectl set-hostname - -static nasbox.testlan** (en daarna reboot)

**#hostnamectl set-hostname - -static client1.testlan** (en daarna reboot)

Na het rebooten controleren we best de dhcp server.

Als we met hostnames willen gaan werken, gaan de hostnamen aan onze /etc/hosts

Shares aanmaken🡪

Public: voor iedereen leesbaar zonder inloggen. Voor geregistreerde gebruikers (met login) => zowel lees- als schrijfrechten.

Private: enkel toegankeljijk voor mensen met login en die hebben lees- en schrijfrechten

Home directories: moeten toegankelijk zijn voor elke gebruiker.

Users aanmaken: -alice en pete =>toevogen aaan groep “nasusers” met lees- en schrijfrechten voor public en private

SELinux aanlaten!

Firewall moet opstaan!

Samba: security = user (aangeraden door Samba zelf, nooit op share zetten)

**11.2 Samba server en client installeren, shares maken**

VM1 :

**#dnf install** **-y** **samba** (zodat deze automatisch op Yes drukt)

**#dnf install -y samba-client**

Op VM2 gaan we Samba client installeren.

VM1:

Groep aanmaken van gerbuikers:

**#groupadd nasusers**

**#useradd - -create-home -G nasusers alice**

**#passwd alice**

**#smbpasswd -a alice** (Samba password geven) (omdat dit de eerste keer is)

**#id alice** (controleren)

**#useradd - -create-home -G nasusers pete**

**#passwd pete**

**#smbpasswd -a pete**

Shares aanmaken:

**#mkdir -p /srv/shares/{public,private}**

**#chgrp -R nasusers /srv/shares/\*** (we veranderen de groep)

**#chmod -R g+w /srv/shares/\*** (schrijfrechten toekennen)

**#ls -lR /srv/shares/**

**#su – alice**

**$vim /srv/shares/public/pub.txt**

**$exit**

**#su – pete**

**$vim /srv/shares/private/priv.txt**

**$exit**

**11.3 Samba en SELinux**

VM1:

**#setenforce 1 ( SELinux aanzetten)**

**#sestatus**

**#less /etc/sysconfig/selinux**

SELinux:

* Booleans aanpassen
* File context (type van SELinux)

**# getsebool -a|grep samba (Booleans die te maken hebben met Samba)**

**#setsebool -P samba\_enable\_home\_dirs on (zetten we aan)**

**#setsebool -P samba\_export\_all\_rw on**

**# getsebool -a|grep samba**

**#ls -Z /srv/shares**

**#chcon -Rt samba\_share\_t /srv/shares (type instellen)**

**#semanage fcontext -a -t samba\_share\_t “/srv/shares(/.\*)” (permanent gaan doorvoeren)**

**#restorecon -Rv /srv**

**#less /etc/selinux/targeted/contexts/files/file\_contexts.local**

**11.4 Samba configuratiebestand**

**#vim /etc/samba/smb.conf**

**#cp /etc/samba/smb.conf /etc/samba/smb.conf.original (back-up maken)**

**#testparm (systax controleren)**

Smb.conf aanpassen- de aanpassingen die we gaan uitvoeren vinden we terug op de slides Samba configuratie.

Geen tegenstrijdige aanpassingen uitvoeren in deze config file: vb. Writable Yes 🡪 read only Yes

We moeten Samba restarten na dat de aanpassingen zijn uitgevoerd.

**#systemctl restarts mb**

**#systemctl enable smb**

**#systemctl restart nmb**

**#systemctl enable nmb**

**11.5 Samba firewall instellingen**

**#systemctl status smb**

**#systemctl status nmb**

**#netstat -tulpn | grep smbd (checken of de poorten open zijn)**

**#netstat -tulpn | grep nmbd**

Bekijk de slides – Firewall instellingen

**#firewall-cmd - -permanent - -add-service=samba (Service van Samba toevoegen)**

**#systemctl restart firewalld**

De poorten controleren op de client

**#dnf install -y nmap**

**#nmap ipvanvm1**

**#nmap -sU -p 137.138. 10.10.10.1 (udp checken)**

VM1

**#nmblookup nasbox**

**11.6 Samba shares toegang testen**

VM1

Grafich via files

**#ls -ZL /srv/shares/public** (shares en rechten checken)

**#vim /etc/samba/smb.conf**

**#systemctl restart smb**

**#systemctl restart nmb**

**#smbclient //localhost/public -Ualice**

**smb : \>ls**

**smb: \>get pub.txt** (om bestand te downloaden)

**smb: \>exit**

**smb: \>put testbestandje.txt** (om bestand te uploaden)

**12.1 Printserver en CUPS**

We hebben twee soorten printers:

* + - 1. Printer die rechtstreeks verbonden zijn met de computer met usb.
      2. Printer aan een switch =>gedeeld in een netwerk.

Printersoftware: CUPS (Common Unix Printing System). Printserver moet altijd aan staan.

4 tools:

CUPS web based

CUPS configuratiebestanden aanpassen

~~Third party software~~

~~GNOME printerinstallingen~~

**$systemctl status cups**

**#systemctl enable cups**

**#dnf install -y httpd ( indien we geen webserver hebben)**

**#systemctl start httpd**

**#systemctl enable httpd**

CUPS luistert standaard naar poort 631.

**12.2 CUPS-PDF printer toevoegen**

#dnf install cups-pdf Gaat niet meer op Linux, daarom moeten we deze via een webbrowser downloaden.

**#cd /home/tom/Downloads**

**#ls**

**#rpm -ivh cups-pdf-2.6.1-7.el7.x86\_64.rpm**

<http://localhost:631> in browser om cups te openen.

CUPS-PDF is geen printer er gaat gewoon PDF bestand gegenereerd worden.

**12.3 CUPS administration**

<http://localhost:631>

**12.4 CUPS configuratiebestanden**

**Downloads]#sudo su**

**Downloads]#cd /etc/cups**

**cups]#ls**

**cups]#vim /etc/cups/cupsd.conf ( hier kunnen we aanpassingen doen indien gewenst)**

**cups]#vim /etc/cups/printers.conf (printer configuratie)**

**12.5 Printercommando’s**

**lpr** – om te gaan printen

**lpq** – onhoud van printer queue bekijken

**lpc** – printer controlling

**lprm** - jobs uit de printer queue verwijderen

**#cupsdisable** – alle printers disablen

**#cupsdisable Cups-PDF** (om specifieke printers te disablen)

<http://localhost:631> 🡪 administration (hier kunnen we aanpassingen die we wensen uitvoeren)

Applicaties zoals LibreOffice, OpenOffice gebruiken onderliggend die commando’s

**12.6 CUPS printer delen in netwerk via Avahi**

Delen met verschillende protocollen:

* IPP
* LPD
* HP Jetdirect
* Apple AirPrint (kan enkel voor printers die het ondersteunen)
* Google Cloud Print (kan enkel voor printers die het ondersteunen)

Om een printer discoverable te maken:

* Samba
* Avahi

We gaan CUPS-PDF printer delen

**#cupsctl - -share-printers (printers delen)**

**#cupsctl - -share-printers - -remote-any (printers toestaan van een ander subnet)**

**#systemctl stop firewalld**

**#lpadmin -p cups-pdf -o printer-is-shared=true (cups-pdf gaan delen)**

**#systemctl status avahi-daemon**

**#systemctl start firewalld**

VM2-client

**#dnf install -y httpd**

**#systemctl start cups**

**#systemctl stop firewalld**

We gaan naar http://localhost:631 -->administration🡪add printer🡪CUPS-PDF

Het kan zijn dat we CUPS-PDF moeten gaan installeren op de cliernt.

**#rpm -ivh cups-pdf-2.6.1-7.el7.x86\_64.rpm**

**#rpm -ql cups-pdf**

**12.7 CUPS printer delen in netwerk via Samba**

**#dnf isntall -y samba**

**#vim /etc/samba/smp.conf (we gaan ‘client min protocol = NT1 en server min protocol = NT1 ‘ er** **uithalen)**

**13.1 NFS (Network File System)**

Wordt gebruikt om mappen en bestanden te delen over het netwerk tussen de verschillende Linux machines het is een alternatief voor het smb-protocol.

NFS is veel eenvoudiger dan Samba.

Versie 4 van NFS is standaard:

* Ondersteunt Kerberos identificatie van uzelf in het netwerk
* Veiliger (gebruikt TLS/SSL)
* Kan overweg met TCP en UDP

Opstelling

Server heeft twee mappen:

/home 🡪 delen voor alle clients

/misk/projectX 🡪 delen voor de eerste 2 clients in het netwerk

**13.2 NFS server installeren en opzetten**

Dit doen we op de server

**#dnf install nfs-utils** ( het kan zijn dat het pakket al geïnstalleerd is want het wordt standaard geinstalleerd op veel distro’s)

**#rpm -gd nfs-utils | less**

**#man exports**

**#man exportfs**

**#man mount.nfs**

**#systemctl start nfs-server**

**#systemctl enable nfs-server**

**13.3 NFS mappen delen**

Regels waarmee we rekening moeten houden:

* Enkel locale filesystems delen 🡪server deelt iets met clients en de clients kunnen niet verder gaan delen
* Directory en een subdirectory kunnen niet samen geëxporteerd worden (uitzondering: wanneer dat die directory en subdirectory op aparte disks staan

Het volstaat dus om gewoon de hoofddirectory te exporteren en dan wordt de subdirectory automatisch mee geëxporteerd.

Bekijk ook de slides

**13.4 NFS server beveiligen**

We gaan gebruik maken van Firewall en SELinux

Beveiliging problemen zijn opgelost sinds NFS versie 4 en tegenwoordig kunnen we gebruik gaan maken van TLS of SSL.

**#mkdir /geheim**

**#mkdir -p /export/users** ( -p betekent parent, we gebruiken deze om ook parent map aan te maken)

**#ls -d /export/users**

**#mount –bind /geheim /export/users**

**#touch /export/users/blabla.txt** ( als we dit doen dan wordt ons txt bestand effectief aangemaakt in het mapje Geheim omdat we /export/users gemont hebben aan /geheim)

Als we onze computer terug opnieuw gaan opstarten gaat de **mount** niet doorgevoerd zijn.

**#vim /etc/fstab ( onderaan gaan we nog een regel toevoegen, nl. /geheim /export/users none** **bind 0 0) en wq**

Als we nu reboot doen zal deze **moun**t wel uitgevoerd worden.

Directory exporteren via NFS:

**#vim /etc/exports ( regel toevoegen: /export/users \*(rw) )**

**#exportfs -a -r -v**

Services open zetten via firewall:

**#firewall-cmd - -permanent - -add-service=nfs**

**#firewall-cmd - -permanent - -add-service=rpc-bind (rpc=remote procedure calls)**

**#firewall-cmd - -permanent - -add-service=mountd**

**#firewall-cmd - -reload**

SELinux instellen:

**#getsebool -a |grep nfs**

**#setsebool -P use\_nfs\_home\_dirs on**

Of via file context:

**#mkdir /whatever**

**#ls -d /whatever**

**#ls -Zd /whatever**

**#semanage fcontext -a -t public\_content\_rw\_t « /whatever(/.\*) ? »**

**#restorecon -F -R -v /whatever**

**13.5 File system mouten op client via mount**

MOUNT

Er zijn paar mogelijkheden: via mount commando of /etc/fstab of autofs commando

**#showmount -e ipadresvan1machine**

**#mkdir /projectX**

**#mount ipvan1machine:/misk/projectX /project**

**#mount -t nfs4** (controle)

**#touch /projectX/blabla/txt**

Cannot touch (we moeten op de server de juiste rechten gaan instellen)

We gaan naar de server

**#chmod o+rw /misk/projectX**

En nu terug proberen op de Client

**#touch /projectX/blabla/txt**

**13.6 File system mounten op client via /etc/fstab**

**#vim /etc/fstab onderaan: ipvanserver:/misk/projectX /projectX nfs rsize=8192,wsize=8192** **0 0)**

**#reboot**

**13.7 File system mouten op client via autofs**

**#dnf install autofs**

**#systemctl start autofs**

**#systemctl enable autofs**

**#cd /net/ipvan1machine** (we gaan naar pc op afstand)

**13.8 Unmonten op clients**

**#unmount /projectX**

**#unmount ipadres:/misc/projectX**

**#cat /etc/fstab**

**#vim /etc/fstab** (laaste regel die we hebben toegevoegd verwijderen)

**#reboot**