
Contents

1	Centos 7 - System Administration Guide	3
1.1	System Local en toetsenbord	3
1.1.1	Theorie	3
1.1.2	Commando's	3
1.2	Datum en tijd configureren	4
1.2.1	Commando's	4
1.3	Gebruikers en groepen beheren + Toegang	4
1.3.1	Theorie	4
1.3.2	Commando's	5
1.4	Pakketbeheer met yum-commando	5
1.4.1	Theorie	5
1.4.2	Commando's	6
1.5	Beheren van services met systemd	6
1.5.1	Theorie	6
1.5.2	Commando's	8
1.6	OpenSSH	8
1.6.1	Theorie	8
1.6.2	Commando's	9
1.7	Web Servers	9
1.7.1	Theorie	9
1.7.2	Commando's	9
1.8	Mail Servers	10
1.8.1	Theorie	10
1.8.2	Commando's	10
1.9	File Server	11
1.9.1	Theorie	11
1.9.2	Commando's	12
1.10	System Monitoring tools	13
1.10.1	Commando's	13
1.11	Log Files	13
1.11.1	Commando's	13
2	Centos 7 - Networking Guide	13
2.1	NetworkManager	13
2.1.1	Theorie	13
2.1.2	Commando's	14
2.2	Hostnamen	15
2.2.1	Commando's	15
2.3	DHCP	15
2.3.1	Theorie	15
2.3.2	Commando's	18
2.4	DNS/BIND	18
2.4.1	Theorie	18
2.4.2	Commando's	18
3	Centos 7 - SELinux	18
3.1	Werken met SELinux	18
3.1.1	Theorie	18

3.1.2	Commando's	19
4	Ansible	19
4.1	Installeren van packages	19
4.1.1	Eén package	19
4.1.2	Meerdere packages	20
4.2	Firewall	20
4.2.1	Enable Firewall	20
4.2.2	Configureren één service voor Firewall	20
4.2.3	Configureren van meerdere services voor Firewall	21
4.3	Services	21
4.3.1	Starten van service	21
4.4	Files & Templates	21
4.4.1	Eigenaar veranderen	21
4.4.2	Bestand kopiëren in VM	22
4.4.3	Bestand unzippen en plaatsen	22
4.5	MySQL	22
4.5.1	Benodigde packages	22
4.5.2	Nieuwe database aanmaken	22
4.5.3	Databank gebruiker aanmaken	23
4.6	Web	23
4.6.1	Benodigde packages	23
4.7	DNS	23
4.7.1	Benodigde packages	23
4.7.2	named.conf	24
4.7.3	Forward-bestand	24
4.7.4	Reverse-bestand	25
5	Troubleshooting	26
5.1	Hardware	26
5.2	Netwerkkinterface	26
5.3	Internet	26
5.3.1	Commando's	26
5.4	Transport	27
5.5	Applicatie	27
5.6	Geen internet, wat nu?	27

1 Centos 7 - System Administration Guide

1.1 System Local en toetsenbord

1.1.1 Theorie

De lokale settings zitten in */etc/locale.conf* die wordt gelezen door de *systemd* daemon wanneer een machine boot. In dit bestandje worden de volgende zaken gedefinieerd:

- **LANG** = Een default taal instellen voor de machine
- **LC_COLLATE** = Verandert het gedrag van de functies die strings vergelijken in het lokale alfabet.
- **LC_CTYPE** = Verandert het gedrag van character handling and classification functies en de multibyte karakter functies.
- **LC_NUMERIC** = Beschrijft de manier hoe nummer worden weergegeven met details zoals decimale punten en of komma's.
- **LC_TIME** = Weergave van de tijd. 24-uur of 12-uur klok.
- **LC_MESSAGES** = Zet de locale die gebruikt wordt voor het schrijven van diagnostic berichten naar de standaard output.

1.1.2 Commando's

Commando	Uitleg
localectl status	Huidige status tonen van systeeminstellingen (toetsenbord en taal)
localectl list-locales	Beschikbare Locales tonen
localectl list-locales grep EN	Idem hierboven maar enkel engelse
localectl list-keymaps	Beschikbare layouts vr toetsenbord bekijken.
localectl list-keymaps grep EN	Idem hierboven maar enkel engelse
localectl set-keymap nl	Dit verandert de taal naar Nl van toetsenbord

1.2 Datum en tijd configureren

1.2.1 Commando's

Commando	Uitleg
timedatectl	Dit toont de lokale en universele tijd en nog andere tijdsgebonden informatie.
timedatectl set-time 2015-02-12	Verandert de huidige datum naar 12 februari 2015.
timedatectl set-time 23:26:00	Verandert de huidige tijd.
timedatectl set-timezone Europe/Amsterdam	Verandert de tijdzone naar die van Amsterdam.
timedatectl list-timezones grep Europe	Toont een lijst van alle Europese tijdzones
timedatectl set-ntp yes	Automatische synchronisatie met remote server
date -utc	Toont de huidige datum en tijd
date +"%Y-%m-%d %H:%M"	Geeft huidige datum en tijd weer in leesbaar formaat
date +%F -s 2014-06-02	Verandert de huidige datum naar 2 juni 2014.
date +%T -set 23:26:00	Verandert de huidige tijd
hwclock	Geeft huidige datum en tijd weer samen met seconden
hwclock --localtime	Toont de lokale datum en tijd
hwclock --set --date "21 Oct 2014 21:17"	Dit zet de datum en tijd naar de gegeven waarden.
hwclock --systohc --localtime	Dit synchroniseert de systeem tijd naar hardware klok. Reboot is nodig na dit commando.
hwclock --hctosys --localtime	Dit synchroniseert de hardware klok naar systeemtijd. Reboot is nodig na dit commando.

1.3 Gebruikers en groepen beheren + Toegang

1.3.1 Theorie

Bij het toevoegen van een gebruiker kunnen er een heleboel parameters meegegeven worden. Dit zijn enkele van de belangrijkste:

- -d *directory* = Dit verandert de home directory naar een andere directory dan de default.
- -e *date* = Datum wanneer het account disabled wordt (YYYY-MM-DD)
- -g *groepnaam* = Groepsnaam of nummer waar de gebruiker als default in zal zitten.
- -G *groepsnamen* = Idem als voorgaande maar dan meerdere groepen gescheiden door een komma.
- -N = Maak geen user private groep aan.

-
- -p *wachtwoord* = wachtwoord dat wordt geencrypteerd.

Bij het toevoegen van een groep kun je ook enkele parameters meegeven:

- -f = Zo wordt er automatisch een ander gid gebruikt indien het ingegeven gid al bestaat.
- -g *gid* = Dit is het group ID, dit moet een uniek nummer zijn dat groter is dan 999.
- -p *wachtwoord* = Stelt een geencrypteerd wachtwoord in.

1.3.2 Commando's

Commando	Uitleg
useradd [options] user_name	Een gebruiker toevoegen met eventuele extra parameters (zie theorie).
usermod -G *groep-snaam* *usernaam*	Voegt een gebruiker toe aan een bepaalde groep
groupadd [options] group_name	Een groep toevoegen met eventuele extra parameters.
mkdir /opt/myproject	Map aanmaken met naam "myproject"
groupadd myproject	groep aanmaken met de naam "myproject"
chown root:myproject /opt/myproject	Inhoud van de directory associëren met de groep
chmod 2775 /opt/myproject	Gebruikers de mogelijkheid geven bestanden aan te maken in de directory.
ls -l /opt	Zo kan je alle instellingen van een bepaalde map zien
sudo *commando*	Hierdoor voer je het bijgevoegde commando uit als root

1.4 Pakketbeheer met yum-commando

1.4.1 Theorie

In het bestand */etc/yum.conf* kan je configureren hoe het yum commando precies zal werken. Hier kan je zaken definiëren in het main -en repository-gedeelte.

1.4.2 Commando's

Commando	Uitleg
yum check-updates	Laat zien welke geïnstalleerde packages op jouw systeem die updates nodig hebben.
yum update *pakketnaam*	update een specifiek pakket.
yum group update *groepnaam*	Updaten van een pakketgroep
yum update	Update gewoon alles.
yum search *zoekterm*	Zoekt naar pakketten die een bepaalde naam hebben
yum list all	Geeft een lijst van informatie over alle geïnstalleerde en beschikbare pakketten.
yum list installed "krb?-*"	Een lijst van alle geïnstalleerde pakketten die beginnen met krb.
yum repolist	Lijst van de repository ID, naam en nummer van pakketten.
yum info *pakketnaam*	Geeft informatie over een bepaald pakket.
yumdb info *pakketnaam*	Geeft extra informatie weer
yum install *pakketnaam*	Installeert het pakket
yum localinstall *path*	Installeert een vooraf gedownload pakket.
yum remove *pakketnaam	Verwijderen van pakketten.
yum groups summary	Toont het aantal geïnstalleerde en beschikbare groepen.
yum group install *groepsnaam*	Installeert een groep pakketten.
yum install @kde-desktop	Hetzelfde als bovenstaande commando!
yum group remove *groepsnaam* OF yum remove @kde-desktop	Verwijderen van een groep pakketten.
yum history list (all)	Laat een lijst zien van de 20 meest recente transacties. De all-optie voor allemaal.
yum info yum	Laat je zien welke plugins er actief zijn.

1.5 Beheren van services met systemd

1.5.1 Theorie

Dit kan het best getoond worden a.d.h.v. onderstaande afbeelding:

service	systemctl	Description	service	systemctl	Description
service name start	systemctl start name.service	Starts a service.	service name reload	systemctl reload name.service	Reloads configuration.
service name stop	systemctl stop name.service	Stops a service.	service name status	systemctl status name.service	Checks if a service is running.
service name restart	systemctl restart name.service	Restarts a service.		systemctl is-active name.service	
service name condrestart	systemctl try-restart name.service	Restarts a service only if it is running.	service -- status-all	systemctl list-units -- type service --all	Displays the status of all services.

Ook onderstaande afbeelding is vrij essentieel. (Zijn eigenlijk commando's maar deze afbeelding duidelijke!

Old Command	New Command	Description
halt	systemctl halt	Halts the system.
poweroff	systemctl poweroff	Powers off the system.
reboot	systemctl reboot	Restarts the system.
pm-suspend	systemctl suspend	Suspends the system.
pm-hibernate	systemctl hibernate	Hibernates the system.
pm-suspend-hybrid	systemctl hybrid-sleep	Hibernates and suspends the system.

1.5.2 Commando's

Commando	Uitleg
<code>systemctl list-units --type service</code>	Dit geeft een lijst weer van alle services die geladen zijn.
<code>systemctl status *naam*.service</code>	Geeft de status weer van een service.
<code>systemctl is-active *naam*.service</code>	Controleren of een specifieke service draait.
<code>systemctl start *naam*.service</code>	Een specifieke service starten.
<code>systemctl stop *naam*.service</code>	Een specifieke service stoppen.
<code>systemctl restart *naam*.service</code>	Een specifieke service herstarten.
<code>systemctl enable *naam*.service</code>	Een specifieke service enablen.
<code>systemctl disable *naam*.service</code>	Een specifieke service disablen.
<code>systemctl list-units --type target</code>	Geeft een lijst weer van alle gelade targets.
<code>systemctl set-default *naam*.target</code>	Verander de default target.
<code>systemctl rescue OF emergency</code>	Zet het op een andere modus.
<code>systemctl --host *gebruikersnaam*@*hostnaam* *commando*</code>	dit kan je gebruiken om systemd te controleren op een andere machine.

1.6 OpenSSH

1.6.1 Theorie

De systeem configuratie bestanden bevinden zich op deze locatie: `/etc/ssh/...`

De gebruiker specifieke configuratie bestanden bevinden zich in `~/.ssh/...`

Voor het generen van een ssh sleutel moet je de volgende stappen volgen:

1. typ `ssh-keygen -t rsa/ecdsa` in en druk op enter
2. Vul de *passphrase* in.
3. Verander de permissie van de ssh-directory met `chmod 700 ~/.ssh`
4. Kopieer deze sleutel naar remote machine `ssh-copy-id *gebruiker*@*hostnaam*`

Om een ssh agent te configureren moet je allereerst zeker zijn dat de *openssh-askpass*-package geïnstalleerd is. Daarna moet je bij startup programs `/usr/bin/ssh-add` toevoegen.

1.6.2 Commando's

Commando	Uitleg
systemctl start sshd.service	Het starten van een OpenSSH server.
systemctl stop sshd.service	Stop de service.
systemctl enable sshd.service	Enablen van de service
ssh *hostnaam*	Een sessie starten met ssh naar een andere host.
scp *localfile* *user- naam*@*hostnaam*:*remote- locatie*	Dit verplaatst een lokaal bestand naar een remote locatie.
sftp *user- name@hostname*	Opent een beveiligde FTP sessie.

1.7 Web Servers

1.7.1 Theorie

De configuratie bestanden die de service httpd leest, zijn geplaatst in */etc/httpd/conf/httpd.conf* (de main configuratie file) en in */etc/httpd/conf.d* (niet zo belangrijk). Meer informatie over eventueel zelf maken en toevoegen van keys is te vinden in hoofdstuk 3 van de redhat manual (link laatste blad).

1.7.2 Commando's

Commando	Uitleg
apachectl configtest	De configuratie file testen op errors.
yum install httpd	Installeren dan de apache http server.
systemctl start/restart/stop httpd.service	Basisbewerkingen met de service
systemctl reload httpd.service	Laat de service draaien maar herlaadt de configuratie file.
service httpd graceful	Herlaadt de configuratie file zonder de actieve requests aan te raken.
systemctl is-active httpd.service	Kijken of de service actief is of niet.
yum install httpd-devel	Pakket dat belangrijk is als je nieuwe DSO modules wilt maken.
LoadModule ssl_module modules/mod_ssl.so	Een nieuwe module toevoegen.
apxs -i -a -c *module- naam.c*	Zelf een module bouwen.
yum install mod_ssl openssl	Pakket dat nodig is om SSL server te maken

1.8 Mail Servers

1.8.1 Theorie

Redhat geeft je twee primaire MTA's (mail transport agents) namelijk Postfix en Sendmail. Postfix is de default MTA en sendmail is de tweede in de rangorde.

Create a `/etc/postfix/ldap-aliases.cf` file if you do not have one already and make sure it contains the following:

```
server_host = ldap.example.com
search_base = dc=example, dc=com
```

where `ldap.example.com`, `example`, and `com` are parameters that need to be replaced with specification of an existing available LDAP server.

De sendmail configuratie file bevindt zich in `/etc/mail/sendmail.cf`. Hier mag je best geen directe wijzigingen doen, die doe je best in `/etc/mail/sendmail.mc`. Om dit verder in detail te bekijken, bekijk je best eens 10.3.2.2. Je hebt ook nog het programma fetchmail. Dit ontvangt mail van een remote server en levert die aan de lokale MTA.

1.8.2 Commando's

Commando	Uitleg
<code>alternatives -config mta</code>	Met dit commando verander je de default MTA naar de 2de MTA.
<code>systemctl restart postfix</code>	Herstarten van de postfix service.
<code>yum install sendmail</code>	Installeren van sendmail package.
<code>yum install sendmail-cf</code>	Installeren en configureren van sendmail package
<code>make all -C /etc/mail/</code>	Maken van nieuwe configuratiefile.
<code>yum install fetchmail</code>	Fetchmail package aanmaken.
<code>yum install spamassassin</code>	Installeren van spamfilter.
<code>systemctl start/enable spamassassin</code>	starten van spamfiler.
<code>yum install stunnel</code>	Voor een externe OpenSSL bibliotheek.
<code>make stunnel.pem</code>	Maken van zelf gesigneerd SSL certificaat in de locatie <code>/etc/pki/tls/certs/</code> .

1.9 File Server

1.9.1 Theorie

De samba daemons zijn **smbd**, **nmbd** en **winbindd**. Om te connecteren met een sambashare via Nautilus kijk je best eens naar 12.1.3! Nu volgt een belangrijk stuk, het invullen van de configuratie file van de samba server!

To specify the Windows workgroup and a brief description of the Samba server, edit the following lines in your `/etc/samba/smb.conf` file:

```
workgroup = WORKGROUPNAME
server string = BRIEF COMMENT ABOUT SERVER
```

```
[sharename]
comment = Insert a comment here
path = /home/share/
valid users = tfox carole
public = no
writable = yes
printable = no
create mask = 0765
```

The above example allows the users `tfox` and `carole` to read and write to the directory `/home/share`, on the Samba server, from a Samba client.

Bovenstaande zaken worden ingevuld in de configuratiefile op deze locatie: `/etc/samba/smb.conf`. Indien de samba server ook moet dienen als een WINS-server, dan voegen we dit lijntje toe aan de `[global]` sectie van het configuratie bestand: `wins support = yes`.

1.9.2 Commando's

Commando	Uitleg
yum install samba	Installeren van de file server package.
smbclient //ihost-name _i /isharename _i -U iusername _i	Verbinding maken naar een samba share van de shell prompt.
mount -t cifs //iserver-name _i /isharename _i /mnt/point/ -o user-name=iusername _i ,password=ipassword _i	Het mounten van een sambashare.
yum install cifs-util	Noodzakelijk om een share te mounten.
systemctl restart smb.service	Herstarten van de sambaserver.
systemctl start/stop smb.service	Stoppen en starten van de samba service.
systemctl try-restart smb.service	Kijken of herstarten mogelijk is.
net -l share -S wakko	Toont alle beschikbare shares voor een host met de naam wakko.
net -l user -S Wakko	Toont een lijst van samba users voor een host met de naam wakko.
nmblookup trek	Geeft het ip adres van de NetBIOS naam trek.
pdbedit -a Kristin	Voegt ene gebruiker Kristin toe aan de SAM database.
smbclient i//server/share _i ipass-word _i ioptions _i	Ongeveer zelfde functionaliteit als ftp.
smbcontrol -i	Zendt control berichten naar de draaiende smbd, nmbd en winbind daemons.
smbpasswd ioptions _i iusername _i ipassword _i	Beheer van wachtwoorden, een superuser kan elke user zijn wachtwoorden hier met veranderen.
smbstatus ioptions _i	De status van huidige connecties naar de samba server.
testparm	Handig of te testen of je configuratie file wel in orde is.
systemctl start/stop/restart vs-ftp.service	Opdrachten uitvoeren bij deze service.
chcon -R -t public_content_t /path/to/directory	Ervoor zorgen dat shares anoniem worden gedeeld.
setsebool -P allow_ftp.anon_write=1	Noodzakelijk om bovenstaande commando uit te voeren.

1.10 System Monitoring tools

1.10.1 Commando's

Commando	Uitleg
ps ax	Toont alle processen die momenteel draaien op de machine
ps aux	Toont alle processen met usernames erbij.
top	Geeft een real time lijst van processen mee.
free	Toont het vrije en gebruikte geheugen.
gnome-systemmonitor	Toont CPU-gebruik.
lsblk	Toont een lijst van beschikbare block apparaten.
blkid	Geeft informatie over beschikbare block devices.
findmnt	Geeft lijst van huidige gemounte bestand systemen.
df	Geeft gedetailleerd rapport weer van schijfgebruik van het systeem.
du	Laat zien hoeveel schijfruimte er wordt gebruikt door bestanden in een directory.
lspci	Informatie over de PCI buses n apparaten die eraan hangen.
yum install net-snmp net-snmp-libs net-snmp-utils	installeren van pakketen om SNMP te installeren.
systemctl start/stop/restart snmpd.service	interactie met de service.

1.11 Log Files

1.11.1 Commando's

journalctl	Laat het journaal zien met de logs.
systemctl restart systemd-journald	Journal herstarten.
yum install gnome-system-log	Installeren van een system log.
gnome-sysem-log	Opent de system log.

2 Centos 7 - Networking Guide

2.1 NetworkManager

2.1.1 Theorie

De default manier van netwerken te configureren is via het script dat zich bevindt op deze locatie: */etc/init.d/network*. De */etc/sysconfig/* map is een

locatie voor al de configuratie bestanden en scripts. De meeste netwerkconfiguratie bevindt zich hier. Het bestand `/etc/sysconfig/network/` is voor de globale settings van het netwerk. Voor de VPN-informatie kijk je best naar `/etc/NetworkManager/system-connections/`.

Om alle opties van nmcli te begrijpen en te bekijken, ga je best naar de tweede cursus van RedHat en naar puntje 2.3.1.

2.1.2 Commando's

yum install NetworkManager	Installeren van de netwerkmanager.
systemctl status NetworkManager	Kijken naar de status van de netwerkmanager.
systemctl start/stop/restart NetworkManager	Service beheren.
nmcli	Command line manager tool gebruiken.
ip -V	Kijken of de iproute package geïnstalleerd is.
yum install package iproute	Package installeren.
systemctl stop/start/status/restart network	Acties op het script dat zich bevindt op de locatie die in het theorie gedeelte vermeldt staat.
nmcli connection reload	De verbinding met de netwerk manager herladen als je iets hebt aangepast in de ocnfiguratiebestanden.
nmcli dev disconnect jinterfacenaamj	Het stoppen van een interface (deel 1 van een reload)
nmcli con up jinterface-naamj	Het terug starten van een interface (deel 2 van een reload)
nmcli general status	De algemene status van de NetworkManager.
nmcli general logging	Controleer de logging van de NetworkManager.
nmcli connection show (-active)	Toon alle (actieve) connecties van de NetworkManager.
nmcli device status	Toon apparaten die herkent zijn door de NetworkManager.
nmcli con up id bond0	netwerk interface met de naam bond0 aanzetten.
nmcli dev disconnect iface bond0	netwerk interface met de naam bond0 uitzetten.
nmcli con edit	De interactieve tool van nmcli.
nmcli connection add type ethernet con-name jconnection-namej ifname jinterfacenaamj	Een dynamische ethernet connectie toevoegen.
nmcli con up jnaamj	De net aangemaakte connectie aanzetten.

2.2 Hostnamen

2.2.1 Commando's

nmtui	text user interface die kan gebruikt worden om host namen te configureren in een terminal window.
systemctl restart systemd-hostnamed	Herstarten van de hostname daemon na het aanbrengen van wijzingen.
hostnamectl status	de huidige hostname bekijken.
hostnamectl set-hostname [naam]	Alle hostnamen zetten naar deze naam.
nmcli general hostname [naam]	Zelfde effect als hierboven.

2.3 DHCP

2.3.1 Theorie

Bij het installeren van de package, wordt er een configuratiebestand aangemaakt op deze locatie: */etc/dhcp/dhcpd.conf*. In deze configuratiefile zitten veel zaken zoals de subnetdeclaratie:

```
subnet 192.168.1.0 netmask 255.255.255.0 {  
    option routers          192.168.1.254;  
    option subnet-mask      255.255.255.0;  
    option domain-search    "example.com";  
    option domain-name-servers 192.168.1.1;  
    option time-offset      -18000;      #  
    Eastern Standard Time  
    range 192.168.1.10 192.168.1.100;  
}
```

Een range parameter:

```
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-search "example.com";
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.10 192.168.1.100;
}
```

Static IP adres toewijzen:

```
host apex {
    option host-name "apex.example.com";
    hardware ethernet 00:A0:78:8E:9E:AA;
    fixed-address 192.168.1.4;
}
```

Static met meerdere interfaces:

```
Host apex.0 {
    option host-name "apex.example.com";
    hardware ethernet 00:A0:78:8E:9E:AA;
    option dhcp-client-
identifier=ff:00:00:00:00:00:02:00:00:02:c9:00:00:02:c9:0
3:00:31:7b:11;
    fixed-address
172.31.0.50,172.31.2.50,172.31.1.50,172.31.3.50;
}

host apex.1 {
    option host-name "apex.example.com";
    hardware ethernet 00:A0:78:8E:9E:AB;
    option dhcp-client-
identifier=ff:00:00:00:00:00:02:00:00:02:c9:00:00:02:c9:0
3:00:31:7b:12;
    fixed-address
172.31.0.50,172.31.2.50,172.31.1.50,172.31.3.50;
}
```

Shared network declaratie:

```
shared-network name {
    option domain-search          "test.redhat.com";
    option domain-name-servers    ns1.redhat.com,
ns2.redhat.com;
    option routers                192.168.0.254;
    #more parameters for EXAMPLE shared-network
    subnet 192.168.1.0 netmask 255.255.252.0 {
        #parameters for subnet
        range 192.168.1.1 192.168.1.254;
    }
    subnet 192.168.2.0 netmask 255.255.252.0 {
        #parameters for subnet
        range 192.168.2.1 192.168.2.254;
    }
}
```

Group declaratie:

```
group {
    option routers                192.168.1.254;
    option subnet-mask            255.255.255.0;
    option domain-search          "example.com";
    option domain-name-servers    192.168.1.1;
    option time-offset            -18000;    # Eastern
Standard Time
    host apex {
        option host-name "apex.example.com";
        hardware ethernet 00:A0:78:8E:9E:AA;
        fixed-address 192.168.1.4;
    }
    host raleigh {
        option host-name "raleigh.example.com";
        hardware ethernet 00:A1:DD:74:C3:F2;
        fixed-address 192.168.1.6;
    }
}
```

Een goed voorbeeld kan je altijd nog vinden in puntje 10.4.1. uit hoofdstuk 2!

2.3.2 Commando's

yum install dhcp	Installeren van dhcp.
cat /etc/dhcp/dhcpd.conf	Openen van de configuratiefile.
systemctl start/stop/restart dhcpd.service	Acties met de dhcp server daemon.
systemctl start dhcpd6	Starten van de service voor ipv6 versie van dhcp.

2.4 DNS/BIND

2.4.1 Theorie

Welke bestanden je moet aanmaken en hoe deze eruit zien, kan je vinden in het ansible-gedeelte van deze samenvatting. Daar wordt er ook over DNS gepraat en hoe je deze files moet invullen! De main configuratiefile bevindt zich in */etc/named.conf*.

2.4.2 Commando's

yum install bind-chroot	Installeren van bind in een chroot omgeving.
systemctl status named	Kijken of de service wel effectief draait.
systemctl stop/start/restart named	Spreekt voor zich.
rndc reload	herladen van de configuratie file en de zones.
rndc reload localhost	Specifieke zone herladen.
rndc freeze localhost	Als je zelf een zone gaat aanpassen die Dynamic DNS gebruikt, moet je dit commando eerst invoeren.

3 Centos 7 - SELinux

3.1 Werken met SELinux

3.1.1 Theorie

Er zijn heel wat pakketten nodig om selinux te draaien en al deze pakketten staan in puntje 4.4.1 van deel 3. Kijk of deze allemaal geïnstalleerd staan en zo niet, dan moet je ze natuurlijk installeren!

3.1.2 Commando's

<code>ls -l {filenaam}</code>	Kijken naar de permissies van een bestand.
<code>passwd</code>	Veranderen van een wachtwoord voor een gebruiker.
<code>id -Z</code>	Kijken naar de SELinux context die geassocieerd is met jouw Linux gebruiker.
<code>systemctl enable auditd.service</code> (en <code>rsyslog.service</code>)	De log services enablen.
<code>systemctl is-enabled auditd</code> (en <code>rsyslog</code>)	Kijken of ze wel enabled staan.
<code>sestatus</code>	Kijk de status van SELinux.
<code>getenforce</code>	Kijken of SELinux aanstaat of niet.
<code>getsebool -a</code>	Een lijst met alle booleans die er zijn en of ze aan of uit staan.
<code>getsebool {naam} on</code>	Een specifieke boolean aanzetten.
<code>chcon -t httpd_sys_content_t {filenaam}</code>	Permanent veranderen van een specifiek bestand.
<code>ls -Z {directory} {bestand}</code>	Kijken naar alle gegevens van een directory of bestand.
<code>cp -preserve=context {bestandnaam} {nieuwelocatie}</code>	SELinux toewijzing behouden van een bestand als het wordt gekopieerd naar nieuwe locatie.

4 Ansible

4.1 Installeren van packages

4.1.1 Eén package

```
- name: Install common packages
  yum: pkg=nginx state=installed
```

De naam kies je zelf wat je hier invult, het spreekt voor zich dat dit betrekking heeft tot de actie die je uitvoert. Dan volgt het *yum*-commando waar je een specifieke package typt en deze als state *installed* meegeeft.

4.1.2 Meerdere packages

```
- name: Install common packages
  yum: pkg={{item}} state=installed
  with_items:
    - libselinux-python
    - php
    - nginx
```

Hier geven we bij `pkg` een verzameling van items mee. Deze items worden in `with_items` onder elkaar gespecificeerd. Opgelet wel dat er geen tabs worden gebruikt, enkel spaties! Het is ook belangrijk dat deze recht onder elkaar komen of je krijgt een error.

4.2 Firewall

4.2.1 Enable Firewall

```
- name: Enable firewall
  service: name=firewalld state=running enabled=true
```

Hier pakken we de service met de naam *firewalld* (zo noemt de firewall service) en zorgen we dat de status verandert naar *running* en zorgen we er ook voor dat hij aanstaat.

4.2.2 Configureren één service voor Firewall

```
- name: Configure firewall
  firewalld: service=http state=enabled permanent={{ item }}
  with_items:
    - [ 'yes' , 'no ']
```

Hier specificiëren we de service `http` in de firewall daemon en zetten we deze op *enabled*. Daarna zetten we dit op permanent.

4.2.3 Configureren van meerdere services voor Firewall

```
- name: Configure firewall
  firewallld: service={{ item[0] }} state=enabled permanent={{ item[1] }}
  with_nested:
    - [ 'http' , 'https' ]
    - [ 'yes' , 'no ' ]
```

Hier werken we ook met een itemlist om meerdere services door te laten door de firewall.

4.3 Services

4.3.1 Starten van service

```
- name: Start mariadb service
  service: name=mariadb state=running enabled=yes
```

Niet zo moeilijk, je geeft de naam in van de service die je wilt starten. Daarna zet je de state op *running* en enabled op yes. Je kan dit ook voor meerdere services tegelijkertijd doen, maar dat is niet echt meer overzichtelijk.

4.4 Files & Templates

4.4.1 Eigenaar veranderen

```
- name: Change ownership of /var/www/html/
  file: >-
    path=/var/www/html/
    owner=apache
    group=apache
    state=directory
    recurse=yes
```

Hier is het belangrijk dat je het juiste pad ingeeft en natuurlijk de naam van de eigenaar en van de groep waarin deze zit. Als het een directory is dan moet de state *directory* zijn natuurlijk.

4.4.2 Bestand kopiëren in VM

```
- name: Copy wp-config file to /var/www/html/wordpress
  template: src=wp-config.php dest=/var/www/html/wordpress
```

Belangrijk is hier dat het bestand dat je wilt kopiëren zich in de templates directory bevindt. Als deze zich daar bevindt, dan hoef je bij src enkel de naam van het bestand in te typen. Bij dest moet je wel nog het volledige pad intypen.

4.4.3 Bestand unzippen en plaatsen

```
- name: Install unzip
  yum: pkg=unzip state=latest

- name: Unzip WordPress
  unarchive: src=wordpress.zip dest=/var/www/html
```

Eerst installeren we de package die nodig is om later het rar-bestandje te unzippen. De state hier is *latest* zodat de laatste versie genomen wordt. Dan gaan we het rar-bestandje unzippen en plaatsen op de juiste locatie in de virtuele machine.

4.5 MySQL

Buiten het installeren van onderstaande packages, moet je ook de service *mariadb* starten.

4.5.1 Benodigde packages

- mariadb
- mariadb-server
- mySQL-python

4.5.2 Nieuwe database aanmaken

```
- name: Create a new database
  mysql_db: name=dbname state=present collation=utf8_general_ci
```

Spreekt voor zich. Je geeft een naam mee en je zorgt ervoor dat de staat *present* is en dan geef je de bijhorende collatie mee. Eventueel kunnen we er ook nog *enabled = yes* achter zetten.

4.5.3 Databank gebruiker aanmaken

```
- name: Create a database user
  mysql_user: name=dbuser password=dbpasswd priv=*.*:ALL host=localhost state=present
```

Het is belangrijk dat deze gebruiker buiten een naam ook een wachtwoord meekrijgt. Voor de rest (PRIV NOG OPZOEKEN) en de host is *localhost* en de state moet natuurlijk ook *present* zijn.

4.6 Web

Je downloadt de wordpress zip en plaatst die in de map *files*. Daarna unzip je die en plaats je die in */var/www/html* (zie voorbeeld *Bestandunzippenenplaatsen*). Dan moet je de firewall enablen en de services http en httpd doorlaten door de firewall (zie voorbeeld van firewall). Ook moet apache gestart worden (service httpd starten).

4.6.1 Benodigde packages

- httpd
- php
- php-xml
- php-mysql

4.7 DNS

Allereerst moet de service *dns* doorgelaten worden door de firewall. Dan moeten we enkele bestanden aanmaken in de templates map en deze op de juiste locatie plaatsen in de VM. Dit gaat namelijk over *named.conf*, *forwardbestandenreversebestand*

4.7.1 Benodigde packages

- bind
- bind-utils

4.7.2 named.conf

```
options {
    listen-on port 53 { any; };
    listen-on-v6 port 53 { any; };
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query { any; };

    recursion yes;

    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside auto;

    /* Path to ISC DLV key */
    bindkeys-file "/etc/named.iscdlv.key";

    managed-keys-directory "/var/named/dynamic";

    pid-file "/run/named/named.pid";
    session-keyfile "/run/named/session.key";
};

logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};

zone "." IN {
    type hint;
    file "named.ca";
};

zone "linuxlab.net" IN {
    type master;
    file "linuxlab.net.zone";
    allow-update { none; };
};

zone "2.0.192.in-addr.arpa" IN {
    type master;
    file "2.0.192.in-addr.arpa";
    allow-update { none; };
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

bovenaan is het belangrijk dat *listen-onport53* de waarde *any* heeft. Hetzelfde met *listen-on-v6port53*. Verder moeten we nog een zone aanmaken voor het domein (in dit geval linuxlab.net) die verwijst naar het forward lookup bestand (met de naam linuxlab.net.zone). Daaronder komt dan een zone voor de reverse lookup (in dit geval 2.0.192.in-addr.arpa)

```
- name: config bestanden terugzetten
  template:
    src=named.conf
    dest=/etc/named.conf
    owner=root
    group=root
    mode=0644
    validate='named-checkconf %s'
  notify: restart named
```

Hier nemen we het configuratiebestandje en plaatsen we dit op de juiste locatie in de VM. We doen ook een validatie om te kijken af alles wel in orde is. Tot slot herstarten we named door de notify (deze staat gedefinieerd in de handlers-map).

4.7.3 Forward-bestand

Hier moet er maar één bestand van gemaakt worden met de naam **jouwdomein*.zone*

```

; Zone file for linuxlab.net
$ORIGIN linuxlab.net.
$TTL 1W

@ IN SOA pu001.linuxlab.net. hostmaster.linuxlab.net. (
14101813 ; serial
1D ; refresh
1H ; retry
1W ; expire
1D ) ; negative caching TTL

    IN NS pu001.linuxlab.net.

@ IN MX 10 mail.linuxlab.net.

pu001 IN A 192.0.2.2
ns1 IN CNAME pu001

mail IN A 192.0.2.10

```

Overall waar je *linuxlab.net* ziet staan, moet dus jouw domein komen. De ip-adressen zijn die van de dnsserver (pu001 IN A 192.0.2.2) en de andere voor de mailservers die in dit geval 192.0.2.10 is.

```

- name: forward bestand toevoegen
  template:
    src=linuxlab.net.zone
    dest=/var/named/linuxlab.net.zone
    owner=root
    group=root
    mode=0644
  notify: restart named

```

Hier wordt het forward-bestand op de juiste locatie gezet en hierna wordt er weer gebruik gemaakt van de handler *restartnamed*.

4.7.4 Reverse-bestand

```

; Reverse zone file for {{ bind_zone_name }}
; {{ ansible_managed }}
; vi: ft=bindzone

$TTL {{ bind_zone_ttl }}
$ORIGIN {{ item.reverse }}.in-addr.arpa.

@ IN SOA {{ bind_zone_name_servers|first }}.{{ bind_zone_name }}. {{ bind_zone_hostmaster_email }}.{{ bind_zone_name }}. (
{{ timestamp.stdout }}
{{ bind_zone_time_to_refresh }}
{{ bind_zone_time_to_retry }}
{{ bind_zone_time_to_expire }}
{{ bind_zone_minimum_ttl }} )

{% for ns in bind_zone_name_servers %}
    IN NS    {{ ns }}.{{ bind_zone_name }}.
{% endfor %}

{% for host in bind_zone_hosts if host.ip.startswith(item.ip) %}
{{ ('.'.join(host.ip.replace(item.ip+'.','').split('.')[:-1])).ljust(8) }} IN  PTR  {{ host.name }}.{{ bind_zone_name }}.
{% endfor %}

```

```
- name: reverse bestand publiek toevoegen
template:
  src=2.0.192.in-addr.arpa
  dest=/var/named/2.0.192.in-addr.arpa
  owner=root
  group=root
  mode=0644
notify: restart named
```

5 Troubleshooting

5.1 Hardware

Zijn de kabels correct aangesloten? Dit kan je in virtualbox testen door bij instellingen en netwerkkaarten te kijken of deze wel aangesloten zijn.

5.2 Netwerkinterface

Kijken naar de Ethernet-poort van de pc of de switch. De kleur van de lichtjes zijn hier belangrijk! Bij een VM kan je kijken of de correcte adapter is gekozen. Dit doe je door naar de settings te gaan van het netwerk en daar kan je kijken naar NAT, Bridged, enz enz...

5.3 Internet

Hier kijken we eerst naar de machine zelf en dan pas naar buiten!

5.3.1 Commando's

ip a	Kijken of de ip adresseringen nog wel kloppen.
ip r	Kijken naar de Default Gateway, of deze wel nog correct is.
cat /etc/resolv.conf	Kijken naar configuratie bestand voor DNS-server.
ping {default gateway}	Is d default gateway nog bereikbaar.
ping {andere host binnen subnet}	Kijken of je andere host in subnet kan bereiken.
tracert, traceroute, tcp-traceroute, tracepath	De route naar buiten bekijken, maar kan ook niet werken als router ICMP blokkeert.
ping {DNS}	Kijken of je de DNS-server kan pingen.
dig, host, nslookup	Kijken of er DNS requests kunnen opgevraagd worden.

5.4 Transport

Zijn de juiste poorten open en draait de service?

- `sudo systemctl status httpd.service`
- `sudo ss -tulpn`
- `ps -ef`

Wordt de poort geblokkeerd door de firewall?

- `sudo firewall-cmd --list-all`
- `sudo iptables -L -n -v`

Van buitenaf: portscanner

- `nmap -A -T4`
- `nmap -sS -sU`

5.5 Applicatie

Client software of troubleshooting tools

- `curl`, `wget` = voor een webbrowser
- `smbclient`, `nmblookup`, `net use` = fileserver

BEKIJKEN VAN DE LOGFILES!!!!

- `sudo journalctl -f -u httpd.service` (voor deze service dan specifiek)
- `journalctl -f` = opent een speciaal terminalvenster
- `journalctl -b` = logfiles van de huidige boot.

5.6 Geen internet, wat nu?

1. Kijken of de kabels zijn aangesloten.
2. Kijken naar de led lichtjes
3. IP-adres controleren, kun je doen met `ip a`. Hier zie je alle Ethernetpoorten en het loopback adres met hun configuratie.
4. Default gateway checken met `ip r`.
5. `cat /etc/resolv.conf` = Kijken naar nameserver shizzle.

Als er bij stap 3 enkel 'lo' te zien valt, dan wilt dit zeggen dat je netwerkkkaart(en) niet zijn opgestart. Dit kan je nakijken in `/etc/sysconfig/network-scripts/`. Daar moet je het bestandje `ifcfg-naam` van poort_{*i*} zien. Als de netwerkkkaart zichtbaar is, maar als er geen ip adres is, dan kijk je best nog eens naar de kabel. Het kan ook zijn dat je geen ip adres hebt gekregen van de dhcp-server, dit kan je testen door het commando `less /var/log/messages`. Hier moet je een

DHCPDISCOVER, OFFER, REQUEST en PACK zien. Je kan ook een verkeerd ip adres zien, dit kun je ook weer controleren door naar de pagina van de Ethernetpoort te kijken.

Bij stap 4, als er een verkeerde is ingesteld, kan je dit weer zien in */etc/sysconfig/network-scripts/*. Als je er geen hebt gehad van de dhcp server dan kan je ook is kijken bij *less /var/log/messages*.

Als dit bestand bij stap 5 leeg is dan heb je geen gekregen van dhcp server en moet je weer eens kijken bij de messages.

Als je netwerkkaart verkeerd geconfigureerd is of helemaal niet, dan kan je deze zo configureren door allereerst al naar */etc/sysconfig/network-scripts/* te gaan en daar deze zaken in te vullen:

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
IPADDR=10.0.1.27
NETMASK=255.255.255.0
GATEWAY=10.0.1.1
DNS1=10.0.1.2
DNS2=10.0.1.3
PEERDNS=yes
USERCTL=no
```