Samenvatting Examen Linux for operations

Herhaling leerstof computer systems

Commando's voor het beheren van permissies:

Commando	Taak
`chown`	Verander de eigenaar en groep van een bestand
`chmod`	Verander de permissies van een bestand
`chgrp`	Verander de groep waartoe een bestand behoort
`umask`	Verander de standaard permissies voor nieuwe bestanden
`ls -l`	Toon permissies van bestanden in de huidige directory

Gebruikers en groepen beheren

Commando's voor het beheren van gebruikers en groepen:

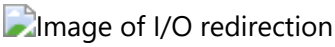
Commando	Taak
`useradd`	Voeg een nieuwe gebruiker toe
`userdel`	Verwijder een gebruiker
`usermod`	Verander de eigenschappen van een gebruiker
`groupadd`	Voeg een nieuwe groep toe
`groupdel`	Verwijder een groep
`groupmod`	Verander de eigenschappen van een groep
`passwd`	Verander het wachtwoord van een gebruiker
`chage`	Verander de eigenschappen van het wachtwoord van een gebruiker

Commando's combineren

I/O redirection:

Syntax	Betekenis
`>`	Stuur de output naar een bestand
`>>`	Voeg de output toe aan een bestand
`<`	Gebruik een bestand als input
pipe	Stuur de output van het ene commando naar het andere commando

Syntax	Betekenis
`2>`	Stuur de error output naar een bestand




```
# stdout en stderr apart wegschrijven
find / -type d > directories.txt 2> errors.txt

# stderr "negeren"
find / -type d > directories.txt 2> /dev/null

# stdout en stderr samen wegschrijven
find / -type d > all.txt 2>&1
find / -type d &> all.txt

# invoer én uitvoer omleiden
sort < unsorted.txt > sorted.txt 2> errors.txt
```

DHCP installeren

Deze handleiding beschrijft hoe je een DHCP-server op AlmaLinux installeert en configureert, en hoe je een Linux Mint VM configureert om via DHCP een IP-adres te verkrijgen.

Stap 1: Installeer de ISC DHCP Server op AlmaLinux

1. **Update je AlmaLinux-pakketlijst**:

   ```
   sudo dnf update -y
   ```

2. **Installeer de ISC DHCP-server**:

   ```
   sudo dnf install dhcp-server -y
   ```

3. **Start en schakel de DHCP-service in om automatisch te starten bij het opstarten**:

```
sudo systemctl start dhcpd
sudo systemctl enable dhcpd
```

Stap 2: Configureer de DHCP Server

1. **Bewerk het configuratiebestand van de DHCP-server**: Open het configuratiebestand `dhcpd.conf` met een teksteditor:

```
sudo vi /etc/dhcp/dhcpd.conf
```

2. **Pas de volgende configuratie toe**:

   Vervang `192.168.76.245` met het juiste gateway-IP van de server, `192.168.76.254`:

```
subnet 192.168.76.0 netmask 255.255.255.0 {
    range 192.168.76.101 192.168.76.254;
    option routers 192.168.76.254;
    option domain-name-servers 8.8.8.8, 8.8.4.4;
    default-lease-time 3600;
    max-lease-time 7200;
}
```

3. **Sla het bestand op** en sluit de editor af (`Ctrl + O` om op te slaan, `Ctrl + X` om af te sluiten).

4. **Start de DHCP-server opnieuw** om de wijzigingen toe te passen:

```
sudo systemctl restart dhcpd
sudo systemctl status dhcpd
sudo systemctl enable --now dhcpd
```

De leases kunnen worden bekeken in: `/var/lib/dhcpd/dhcpd.leases`

Stap 3: Configureer de Linux Mint VM om DHCP te gebruiken

1. **Verwijder het bestaande DHCP-lease op de Linux Mint VM**:

```
sudo dhclient -r
```

2. **Verkrijg een nieuw IP-adres via DHCP**:

```
sudo dhclient
```

3. **Controleer het toegewezen IP-adres en de routing tabel**:

```
ip a
ip route
```

De `ip route` output moet nu het volgende tonen:

```
default via 192.168.76.254 dev enp0s3
```

Stap 4: Controleer Internetverbinding op Linux Mint

1. **Test de verbinding met een extern IP-adres**:

```
ping 8.8.8.8
```

2. **Test de verbinding met een domeinnaam**:

```
ping google.com
```

Stap 5: Oplossen van Problemen

Verkeerde Default Gateway

Als de Linux Mint VM nog steeds de verkeerde default gateway krijgt, zorg er dan voor dat de configuratie van de DHCP-server het juiste gateway-IP bevat:

- **Herstart de DHCP-server op AlmaLinux**:

```
sudo systemctl restart dhcpd
```

- **Verkrijg een nieuw DHCP-lease op Linux Mint**:

```
sudo dhclient -r
sudo dhclient
```

Controleer daarna opnieuw de routing tabel:

```
ip route
```

Installatie van een webserver

Installatie van een webserver op een enterprise Linux-distributie:

- L: Linux (AlmaLinux)
- A: Apache

- M: MariaDB
- P: PHP

LAMP stack installeren op AlmaLinux:

```
sudo dnf install httpd mariadb-server php
sudo systemctl start httpd mariadb
sudo systemctl enable httpd mariadb
```

Services testen

```
sudo systemctl status httpd mariadb
```

Poort van de webserver openen in de firewall:

```
sudo firewall-cmd --add-service=http --permanent
sudo firewall-cmd --reload
```

Om te kijken welke poorten er in gebruik zijn:

```
sudo ss -tulnp
```

Mysql secure installeren:

```
sudo mysql_secure_installation
```

Hardening van een webserver

Firewall instellingen aanpassen:

```
sudo systemctl status firewalld
sudo firewall-cmd --list-all
sudo firewall-cmd --add-service http --permanent
sudo firewall-cmd --add-service https --permanent
sudo firewall-cmd --reload
```

Zones

Een zone is een lijst van regels voor een specifieke situatie. Bv in een publieke ruimte, een thuisnetwerk, werk ...

Commandos voor zones:

Commando	Taak
`firewall-cmd --get-active-zones`	Toon de actieve zones
`firewall-cmd --get-zones`	Toon alle zones
`firewall-cmd --list-all`	Toon de huidige regels

Task	Command
Laat service toe	firewall-cmd --add-service=http
Toon beschikbare services	firewall-cmd --get-services
Laat poort toe	firewall-cmd --add-port=8080/tcp
Firewall-regels herladen	firewall-cmd --reload
Alle netwerkverkeer blokkeren	firewall-cmd --panic-on
Paniekmodus uitschakelen	firewall-cmd --panic-off

SELinux

SELinux is een beveiligingsmechanisme dat extra beveiliging biedt bovenop de standaard Linux-permissies.

Je kan kijken of SELinux actief is met:

```
getenforce
```

Configuratiebestanden van SELinux:

```
cat /etc/selinux/config
```

3 soorten selinux instellingen:

- Booleans
- Contexts, labels
- Policy modules

Context van een bestand controleren

Wat is de huidige context van een bestand?

```
ls -Z /var/www/html/index.html
```

De standaard context van een bestand herstellen:

```
restorecon /var/www/html/index.html
```

Context instellen naar een bepaald type:

```
chcon -t httpd_sys_content_t /var/www/html/index.html
```

Hoe weet je wat selinux blokkeert?

```
sudo tail -f /var/log/audit/audit.log
sudo grep denied /var/log/audit/audit.log
```

Plannen van systeembeheertaken

We kunnen met behulp van cronjobs taken plannen op een Linux-systeem.

ctrl + z om de uitvoer van een proces stil te zetten. bg zet het proces op de achtergrond. & start een proces op de achtergrond (combinatie van ctrl z en bg) Dit zijn de verschillende manieren om cronjobs te beheren:

Commando	Taak
`jobs`	Toon de actieve jobs
`fg NUM`	Breng proces op voorgrond
`bg NUM`	Breng proces op achtergrond

Processen plannen:

Commando	Taak
`crontab -e`	Bewerk de cronjobs van de huidige gebruiker
`crontab -l`	Toon de cronjobs van de huidige gebruiker
`crontab -u USER -e`	Bewerk de cronjobs van een andere gebruiker
`crontab -u USER -l`	Toon de cronjobs van een andere gebruiker
`at now +2 minutes`	Binnen 2 minuten eenmalig een taak uitvoeren
`at 10:00`	Om 10 uur eenmalig een taak uitvoeren
`atq`	Toon de wachtrij van at-taken
`at midnight`	Om middernacht een taak uitvoeren

Taak plannen met crontab:

```

```

```
# m h  dom mon dow   command
  0 0  *   *   *     /path/to/script.sh
```

Veld	Beschrijving	Waarden
MIN	Minuten	0-59
HOUR	Uren	0-23
DOM	Dag van de maand	1-31
MON	Maand	1-12
DOW	Dag van de week	0-7
CMD	Commando	Commando dat moet worden uitgevoerd

Trouble shooting

Fysiekelaag

Controleer de netwerkkabels in de virtual box

- inspecteer de fysieke verbindingen

Datalink

Controleer de IP-configuratie en routing

´´´bash ip a ip r ´´´

Netwerklaag

Bekijk en bewerk de netwerkconfiguratiebestanden.

Resolver configuratiebestand:

```
cat /etc/resolv.conf #Check de nameservers en pas deze aan indien nodig
```

Netwerkconfiguratiebestand:

```
cat /etc/sysconfig/network-scripts/ifcfg-eth1
```

Voorbeeld van confuguratiebestand:

```
BOOTPROTO=none
ONBOOT=yes
```

```
IPADDR=192.168.76.73
NETMASK=255.255.255.0
DEVICE=enp0s8
```

Netwerkinterfaces beheren:

```
sudo systemctl restart NetworkManager #Herstart de netwerkmanager
ip link set eth1 down #Schakel de interface uit
ip link set eth1 up #Schakel de interface in
ip a
```

DNS beheren

DNS-instellingen controleren:

```
cat /etc/resolv.conf
```

Transportlaag

Controleer en configureer de netwerkinstellingen en firewallregels.

```
sudo ss -tulnp
```

Firewall status en regels:

```
sudo systemctl status firewalld
sudo firewall-cmd --list-all
sudo firewall-cmd --add-service=http --permanent
sudo firewall-cmd --zone=public --add-port=80/tcp --permanent
sudo firewall-cmd --reload
sudo firewall-cmd --panic-off
sudo firewall-cmd --set-log-denied=all
```

Applicatielaag

Logs bekijken, applicatie-instellingen en selinux controleren.

```
sudo journalctl -flu x #x vervangen door programma
sudo tail -f /var/log/x #x vervangen door programma
```

SELinux status en logs:

```
sepolocy
sudo restorecon -R /var/www/html
sudo setsebool -P httpd_can_network_connect_db on # geeft toegang om  selinux op
netwerk niveau te omzijlen
```

SSH

SSH is een protocol dat wordt gebruikt om veilig in te loggen op een externe computer.

SSH installeren:

```
sudo dnf install openssh-server
```

SSH service starten:

```
sudo systemctl start sshd
```

SSH service inschakelen:

```
sudo systemctl enable sshd
```

SSH service status controleren:

```
sudo systemctl status sshd
```

SSH poort openen in de firewall:

```
sudo firewall-cmd --add-service=ssh --permanent
sudo firewall-cmd --reload
```

SSH configuratiebestand:

```
cat /etc/ssh/sshd_config
```

SSH service herstarten:

```
sudo systemctl restart sshd
```

SSH logs bekijken:

```
sudo journalctl -u sshd
```

Mounten van een schijf

Alle schijven bekijken:

```
ls /dev/sd*
```

Elke schijf kan maximum 4 partities hebben:

Partitie type	Naming
Primary (max 4)	1 - 4
Extended (max 1)	5
Logical	5+

Een extended partitie kan meerdere logische partities bevatten.

fdisk is een commando om partities te beheren:

```
sudo fdisk -l #Toon alle schijven en partities
```

```
sudo fdisk /dev/sdb #Start fdisk voor schijf sdb
```

Verschillende bestandsystemen:

Bestandssysteem	Commando
ext4	mkfs.ext4
xfs	mkfs.xfs
btrfs	mkfs.btrfs
ntfs	mkfs.ntfs

Partitie formatteren:

```
sudo mkfs -t ext4 /dev/sdb3
```

```
sudo tune2fs -l /dev/sdb3 | grep -i "block count" #Toon het aantal blokken van een partitie
```

Updaten van de reserved blocks, naar 3%:

```
sudo tune2fs -m 3 /dev/sdb3
```

Manueel een partitie mounten:

```
sudo mount /dev/sdb1 /mnt/newmountpoint
```

De partitie binden aan het mountpunt:

```
sudo mount -t ext3 /dev/sdb3 /mnt/newmountpoint
```

Mount punten bekijken:

```
mount | grep sd
```

Permanente mount:

```
cat /etc/fstab
```

UUID

Defenitie: Universally Unique Identifier

- 128 bits
- Gegenereerd tijdens het formatteren

lookup UUID:

```
ls -l /dev/disk/by-uuid
```

DNS met BIND

DNS is een systeem dat domeinnamen vertaalt naar IP-adressen. BIND is een populaire DNS-server. Root DNS servers: zijn de servers die de root zone beheren. Wanneer een DNS server een aanvraag krijgt voor een domeinnaam die hij niet kent, zal hij de root DNS servers contacteren. Deze zullen de DNS server doorverwijzen naar de juiste DNS server. Er zijn verschillende types van DNS servers:

- Authoritative DNS server: bevat de DNS records voor een domeinnaam.
- Forwarding / caching DNS server: zal DNS aanvragen doorsturen naar andere DNS servers en de antwoorden cachen.
- Primary DNS server: bevat de master zone files.

Interactie met BIND

Vraag een domeinnaam op:

```
dig google.com # Nieuwe methode
nslookup google.com # oudere methode
```

Dig reverse lookup:

```
dig -x 193.190.173.132 @ens1.hogent.be +short
```

Dig met IPv6:

```
dig AAAA google.com +short
```

Hoofdconfiguratiebestand van BIND:

```
cat /etc/named.conf
```

Belangrijkste opties

- **listen-on**: port number + network interfaces
  - `any;`
  - `127.0.0.0/8; 192.168.76.0/24`
- **allow-query**: welke hosts mogen queries sturen?
- **recursion**: recursieve queries toelaten
  - zou `no` moeten zijn op een authoritative name server

Zonebestanden

Forward lookup zone voor example.com

```
zone "example.com" IN {
  type primary;
  file "example.com";
  notify yes;
  allow-update { none; };
};
```

Resource records

```
web    IN  A      192.0.2.10
www    IN  CNAME  web
mail   IN  MX 10  mail.example.com.
```

Start of authority (SOA) record, dit record bevat informatie over de zone: de primary name server, de verantwoordelijke persoon, de serial number, de refresh time, de retry time, de expiry time en de minimum TTL.

```
@      IN  SOA  ns1.example.com. hostmaster.example.com. (
                2024121001 ; serial
                3h         ; refresh
                15m        ; retry
                1w         ; expiry
                3h         ; minimum
                )
```

Reverse lookup zone

```
zone "2.0.192.in-addr.arpa" IN {
  type primary;
  file "2.0.192.in-addr.arpa";
  notify yes;
  allow-update { none; };
};
```

RAID

RAID staat voor Redundant Array of Independent Disks. Het is een technologie die meerdieren harde schijven combineert tot één logische eenheid. Er zijn verschillende RAID-niveaus:

- RAID 0: striping
- RAID 1: mirroring
- RAID 5: striping met parity
- RAID 6: striping met dubbele parity
- RAID 10: striping en mirroring

Voordelen en nadelen van verschillende RAID-niveaus:

RAID-niveau	Voordelen	Nadelen
RAID 0	Sneller lezen en schrijven, geen dataredundantie	Geen dataredundantie, geen fouttolerantie
RAID 1	Dataredundantie, fouttolerantie	Minder efficiënt gebruik van schijfruimte
RAID 5	Dataredundantie, fouttolerantie, efficiënt gebruik van schijfruimte	Minder efficiënt schrijven, risico op datacorruptie bij schijffouten
RAID 6	Dataredundantie, fouttolerantie, efficiënt gebruik van schijfruimte	Minder efficiënt schrijven, risico op datacorruptie bij schijffouten
RAID 10	Sneller lezen en schrijven, dataredundantie, fouttolerantie	Minder efficiënt gebruik van schijfruimte, complexere configuratie

Software RAID VS Hardware RAID:

Software RAID	Hardware RAID
Goedkoper	Duurder
Minder snel	Sneller
Minder complex	Complexer
Minder betrouwbaar	Betrouwbaarder

Shellcheck

Shellcheck is een tool die helpt bij het controleren van shellscripts op fouten en stijlproblemen.

Shellcheck installeren:

```
sudo dnf install shellcheck
```

Shellcheck gebruiken:

```
shellcheck script.sh
```