Troublehooten van een Linux systeem

Om een linux systeem te troubleshooten, zijn er een aantal stappen die je kan volgen. We werken volgens de bottom-up methode, we doorloopen alle lagen van het tcp/ip model en kijken op welke er problemen zijn.

- Network access (Link) layer
- Internet layer
- Transport
- Application Layer
- SELinux

Layer	Protocol	Keywords
Application	HTTP, DNS, SMB, FTP, …	
Transport	TCP, UDP	sockets, port numbers
Internet	IP, ICMP, ARP	routing, IP addresses
Network access	Ethernet	switch, MAC address
Physical		cables and connectors

Om de toetsenbord lay-out op België te zetten gebruik je het volgende commando: `localectl set-keymap be`

Network access (Link) laag

Deze laag is verantwoordelijk voor de communicatie tussen 2 nodes op hetzelfde netwerk. De communicatie gebeurt via MAC adressen.

- Check of de kabels goed zijn aangesloten
- Check of de netwerkkaart aan staat
- Kijk naar de lampjes op de switch en de netwerkkaart

In virtualbox kan je de netwerkkaart instellingen controleren.

Internet laag

Deze laag is verantwoordelijk voor de communicatie tussen 2 nodes op verschillende netwerken. De communicatie gebeurt via IP adressen.

- Check of de netwerkkaart een IP adres heeft
- Check of de netwerkkaart de juiste gateway heeft
- Check of de netwerkkaart de juiste DNS server heeft

Een aantal commando's die je kan gebruiken om deze zaken te controleren:

Command	Description

Command	Description
`ip a`	To display all IP addresses assigned to the system
`ip r`	To display the routing table
`cat /etc/resolv.conf`	To display the DNS servers configured on the system
`resolvectl dns`	To display the DNS servers used by systemd-resolved

Controleer ook steeds de volgende zaken:

- IP address?
- In correct subnet?
- DHCP or fixed IP?

Bij DHCP: is de DHCP server bereikbaar? Voorbeeld van een configuratie voor dhcp en static ip:

De instellingen voor de IP adressen kunnen worden teruggevonden in: `nano /etc/sysconfig/network-scripts/ifcfg-*`

```
cat /etc/sysconfig/network-scripts/ifcfg-enp0s3
TYPE=Ethernet
BOOTPROTO=dhcp
NAME=enp0s3
DEVICE=enp0s3
ONBOOT=yes
```

```
cat /etc/sysconfig/network-scripts/ifcfg-enp0s8
BOOTPROTO=none
ONBOOT=yes
IPADDR=192.168.76.73
NETMASK=255.255.255.0
DEVICE=enp0s8
```

Veel voorkomende problemen met DHCP:

Geen IP DHCP unreachable DHCP won’t give an IP 169.254.x.x (APIPA) No DHCP offer, “link-local” address Unexpected subnet Bad config (fixed IP set?)

Watch the logs: sudo journalctl -f

Veel voorkomende problemen met static IP:

Unexpected subnet Check config Correct IP, “network unreachable” Check network mask

Het command 'ip route' geeft de routing tabel weer. Hier kan je zien welke route er gebruikt wordt om een bepaald IP adres te bereiken.

1. Controleren of de gateway ingesteld is

2. Controleren of je in het juiste subnet zit
3. De andere netwerkconfiguratie controleren

Als dat allemaal in orde is kan je de DNS server controleren. Dit kan je doen door het commando `cat /etc/resolv.conf` uit te voeren. Hierin staat welke DNS server gebruikt wordt. Kijk of er een nameserver is ingesteld en of deze bereikbaar is.

Een algemene checklist voor het controleren van de internet laag:

- [ ] Pingen tussen de verschillende hosts
- [ ] Ping de default gateway en de DNS server
- [ ] Query DNS (dig, nslookup, getent)

Let op: sommige routers blokkeren pings, dus dit is niet altijd een goede test.

Transport laag

Cecklist voor de transport laag:

- [ ] Check of de service draait: `systemctl status <service>`
- [ ] Correcte poorten open: `sudo ss -tuln`
- [ ] Firewall regels: `sudo firewall-cmd --list-all`

Controleer ook of de service standaard draait bij het opstarten van de machine: `systemctl is-enabled <service>` Als dit niet het geval is: `systemctl enable <service>`

Hierna kan je de firewall controleren. Dit kan je doen door het commando `sudo firewall-cmd --list-all` uit te voeren. Hierin staat welke poorten open staan en welke services toegelaten zijn. Met `--add-service` kan je een service toevoegen aan de firewall.

Applicatie laag

Controleer of alles goed werkt op de applicatie laag. Dit kan je doen door de logs te controleren. Dit kan je doen door het commando `journalctl -f` uit te voeren. Hierin staan alle logs van de machine.

De logfiles kan je vinden in `/var/log/`. Hierin staan de logs van de verschillende services. Of via het commando `journalctl -u <service>`.

SELinux

SELinux is een security module die standaard aan staat op Fedora en CentOS. Het kan zijn dat SELinux bepaalde acties blokkeert. Dit kan je controleren door het commando `sestatus` uit te voeren. Hierin staat of SELinux aan staat en in welke mode het staat.

Controleer bestandscontext

Is de bestandscontext zoals verwacht? `ls -Z /var/www/html`

Stel de bestandscontext in op de standaardwaarde `sudo restorecon -R /var/www/`

Stel de bestandscontext in op een specifieke waarde `sudo chcon -t httpd_sys_content_t test.php`

Het kan ook interessant zijn om de booleans te controleren. `getsebool -a | grep http`