odisee

ikdoeict.be

Server Administration

Tim Vermeulen

tim.vermeulen@odisee.be

LID VAN ASSOCIATIE KU LEUVEN

OPO's en OLA's

- OPO Server Administration [5STP]
  - **OLA Server Administration (Theorie) [1STP]**
  - OLA Linux server (Lab) [2STP]
  - OLA Windows server (Lab) [2STP]

Evaluatie

Server Administration

- Schriftelijk theorie examen (100%)

Linux Server (Lab)

- Permanente labo-evaluaties (25%)
- Individuele labosessie tijdens de examenperiode(75%)

Windows Server (Lab)

- Permanente labo-evaluaties (25%)
- Individuele labosessie tijdens de examenperiode (75%)

Inhoud theorie

- Inleiding Linux Server
- Active Directory
- DNS
- Webservers
- File Systems
- Toegangsrechten
- Automatisering
- SElinux, Vagrant, memcache
- …

Inleiding Linux server

LES 1

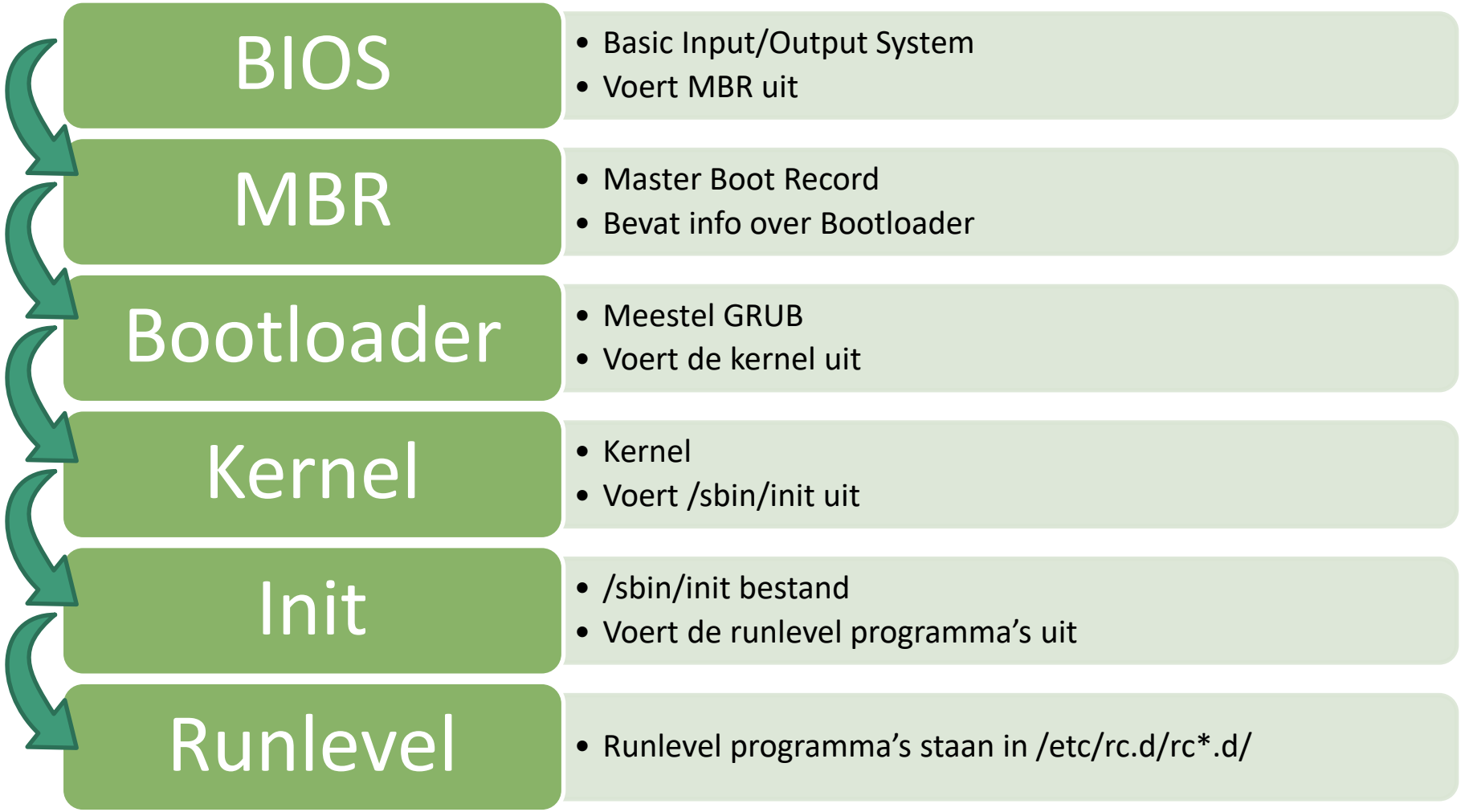
Inhoud

- Boot-proces
- Daemons
- File structuur
- Mounten
- Crontab
- Autenticatie

Inhoud

- **Boot-proces**
- Daemons
- File structuur
- Mounten
- Crontab
- Autenticatie

Linux boot-process



1 BIOS

- BIOS = Basic Input / Output System
- Opgeslagen in ROM (read only)
  - (maar EEPROM, dus ook updates mogelijk)
  - (en BIOS settings in CMOS, batterij gevoed)
- System integrity checks
- Zoekt naar MBR op aangesloten media: CD, USB, HDD, …
  - Volgorde kan ingesteld worden in BIOS settings
  - Tijdens laden BIOS kan ander media gekozen worden (F2, …)
- Voert bootloader uit

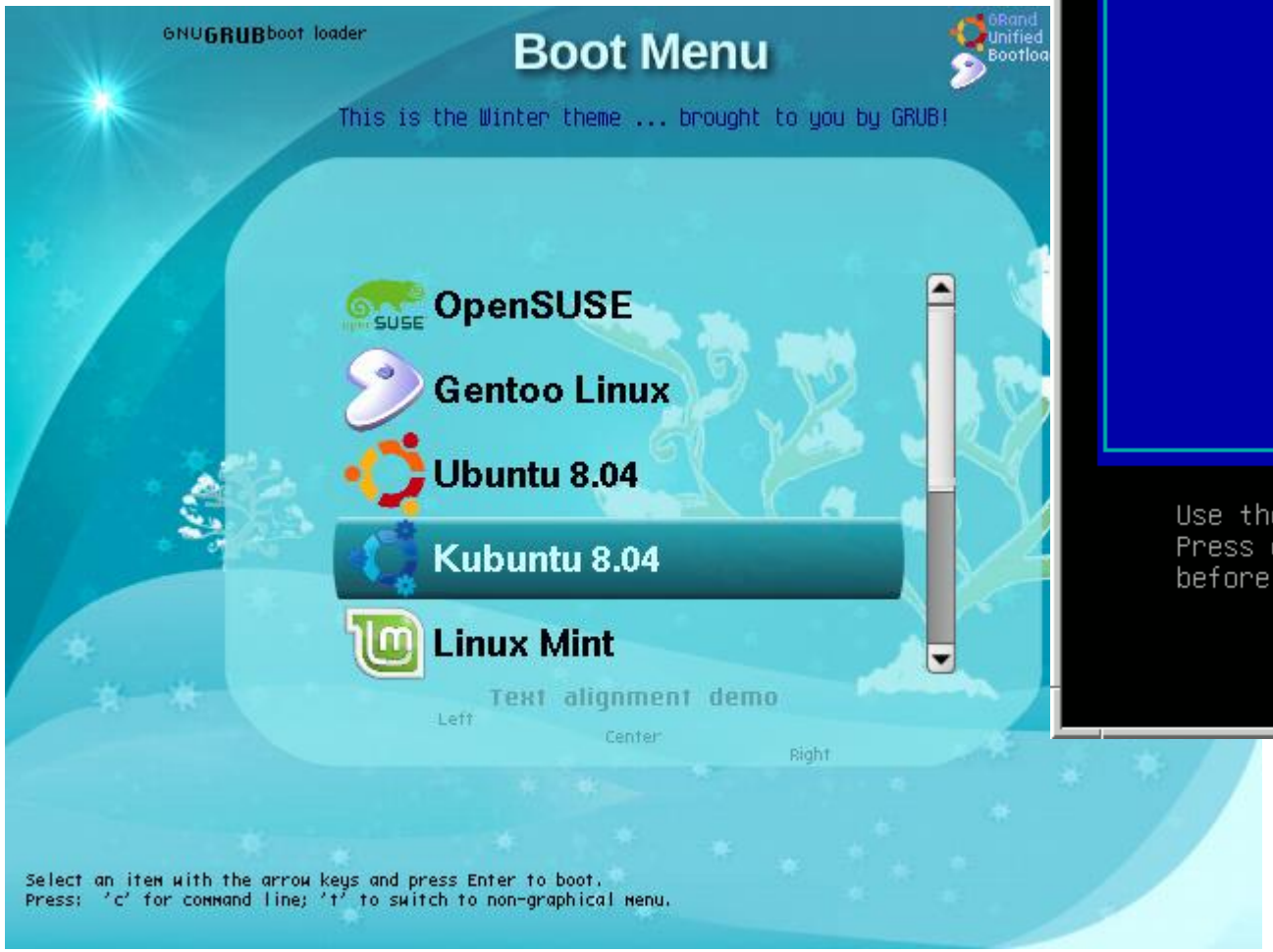
2 MBR

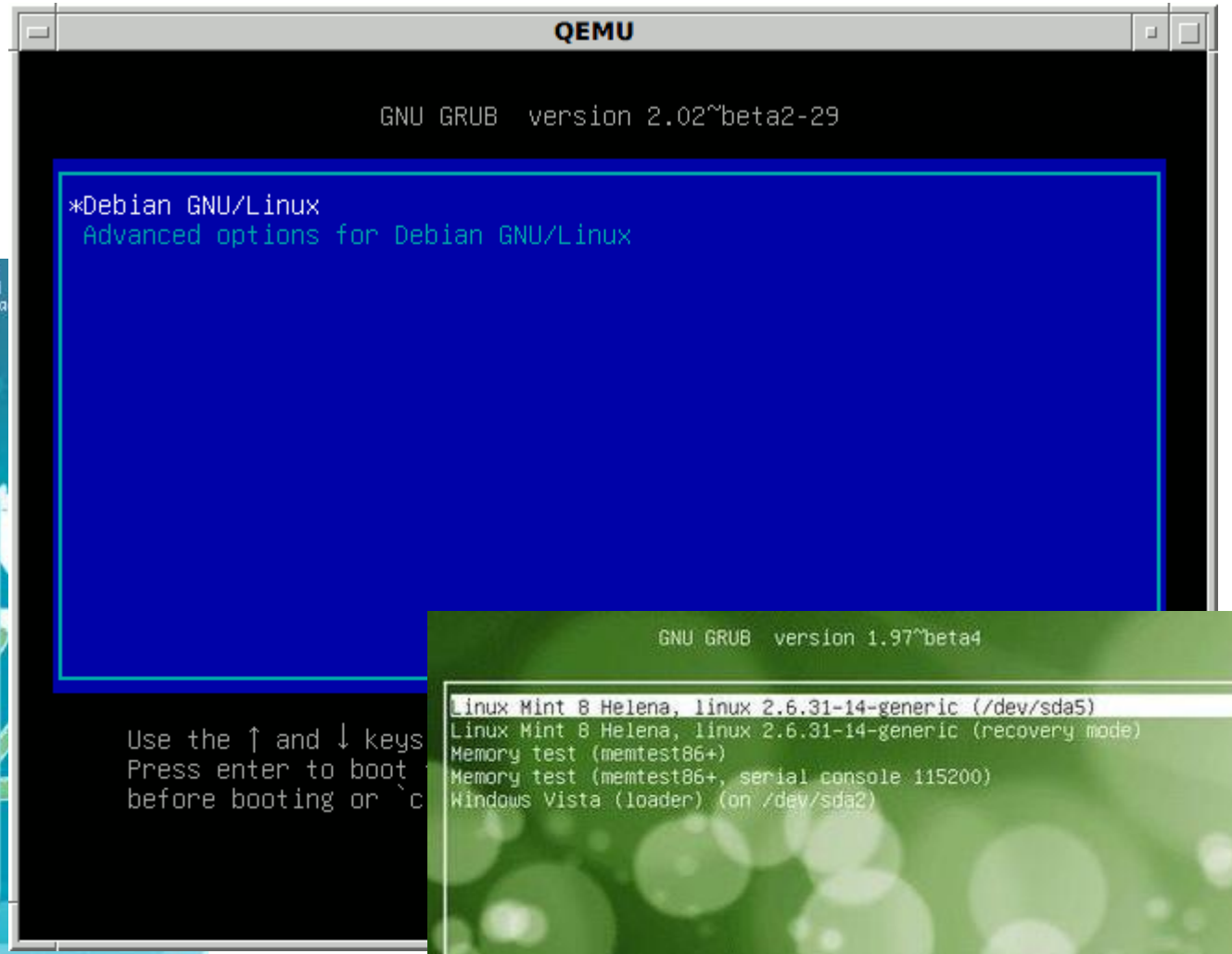
- MBR = Master Boot Record
- 1e sector op opstart media
- Minder dan 515 bytes
  - Primary boot loader (grootste deel)
  - Partitietabel info
  - MBR validation check
- Bevat informatie over bootloader (machine code)
- Laadt de bootloader

3 Bootloader

- Kiezen van te laden OS / kernel via menusysteem
- Command line interface mogelijk
- Lijst van mogelijkheden in configuratie file
- Tegenwoordig vooral GRUB, vroeger LILO
- Uitgebreide lijst: en.wikipedia.org/wiki/Comparison_of_boot_loaders
- Bestaat meestal uit 2 delen:
  - Eerste deel staat in de MBR en heeft als doel het tweede deel te laden
  - Tweede deel bevat de eigenlijke werking

GRUB


GNU GRUB boot loader
Boot Menu
This is the Winter theme ... brought to you by GRUB!
OpenSUSE
Gentoo Linux
Ubuntu 8.04
Kubuntu 8.04
Linux Mint
Text alignment demo
Left
Center
Right
Select an item with the arrow keys and press Enter to boot.
Press: 'c' for command line; 't' to switch to non-graphical menu.


QEMU
GNU GRUB version 2.02~beta2-29
*Debian GNU/Linux
Advanced options for Debian GNU/Linux
Use the ↑ and ↓ keys
Press enter to boot
before booting or `c

GNU GRUB version 1.97~beta4
Linux Mint 8 Helena, linux 2.6.31-14-generic (/dev/sda5)
Linux Mint 8 Helena, linux 2.6.31-14-generic (recovery mode)
Memory test (memtest86+)
Memory test (memtest86+, serial console 115200)
Windows Vista (loader) (on /dev/sda2)
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting or 'c' for a command-line.

GRUB

- GRUB = Grand Unified Bootloader
- Van GNU project
- Grub configuration file (/boot/grub/grub.conf)
  - Beschikbare kernels en besturingssystemen
  - Standaard optie
  - Timeout voor automatische selectie
- Laadt de kernel

GRUB v1

- Opgesplitst in verschillende stages
  - Stage 1:
    - Zit in MBR
    - laden stage 1.5
  - Stage 1.5:
    - File system drivers (=> bestandssysteem beschikbaar)
    - Laden Stage 2 uit bestandssysteem
  - Stage 2:
    - Laden van de configuratiefile (/boot/grub/grub.conf)

GRUB v2

- Aangepaste bestanden
- Meer functionaliteit
- Stage 1: `boot.img`
  - Zit in MBR
  - Laadt `core.img`
- Stage 1.5: `core.img`
- Stage 2: files in `/boot/grub/`, waaronder `grub.cfg`

GRUB2

- Ondersteuning voor scripts met conditionele expressies
- Rescue mode
- Aangepaste menu's
- Themes
- Grafisch boot menu mogelijk
- Ondersteuning voor Live CD ISO's op HDD
- Aangepaste bestands structuur
- Ondersteuning voor meer besturingssystemen
- `update-grub` om updates in de configuratiebestanden door te voeren
- `menu.lst` -> `grub.cfg`

GRUB2

Belangrijkste mappen en bestanden

- /boot/grub/grub.cfg : Het menu
  - Wordt normaal niet manueel aangepast (wel update-grub)
  - Wordt automatisch aangepast bij installatie nieuwe kernel
- /etc/default/grub : Algemene instellingen
- /etc/grub.d/ : scripts
  - Uitgevoerd bij update-grub
  - Samenstellen grub.cfg

4 Kernel

- Initialiseren van RAM
- Mounten van bestandssysteem (root = /)
- Configuratie hardware en laden drivers
- Starten van Init Systeem = eerste proces

5 Init

- Kijkt naar /etc/inittab
- Bepaalt run level adhv default init level in inittab
  - 0 – halt
  - 1 – Single user mode
  - 2 – Multiuser, without NFS
  - **3 – Full multiuser mode**
  - 4 – unused
  - **5 – X11**
  - 6 – reboot
- Start alle processen horende bij deze run level
  (en is dus ouder of grootouder van elk proces)
- Init blijft draaien zolang het systeem actief is

init Init System

- Origineel Init Systeem
- Vast hardgecodeerd bestand: /sbin/init
- Eerste proces => PID = 1
- Alle andere processen worden rechtstreeks of onrechtstreeks gestart door init proces
- Seriële opstart van opstartprocessen

systemd Init system

- Een init systeem gebruikt door steeds meer Linux distributies
- Sinds maart 2010
- 3 functies
  - Systeem en Service manager
  - Software platform
  - Samenhang tussen de kernel en applicaties
- Parallellisatie opstarten van processen -> snelheidswinst
- Standaardisatie van het opstarten en beheren van services
- Naast vervanging voor origineel init systeem verschillende extra features

systemd Init System

Linux distribution	Date added to software repository	Enabled by default?	Can run without?	Date released as default
Debian	April 2012	Yes	Yes	April 2015 (v8)
Fedora	November 2010 (v14)	Yes	No	May 2011 (v15)
Gentoo Linux	July 2011	No	Yes	N/A
openSUSE	March 2011 (v11.4)	Yes		September 2012 (v12.2)
Red Hat Enterprise Linux	June 2014 (v7.0)	Yes	No	June 2014 (v7.0)
SUSE Linux Enterprise Server	October 2014 (v12)	Yes	No	October 2014 (v12)
Ubuntu	April 2013 (v13.04)	Yes		April 2015 (v15.04)

systemd

Belangrijkste onderdelen:

- systemd: systeem en service manager
- systemctl: beheer systemd
- systemd-analyze: statistieken en andere informatie

Services beheren met systemd

Voorbeelden

- `systemctl start sshd`

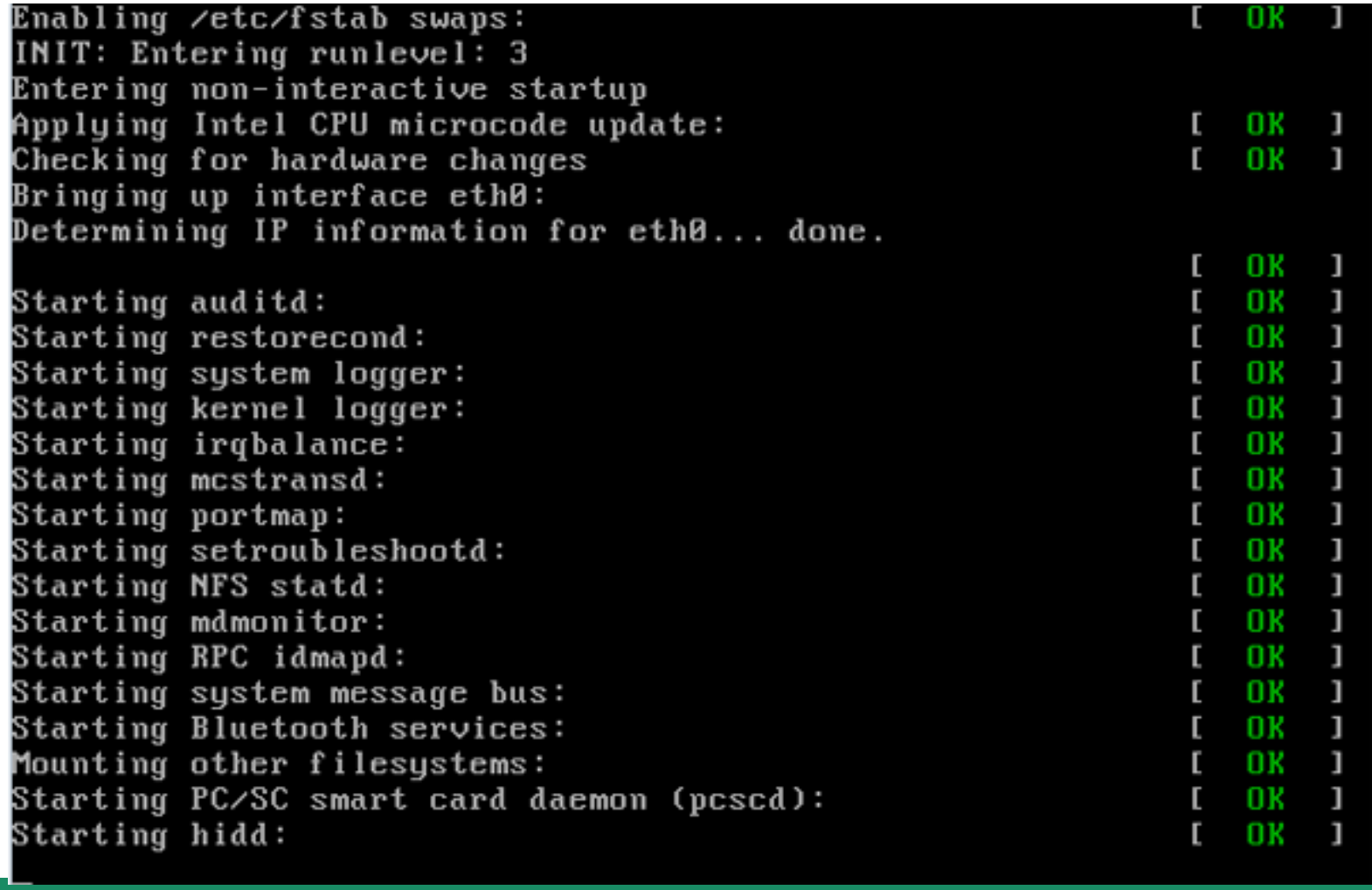
  start de SSH-daemon
- `systemctl restart network`

  herstart de network service
- `systemctl status network`

  kijken of het actief is en of er foutmeldingen zijn

6 Runlevel programs

Afhankelijk van runlevel worden de processen in de map /etc/rc.d/rc*.d/ gestart



rc.local

- Een van de laatste bestanden die uitgevoerd worden door init
- Kan aangepast worden om scripts te laten uitvoeren bij het opstarten

Inhoud

- Boot-proces
- **Daemons**
- File structuur
- Mounten
- Crontab
- Autenticatie

Daemons

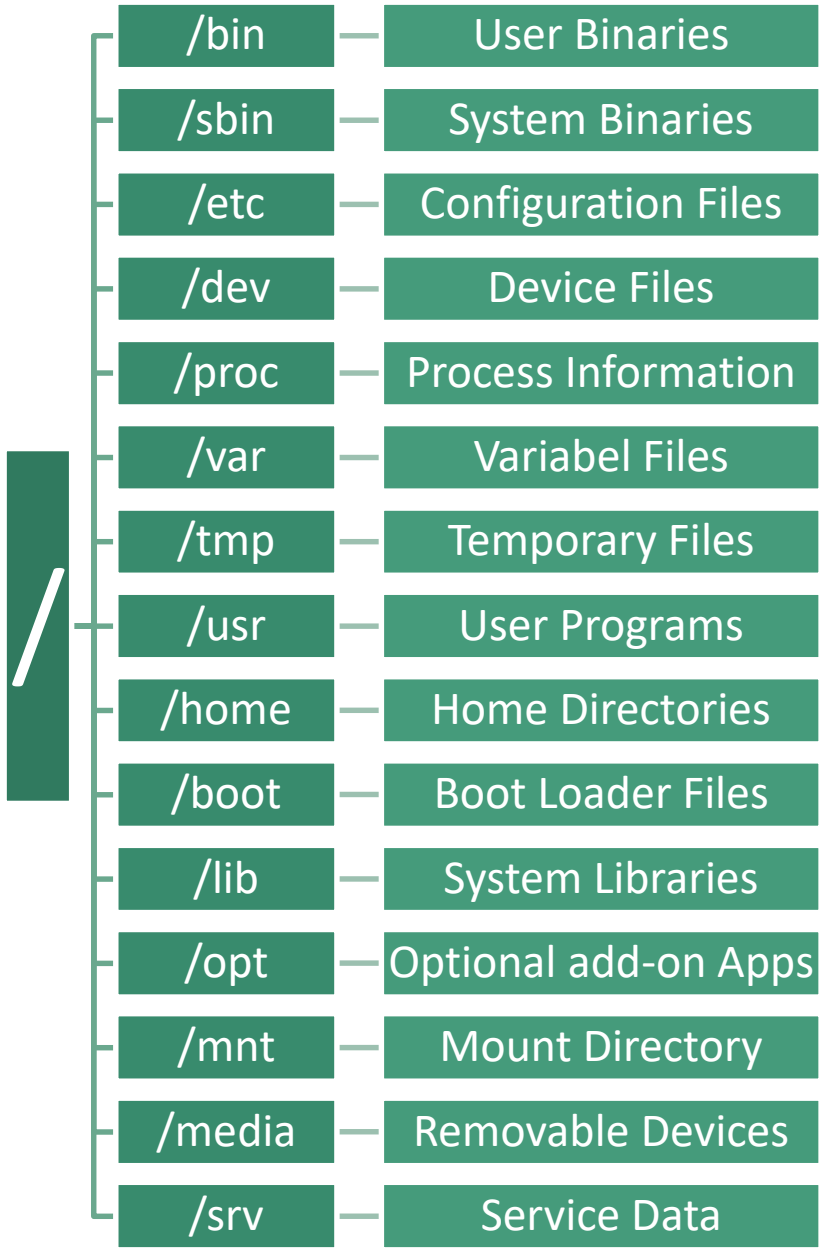
- Processen die op de achtergrond actief zijn
  - Bepaalde taken uitvoeren
  - Diensten verlenen aan andere programma's
- (Services bij Windows)
- Eerste daemon die gestart wordt is `init` (of alternatieven)

Inhoud

- Boot-proces
- Daemons
- **File structuur**
- Mounten
- Crontab
- Autenticatie

File structuur

- Vastgelegd in File Hierarchy Standard



/

- Alle paden van bestanden en mappen beginnen met de root map
- Enkel root gebruiker heeft hier schrijfrechten
- Opmerking: /root is de home folder van de root gebruiker

/bin

User Binaries

- Uitvoerbare binaire bestanden
- Vooral voor gewone gebruikers
- Voorbeelden: ps, ls, ping, grep, cp

/sbin

System Binaries

- Uitvoerbare binaire bestanden
- Vooral voor systeembeheer
- Voorbeelden: iptables, reboot, fdisk, ifconfig, swapon

/etc

Configuration Files

- Algemene instellingen gebruikt door meerdere programma's
- Opstart en stop scripts voor bepaalde programma's
- Voorbeeld: /etc/resolv.conf

/dev

Device Files

- Files gebruikt voor toegang tot devices
- Voorbeelden: /dev/tty1, /dev/usbmono

/proc

Process Information

- Informatie ivm systeem processen en systeem informatie
- Virtuele bestanden en mappen met de informatie
- Voorbeeld: /proc/{pid} bevat informatie over het proces met PID=pid
- Voorbeeld: /proc/uptime

/var

Variable Files

- Bestanden waarvan verwacht wordt dat hun grootte zal toenemen
- Voorbeelden: system log files (/var/log); packages and database files (/var/lib); emails (/var/mail); print queues (/var/spool); lock files (/var/lock); temp files needed across reboots (/var/tmp)

/tmp

Temporary Files

- Tijdelijke bestanden gemaakt door systeem en gebruikers
- Worden verwijderd bij reboot

/usr

User Programs

- binaries, libraries, documentation en source-code voor second level programma's
  - /usr/bin: binary files for user programs
  - /usr/sbin: binary files for system administrators
  - /usr/lib: libraries voor /usr/bin and /usr/sbin
  - /usr/local: users programs that you install from source

/home

Home Directories

- Persoonlijke bestanden van alle gebruikers
- Eén map per gebruiker

/boot

Boot Loader Files

- Kernel initrd, vmlinux, grub files
- Voorbeelden: initrd.img-2.6.32-24-generic, vmlinuz-2.6.32-24-generic

/lib

System libraries

- Libraries voor /bin en /sbin
- Formaat bestandsnamen: ld* of lib*.so.*
- Voorbeelden: ld-2.11.1.so, libncurses.so.5.7

/opt

Optional add-on Applications

- add-on applicaties van individuele verkopers
- Voorbeeld: /opt/lampp/

/mnt

Mount Directory

- Tijdelijke map waar systeembeheerders bestandssystemen kunnen mounten
- Voorbeeld: Windows partitie bij dualboot

/media

Removable Media Devices

- Map om verwijderbare media tijdelijk te mounten
- Voorbeelden: /media/cdrom, /media/floppy, /media/cdrecorder

/srv

Service data

- Data gerelateerd met bepaalde services
- Voorbeeld: /srv/cvs/

Inhoud

- Boot-proces
- Daemons
- File structuur
- **Mounten**
- Crontab
- Autenticatie

Mounten

Commando: `mount`

- In linux alle bestanden geordend in een grote boomstructuur
- Met `mount` bestandssysteem op bepaald device toevoegen aan de boomstructuur op bepaalde plaats
- Standaard gebruik: `mount -t type device dir`
- Terug verwijderen met `umount`

Mounten

`mount -t type device dir`

"This tells the kernel to attach the filesystem found on device (which is of type type) at the directory dir. The previous contents (if any) and owner and mode of dir become invisible, and as long as this filesystem remains mounted, the pathname dir refers to the root of the filesystem on device."

Meer info: `man mount`

Mounten

Voorbeelden

- Mounten van een ISO
  ```
  mount -o loop disk1.iso /mnt/disk
  ```
- Mounten van netwerklocaties
  ```
  mount example.ikdoeict.be:/misc/export /misc/local
  ```
- Mounten van Windows C-schijf bij dual boot
  ```
  sudo mount -t ntfs /dev/hdb1 /media/c
  ```
- Mounten van Windows share
  ```
  mount -t cifs //10.129.32.1/share -o
  username=student,password=Azerty123 /mnt/wserver
  mount -t cifs -o username=voornaam.achternaam
  //fsdm0008.odisee.be/homedir/voornaam.achternaam /mnt/h-schijf
  ```

Mounten

/etc/fstab

- Bepaalt waar bronnen in de filestructuur gemount moeten worden
- Voorbeeld:

```
# device-spec   mount-point     fs-type      options                                    dump pass
LABEL=/         /               ext4         defaults                                      1 1
/dev/sda6       none            swap         defaults                                      0 0
none            /dev/pts        devpts       gid=5,mode=620                                0 0
none            /proc           proc         defaults                                      0 0
none            /dev/shm        tmpfs        defaults                                      0 0

# Removable media
/dev/cdrom      /mnt/cdrom      udf,iso9660  noauto,owner,ro                               0 0

# NTFS Windows 7 partition
/dev/sda1       /mnt/Windows    ntfs-3g      quiet,defaults,locale=en_US.utf8,umask=0,noexec     0 0
```

Inhoud

- Boot-proces
- Daemons
- File structuur
- Mounten
- **Crontab**
- Autenticatie

Crontab

- Uitvoeren van commando's/programma's op bepaalde tijdstippen of met bepaalde periode
- Veel gebruikte toepassingen: ophalen van mails, automatische backups, verzamelen statistieken, …
- (Taakplanner onder Windows)

Crontab

- Lijst van taken bijgehouden in crontab file
  - Globale crontab file in `/etc` of submap
  - Gebruikers kunnen eigen crontab files hebben
- Elke lijn in bestand is een job
  - Voorbeeld:
    0 20 * * * /home/student/scripts/export_dump.sh
  - Structuur:

```
┌──────────────── minuten (0 - 59)
│ ┌────────────── uren (0 - 23)
│ │ ┌──────────── dag vd maand (1 - 31)
│ │ │ ┌────────── maand (1 - 12)
│ │ │ │ ┌──────── dag van de week(0 - 6) (0 tot 6 zijn zondag tot
│ │ │ │ │         zaterdag,  7 is ook zondag)
│ │ │ │ │
* * * * *  commando
```

Inhoud

- Boot-proces
- Daemons
- File structuur
- Mounten
- Crontab
- **Autenticatie**

Authenticatie

- Zowel rechtstreeks als extern (ssh) wordt standaard gebruik gemaakt van gebruikersnaam en wachtwoord
- Verschillende stappen om extra beveiliging te bieden tegen misbruik. Oa:
  - fail2ban
  - Key based authentication

fail2ban

- Bescherming tegen brute force aanvallen op wachtwoorden
- Controle op aantal mislukte aanmeldpogingen
- Verschillende filters mogelijk
- Verschillende services kunnen beschermd worden
  oa: apache, ssh, …
- Verschillende acties mogelijk
  oa: blokkeren IP in firewall, email, …

Key based authentication

- In plaats van aan te melden met gebruikersnaam en wachtwoord, aanmelden door middel van keys
- Voordelen:
  - Veiliger: Geen gebruik van korte wachtwoorden, maar lange random keys
  - Gemakkelijker: Je hoeft niet telkens je wachtwoord in te geven
- TIP: Voor extra beveiliging kan je externe toegang enkel toestaan met key based authentication

Key based authentication

1. Genereer een keypaar (public + private) op de **client**

```
ssh-keygen -t rsa
```

   - Als resultaat 2 bestanden in de map ~/.ssh
     - id_rsa -> de private sleutel
     - id_rsa.pub -> de publieke sleutel

2. Voeg de publieke key toe aan de **server**

```
cat id_rsa.pub >> ~/.ssh/authorized_keys
ssh-copy-id user@server
```

id_rsa.pub

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAg
QDtylVmT7DHSSCBKJRT57TlaGj1Di
jE586m2LfY9E/72xcdqxHg+B0JUaq
qzVSp4UHwXL2CKUjOcxmToDsJOw8a
p/NShYBVJ51PF/oq9F7U0i6KaRU8f
x3VXbvLJSKhBAgHx9QtlO1TxjevIk
zKojuvSczlrgw30RScH8vvIvQvew=
= student@debian
```

Vervolgens de rechten op de bestanden aanpassen zodat enkel de gebruiker rechten heeft

Bronnen

- Linux boot process: http://www.thegeekstuff.com/2011/02/linux-boot-process/ en https://www.centos.org/docs/5/html/Installation_Guide-en-US/s1-boot-init-shutdown-process.html
- GRUB2: https://help.ubuntu.com/community/Grub2
- File System structure: http://www.thegeekstuff.com/2010/09/linux-file-system-structure/
- fstab: https://wiki.archlinux.org/index.php/fstab
- Key based authentication: https://wiki.centos.org/HowTos/Network/SecuringSSH#head-9c5717fe7f9bb26332c9d6757120of8c1e4324bc
- fail2ban: http://www.fail2ban.org/wiki/index.php/MANUAL_0_8