SUSE Linux Enterprise 11
Administration

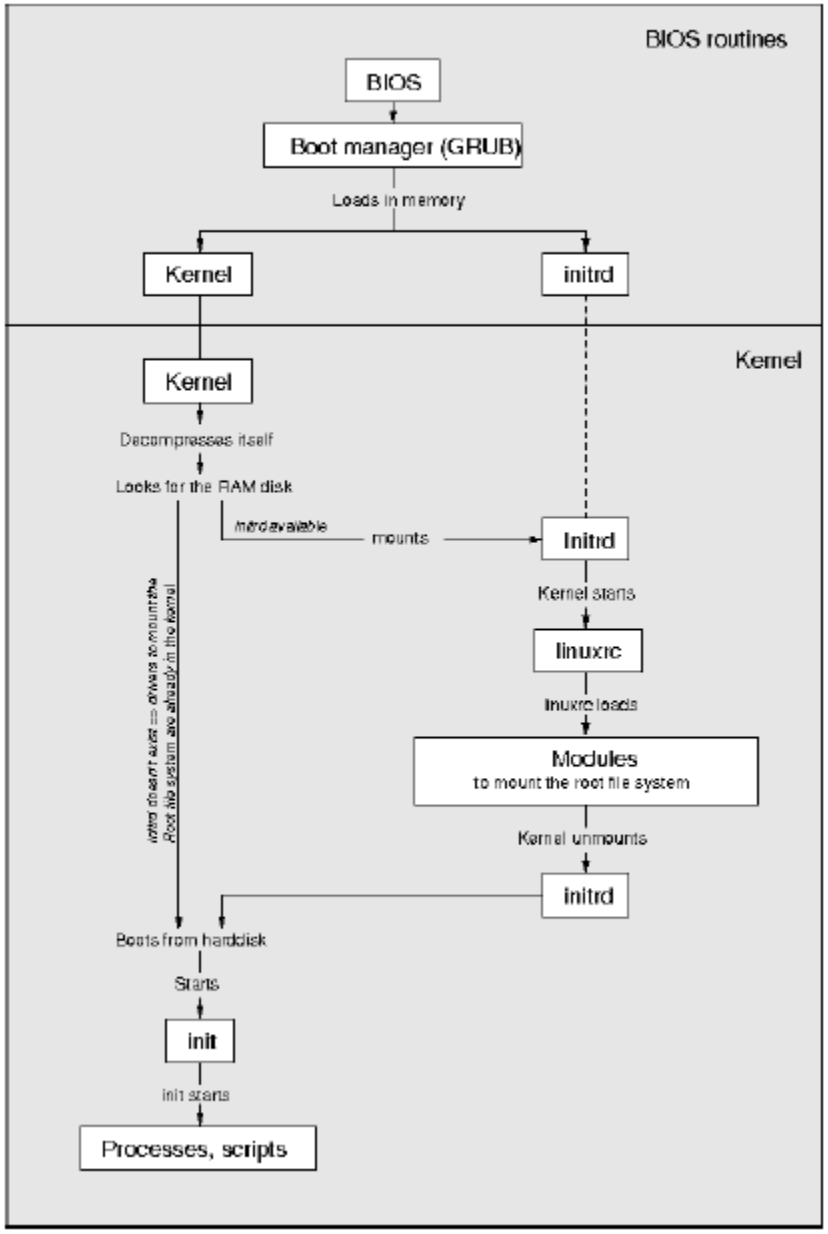
Horváth Gábor K.
vezető konzultáns
Novell PSH

Novell®

A rendszer indulása

A rendszer indulása

- A boot folyamat leírása
  - BIOS és Boot Manager
  - Kernel
  - initramfs
  - init



A GRUB kezelése

- Hogyan működik egy boot manager?
- Boot Managerek a SLE11-ben
  - GRUB
  - Lilo
- GRUB shell indítása
- GRUB konfigurálása
  - parancssor
  - yast2 bootloader
- init=/bin/sh

Futási szintek

- init és a Linux futási szintjei
- /etc/init.d
- futási szint váltása

Processzek és szolgáltatások kezelése

Linux processzek

- jobok és processzek
- processzkezelés
  - parancssori multitasking – előtér, háttér
  - processzek listázása, priorizálása
  - processzek leállítása
  - daemonok működése
  - daemon processzek kezelése

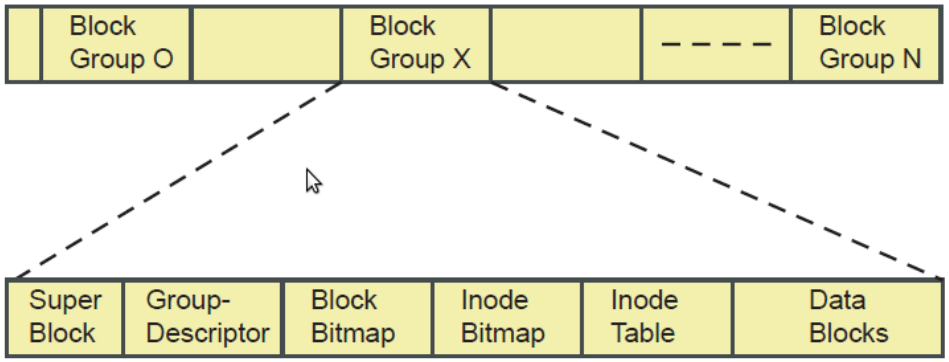
Fájlrendszer adminisztráció

Linux fájlrendszerek

- hagyományos fájlrendszerek
  - ext2
  - MS-DOS/VFAT
  - minix
- naplózó fájlrendszerek
  - ext3
  - reiserFS
  - XFS
  - NTFS
- Naplózás működése

Ext2 belső felépítése

- Szuperblokk
  - szabad és foglalt blokkok száma
  - blokkok száma, és a hozzájuk tartozó inode számok
  - utolsó csatolás ideje, utolsó írás ideje, csatolások száma az utolsó ellenőrzés óta
  - valid bit: 0 csatoláskor, 1 lecsatoláskor
  - több példányban tárolja az FS
- Csoport leíró
  - tartalmazza a többi elem helyét. Ez is többszörösen tárolódik.
- Blokk és inode bitmap
  - szabad/foglalt blokk/inode
- Inode tábla
  - fájl információk jogosultságok, időbélyegek, link az adott fájlhoz tartozó blokkokhoz
- Adatblokkok



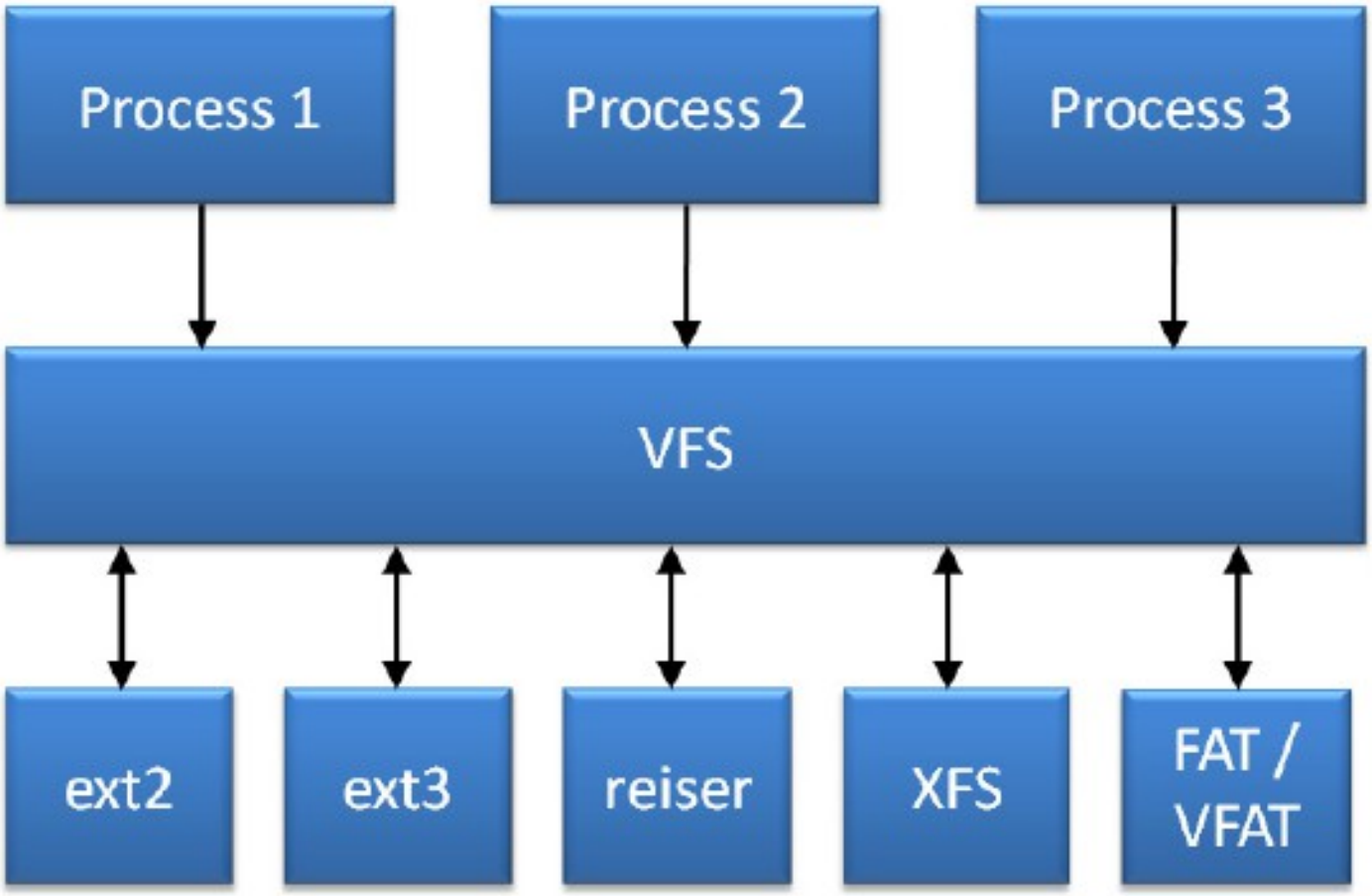
Könyvtárak

- tartalmazza a fájl nevét
- inode számát
- fájl hozzáférés
  - kikeresi a rendszer a szülőkönyvtárat
  - ott megkeresi a fájlbejegyzést
  - kiolvassa az inode-ot
  - ezzel elmegy az inode táblához
  - az inode táblában megleli a hozzá tartozó blokkok listáját, és az egyéb metaadatokat – jogok, időbélyegek, stb.
  - azokat beolvassa

Linkek

- softlink
  - file rendszereken átnyúlhat
  - a célfájl nevét tartalmazza
- hardlink
  - csak egy fájlrendszeren belül értelmezett
  - ez egy új fájlbejegyzés egy könyvtárban
    - növeli az link számot
  - ln paranccsal csak fájlra lehet hard linkelni

VFS: Virtual file system switch

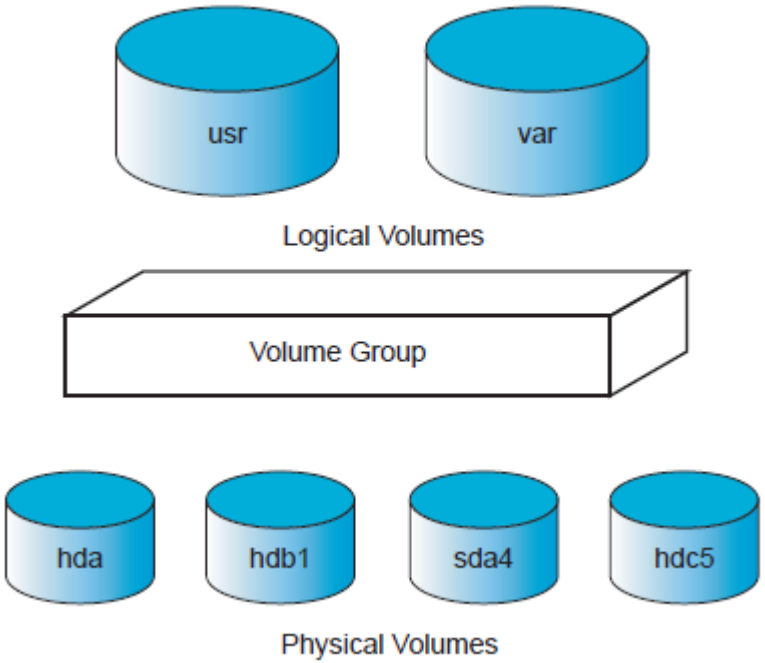


Fájlrendszerek kezelése

- Fájlrendszer létrehozása
  - YaST
  - parancssor
- Fájlrendszer becsatolása
- Fájlrendszerek felügyelete, ellenőrzése

Logikai kötetkezelő

- VM komponensek
- LVM képességek
- LVM konfig YaST-tal
- LVM konfig parancssorból
- szoftveres RAID



Kvótázás

- FS előkészítése – fstab, remount
- kvóta rendszer aktiválása – quotacheck
- kvóta szolgáltatás elindítása – quotaon
- user és group kvóta kezelése
  - edquota
  - soft és hard limitek

Hálózati beállítások

Linux hálózati terminológia

- device
- interface
- link
- address
- broadcast
- route

Hálózati beállítások

- yast2 network

ip parancs használata

- beállítások megjelenítése
  - ip address show
  - ip link show
  - ip -s link show eth0
- beállítások megváltoztatása
  - ip link set eth0 up|down
- beállítások mentése
  - /etc/sysconfig/network/ifcfg-eth0

Routolás beállítása ip paranccsal

- routing tábla kiíratása
  - ip route show
- módosítása
  - lokális háló: ip route add 10.0.0.0/24 dev eth0
  - routeren át: ip route add 10.0.0.0/24 dev eth0 via 10.1.0.1
  - default: ip route add default via 10.0.0.254
- törlés
  - ip route delete 192.168.1.0/24 dev eth0
- fájlba mentés
  - /etc/sysconfig/network/routes
  - 204.127.235.0 0.0.0.0 255.255.255.0 eth0
  - DST GW MASK IF RTYPE
  - man routes

Hálózati kapcsolat tesztelése parancssorból

- ping
- tracert

- Réteghelyes gondolkodás, lentről felfelé hibakeresés

Névfeloldás beállítása

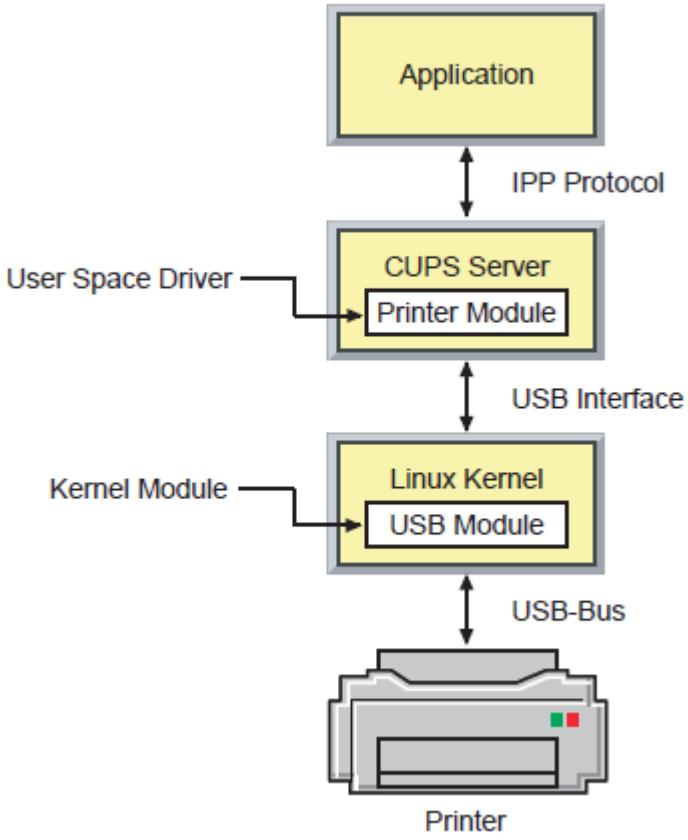
- /etc/HOSTNAME
- /etc/resolv.conf

- nsswitch
  - hosts
  - DNS
  - LDAP
- getent, host/nslookup

Hardver kezelése

Driverek működése

- a különbség device és interface között – eszköz és csatoló/illesztő
- Hogyan működnek a driverek?
- Hogyan töltődnek be?
  - initrd
  - init scriptek
  - udev
  - X szerver
  - kézzel



Kernel modulok kezelése parancssorból

- lsmod, insmod, rmmod, modprobe, depmod, modinfo
- /etc/modprobe.conf
  - install: install eth0 /bin/true
  - alias: alias eth1 bnx2
  - options: options bnx2 disable_msi=1
  - blacklist: blacklist b43
  - man 5 modprobe.conf
- hardver információ kiíratása
  - yast2 hwinfo
  - hwinfo

sysfs

```
# mount | grep sys
sysfs on /sys type sysfs (rw)
# cat /sys/block/sda/queue/scheduler
noop anticipatory deadline [cfq]
# echo deadline > /sys/block/sda/queue/scheduler
# cat /sys/block/sda/queue/scheduler
noop anticipatory [deadline] cfq
# cat /sys/block/sda/device/model
ST9160314AS
```

udev

- eszközfájlok kezelése - /dev
- állandó eszköznevek
- hotplug killer

- uevent
- szabályok
  - eszköz init
  - eszközfájlok, linkek
  - eszközbeállítások módosítása
  - automatikus mountolás
  - kiértesítés

udev

- állandó eszköznevek

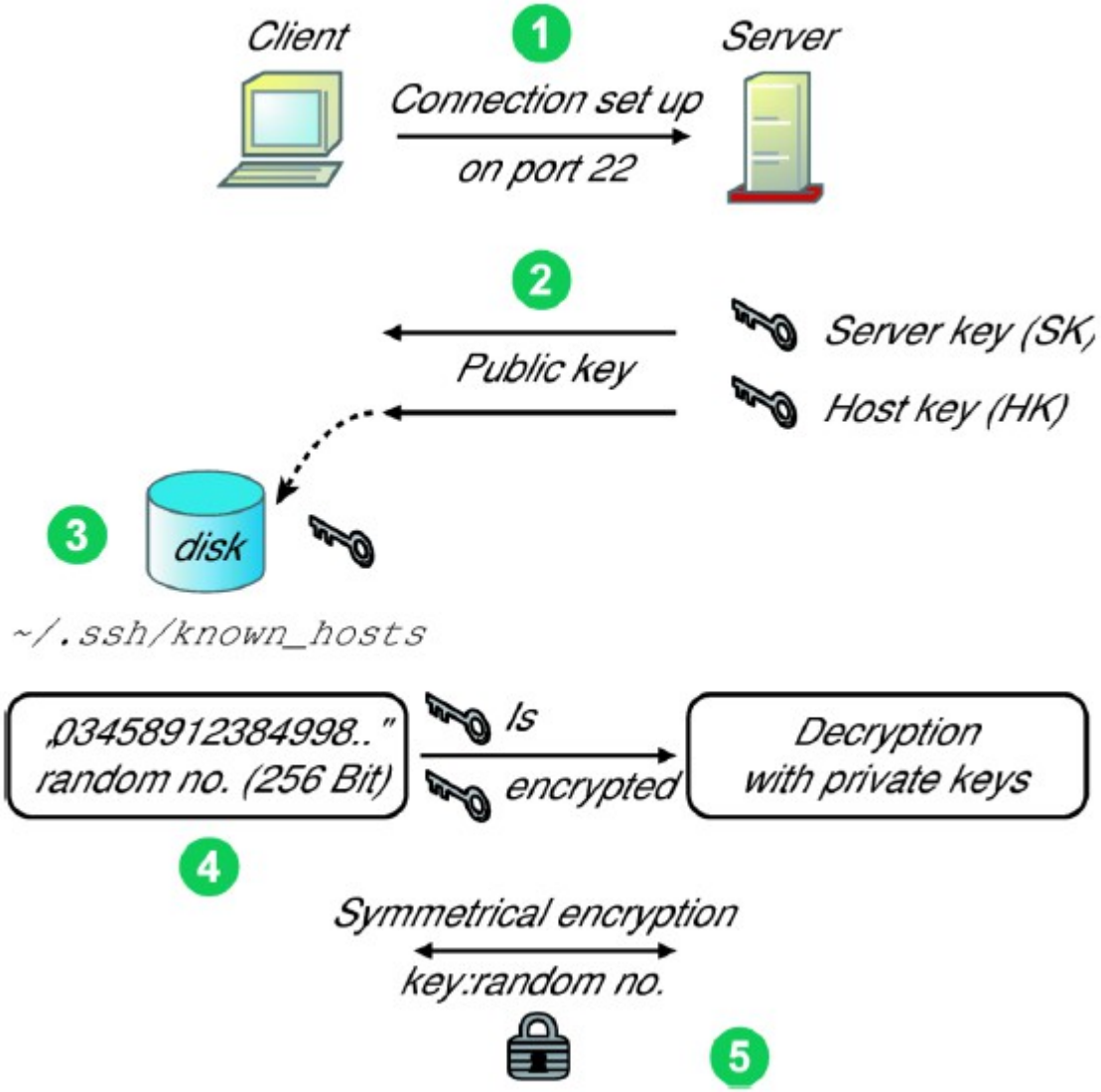
```
# cat /etc/udev/rules.d/70-persistent-net.rules
# PCI device 0x14e4:0x1698 (tg3)
# This file was automatically generated by the /lib/udev/write_net_rules
# program run by the persistent-net-generator.rules rules file.
#
# You can modify it,as long as you keep each rule on a single line.
# PCI device 0x14e4:0x1698 (tg3)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="00:22:19:dc:06:ba", ATTR{type}=="1", KERNEL=="eth*",
NAME="eth0"
```

Távoli hozzáférés

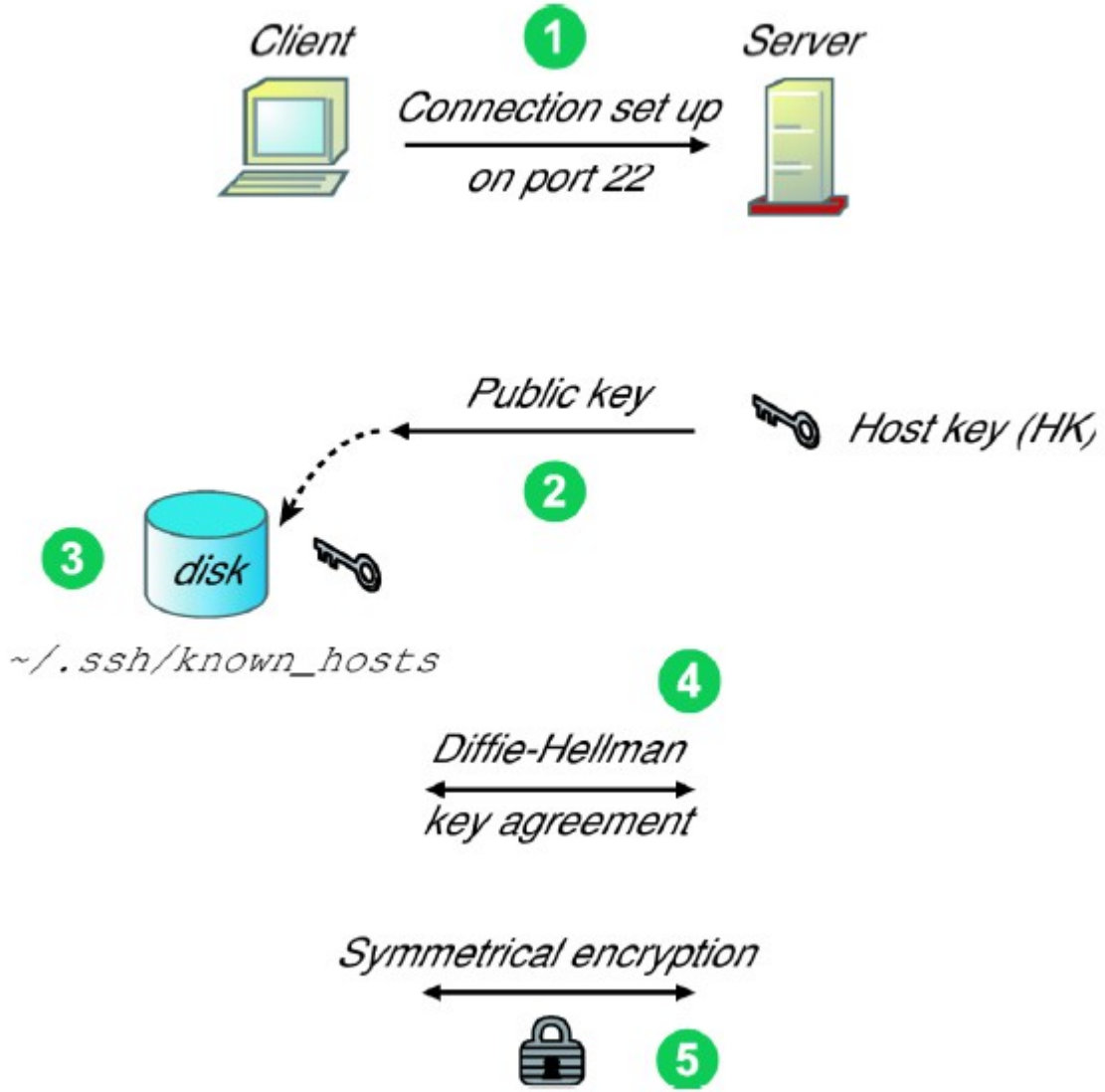
OpenSSH

- kripto alapok
  - szimmetrikus kulcsú
  - aszimmetrikus kulcsú titkosítás
- SSH képességek

OpenSSH v1



OpenSSH v2



OpenSSH

- szerver konfiguráció
  - sshd_config
- kliens konfiguráció
  - ssh_config
- idevágó parancsok
  - ssh, scp, sftp, ssh-keygen, ssh-keyscan, ssh-agent, ssh-add

OpenSSH

- Kulcsos authentikáció
  - ssh-keygen -t (rsa|dsa)
  - pubkey —-->authorized_keys

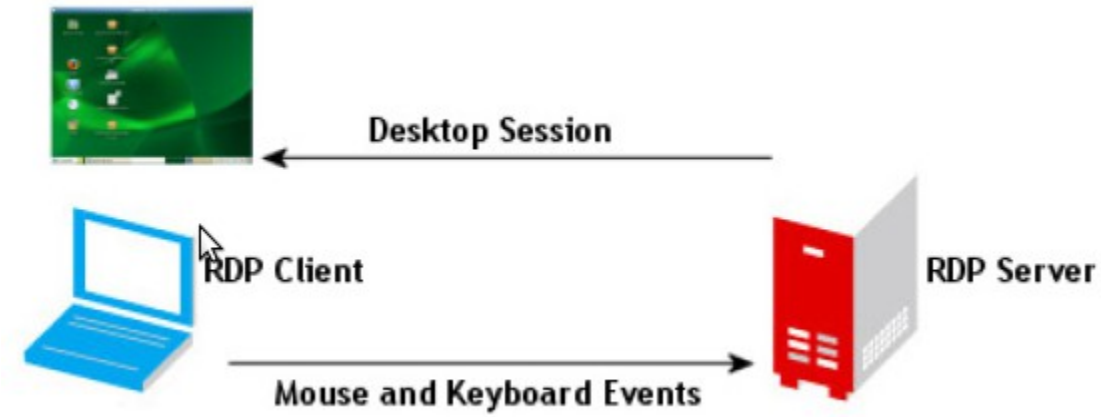
Távoli Adminisztráció VNC-vel

- yast2 remote, rcxdm restart
- https://HOST:5801
- vncviewer HOST:1

Távoli elérés NOMAD RDP-vel

- tömörítés
- titkosítás
- hang
- nyomtatás
- vágólap

- windows kliens
- linux kliens
- teljes keresztműködés



NOMAD telepítése

- zypper install xrdp xorg-x11-server-dmx xorg-x11-server-rdp
- chkconfig xrdp on
- rcxrdp start
- tűzfal TCP 3389
- rdesktop HOST
- tsclient

SLES felügyelete

SLES felügyelete

- dmesg, /var/log/boot.msg, yast2 view_anymsg
- /proc
- hwinfo, hdparm, fdisk, iostat, lspci, siga, sitar
- uptime, netstat, uname, xosview
- sysstat, ksar*
- df, du, Gnome System Monitor

syslog-ng

- /etc/syslog-ng.conf
- /etc/sysconfig/syslog

- /var/log/messages
- Séta a /var/log -ban

Logrotáció

- /etc/logrotate.conf
- /etc/logrotate.d

Felhasználói aktivitás

- who
- w
- finger (plan)
- last -ax
- lastlog
- faillog (pam_tally.so)

Feladatok automatizálása

cron

- crontab formátum
- /etc/crontab
  - /etc/cron.(hourly|daily|weekly|monthly)
- crontab -e
- crontab -l
- crontab -u USER
- /etc/cron.allow
- /etc/cron.deny

at

- at
- at -l
- atrm
- /etc/at.allow
- /etc/at.deny

Mentés és visszaállítás

Mentési stratégia

- módszer
  - teljes
  - inkrementális
  - differenciális
- média
  - szalag
  - hálózati meghajtó
  - helyi diszk
- ütemezés
- célállományok

Mentés a YaST segítségével

- RENDSZER mentés
  - csomagokból a módosított fájlok
  - Kritikus rendszerterületek
  - konfiguráció
- yast2 backup
- yast2 restore

tar

- tape archiver :-D
  - tar c(z|j)f out.tar(.gz|.bz2) directory
  - tar cf /dev/st0 directory
  - tar cf /dev/st0 -X excludefile directory
- kipakolás
  - tar xfv /dev/nst0
  - tar xfvz backup.tar.gz
  - tar xfvz backup.tar.gz -C restoredir

tar

- Inkrementális mentés

Full mentés:

```
# tar -cz -g /backup/snapshot.lst -f /backup/backup.tar.gz /home
```

Inkrementális mentés:

```
# tar -cz -g /backup/snapshot.lst -f /backup/backup.1.tar.gz /home
```

- Differenciális mentés

```
# tar czf /backup/backup.tgz /home
# find /home -type f -newer /backup/backup.tgz -print0 \
| tar --null cfz /backup/backup_mon.tgz  -T -
```

- man tar

Mágnesszalagok kezelése

- /dev/nst0
- mt parancs
  - mt -f DEV status
  - mt -f DEV fsf 1
  - mt -f DEV bsf 1
  - mt -f DEV rewind
  - mt -f DEV offline
  - mt -f DEV datcompression

Mágnesszalagok kezelése

```
# mt -f /dev/st0 status
drive type = Generic SCSI-2 tape drive
status = 620756992
sense key error = 0
residue count = 0
file number = 0
block number = 0
Tape block size 0 bytes. Density code 0x25 (unknown). Soft error
count since last status=0 General status bits on (41010000):
   BOT ONLINE IM_REP_EN
# mt -f /dev/st0 fsf 1
# mt -f /dev/st0 status
drive type = Generic SCSI-2 tape drive
status = 620756992
sense key error = 0
residue count = 0
file number = 1
block number = 0
Tape block size 0 bytes.
Density code 0x25 (unknown).
Soft error count since last status=0 General status bits on
(81010000):
   EOF ONLINE IM_REP_EN
```

dd

Killer App

```
# dd if=/dev/zero of=/dev/sda
```

```
# dd if=/dev/sda of=mbr_copy count=1
```

```
# ssh -C -l root masikgep dd if=/dev/datavg/lvm_snapshot \
| gzip > mysqldata_image.gz
```

rsync

- lokális üzem

```
# rsync -a --progress -v --stats /home/gjakab /srv/backup/home/gjakab

# rsync -a --progress -v --stats /home/gjakab/ /srv/backup/home/gjakab
```

- távoli üzem

```
# rsync -a root@masikgep:/opt/novell /backup/masikgep/
```

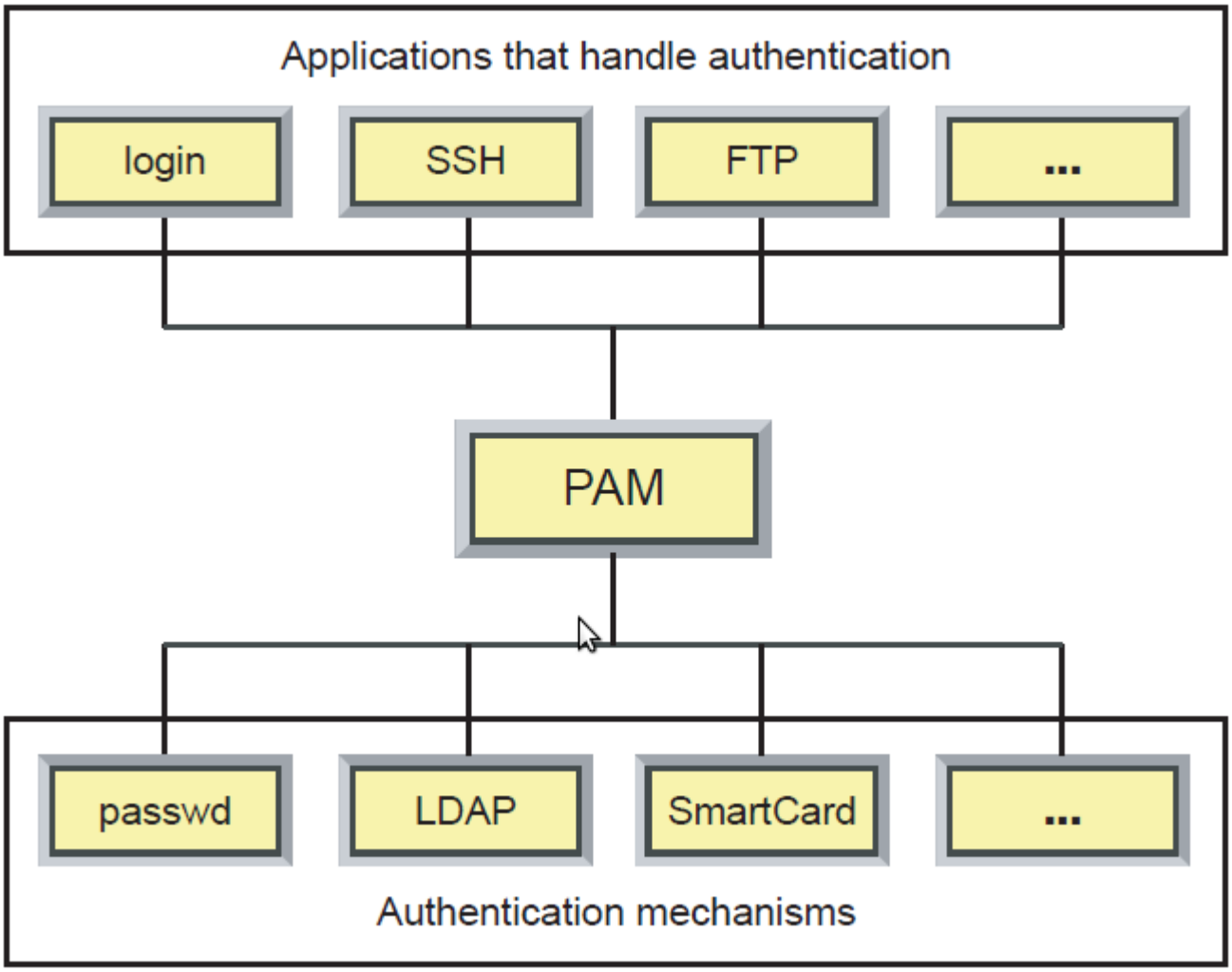
Backup automatizálás cronnal

- megírjuk a scriptet
- berakjuk a cronba
  - user cronba → crontab -e
  - rendszer cronba
    - /etc/cron.daily

Rendszerbiztonság

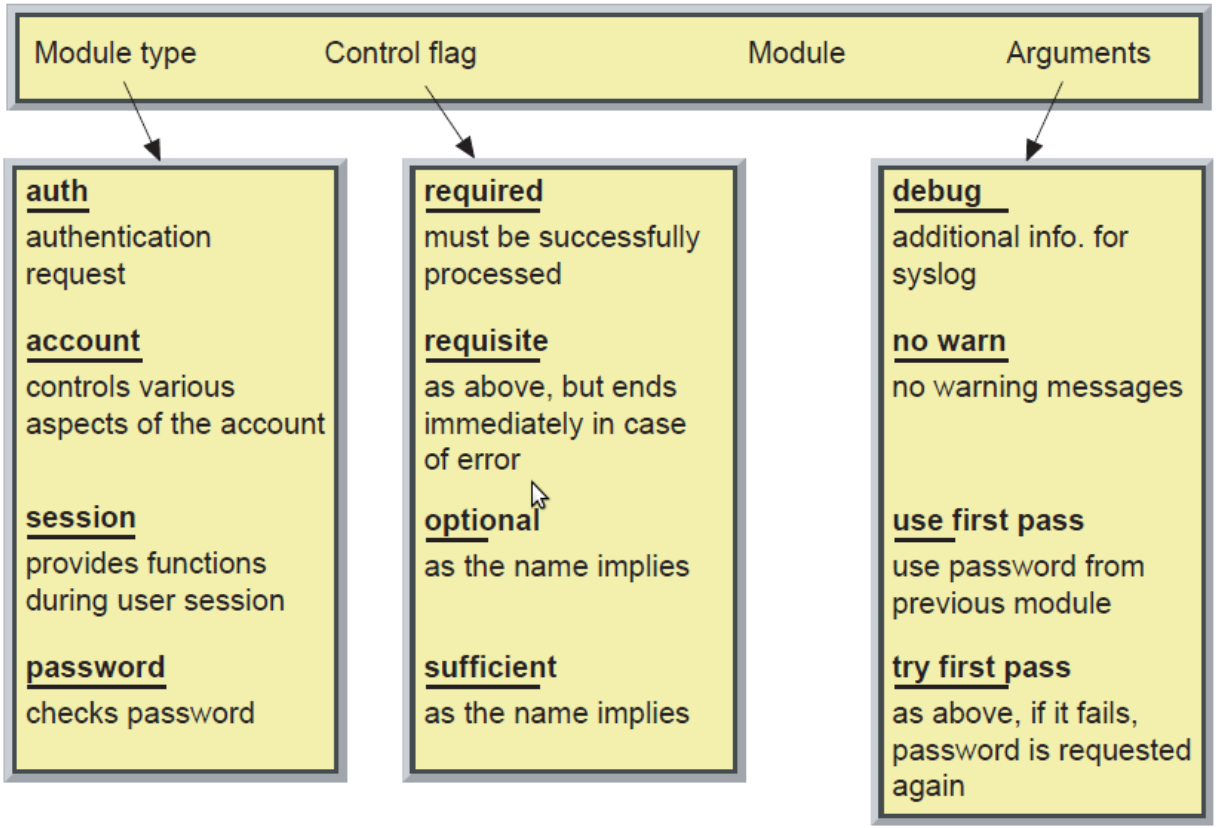
PAM

PAM



PAM

- /etc/security
- /etc/pam.d
  - /etc/pam.d/appname



PAM konfig példa

```
> cat /etc/pam.d/login
#%PAM-1.0
auth       requisite pam_nologin.so
auth       [user_unknown=ignore success=ok ignore=ignore auth_err=die default=bad]
           pam_securetty.so
auth       include   common-auth
account    include   common-account
password   include   common-password
session    required  pam_loginuid.so
session    include   common-session
session    required  pam_lastlog.so      nowtmp
session    optional  pam_mail.so standard
session    optional  pam_ck_connector.so
```

```
auth   required        pam_env.so
auth   optional        pam_gnome_keyring.so
auth   required        pam_unix2.so
```

PAM

- biztonságos jelszóválasztás kikényszerítése
  - pam_pwcheck.so, cracklib
- /usr/share/doc/packages/pam
- Linux-PAM Administrator's Guide
- man oldalak – egyes modulokhoz

Felhasználói környezet

Felhasználói környezet kezelése

- su
- newgrp
- gnomesu

Feladatok delegálása

- sudo
- visudo
- /etc/sudoers
- yast2 sudo

Alapértelmezett beállítások

- yast2 users
- /etc/defaults/useradd
- useradd --show-defaults
- useradd --save-defaults

Rendszerbiztonság felülvizsgálata

Rendszerbiztonsági segédlet

- yast2 security

Access Control List

ACL

- Hagyományos ugo/rwx jogok
  - chmod
  - chown
  - chgrp
- ACL
  - getfacl
  - setfacl

Terminológia

- user class
  - tulaj
  - tulajdonos csoport
  - mások
- Access ACL
- Default ACL – öröklődés, csak könyvtárakra értelmezett
- ACL entry
  - type, qualifier, permissions

ACL típusok

- Minimum ACL
  - ugo/rwx
- Extended ACL
  - nevezett felhasználó
  - nevezett csoport
  - maszk

ACL

```
gahorvath@npsh-gahorvath:~> touch test
gahorvath@npsh-gahorvath:~> getfacl test
# file: test
# owner: gahorvath
# group: users
user::rw-
group::---
other::---
gahorvath@npsh-gahorvath:~> setfacl -m user:oscar:r test
gahorvath@npsh-gahorvath:~> getfacl test
# file: test
# owner: gahorvath
# group: users
user::rw-
user:oscar:r--
group::---
mask::r--
other::---
```

ACL-ek kiértékelése

- sorrend
  - owner
  - named user
  - owning group
  - named group
  - others
- jogok nem adódnak össze
- a legjobban illeszkedő szabály érvényesül
- ha több van, random választja ki melyiket használja

ACL-ek és alkalmazások

- részleges a támogatás
- star, fileutils
- grafikus fájlkezelők nem ismerik az ACL-eket

Csomagszűrő tűzfal YaST segítségével

Csomagszűrés

- Hogyan működik
  - klasszikusan állapotmentes
  - manapság állapotőrző
- SuSEFirewall2
  - yast2 firewall
  - /etc/sysconfig/SuSEfirewall2.d/
  - /etc/sysconfig/SuSEfirewall2
  - /etc/sysconfig/scripts/SuSEfirewall2-custom
- iptables


Novell®