AXXES IT CONSULTANCY

AXXES IT CONSULTANCY

Linux

The Essentials

Who am I

- Sander Descamps
- Fednot as Linux engineer (8 months)
- Dataplan as Cloud engineer
- West-Vlaanderen

Goal of today

- Introduction
- Focus on useful stuff
- Slides with red corner are informational

Index

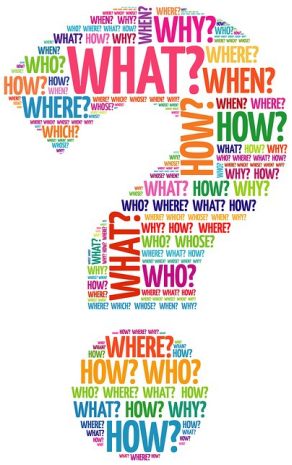
AXXES IT CONSULTANCY

Linux General

Question

1)How do you know Linux?

2)Did you used Linux before?



What is Linux?

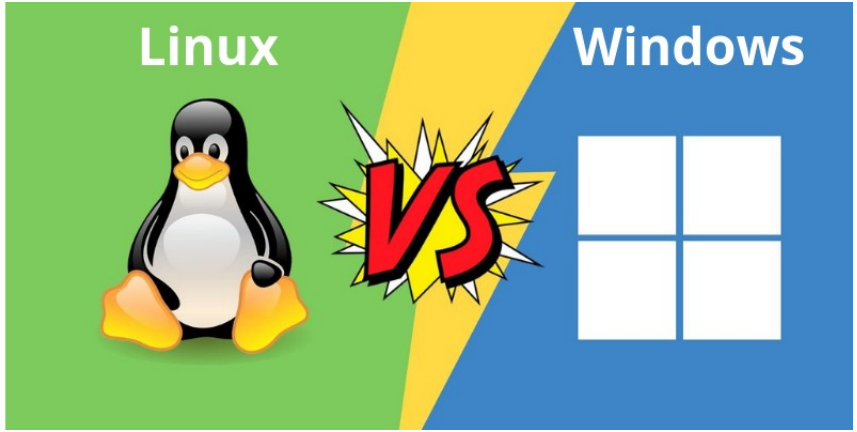
- Kernel, not an OS
- Layer between hardware and software
- Open-source
- Linus Torvalds

Linux philosophy:

1. Small is Beautiful
2. Each Program Does One Thing Well
3. Prototype as Soon as Possible
4. Choose Portability Over Efficiency
5. Store Data in Flat Text Files
6. Use Software Leverage
7. Use Shell Scripts to Increase Leverage and Portability
8. Avoid Captive User Interfaces
9. Make Every Program a Filter

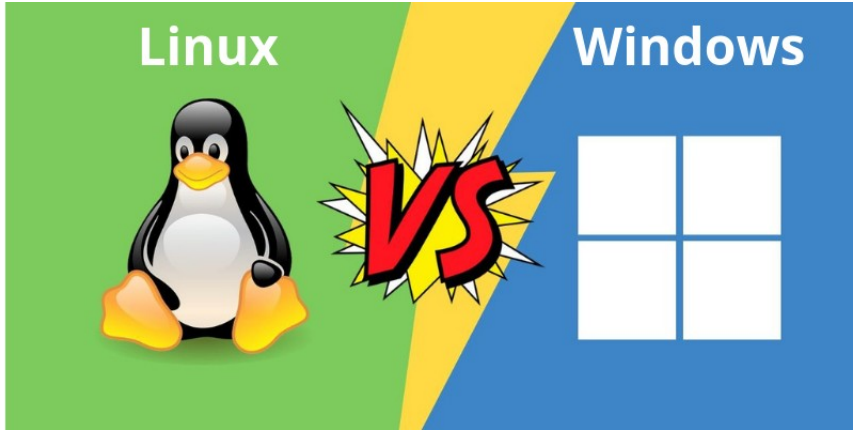
Why use Linux

- Cost
- Reliability
- Security
- Less resources
- Less complex
- Easy automation
- Open-source
- Easy update



Why not use Linux

- Knowledge
- Drivers (not always available)
- Advanced user management
- Software (Office, Photoshop..)
- Windows only environment



Distribution

- Linux + Some important stuff + Packet manager + Custom sauce = distribution
- +250 distributions, 3 to remember
  - Ubuntu (Debian)
  - CentOS, RedHat
  - Suse, SLES

Ubuntu

- Canonical
- Ubuntu 19.04
- Support for 5+5* years for LTS
- Early adopter
- Large community
- Free (subscription is a joke)

Red Hat

- Red Hat, Inc. (Acquired by IBM)
- Red Hat 8
- Support for 10+x years
- Stability first
- Satelite, Ceph, GlusterFS, Ansible,…
- Expensive (especially with tools)

Suse

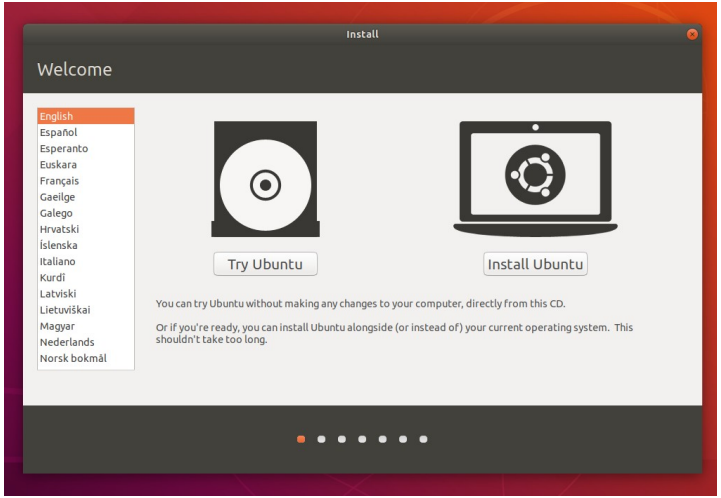
- Suse (EQT Partner)
- SUSE Linux Enterprise Server 15
- Support for 10+3 years
- German quality
- Can be expensive

Desktop environment

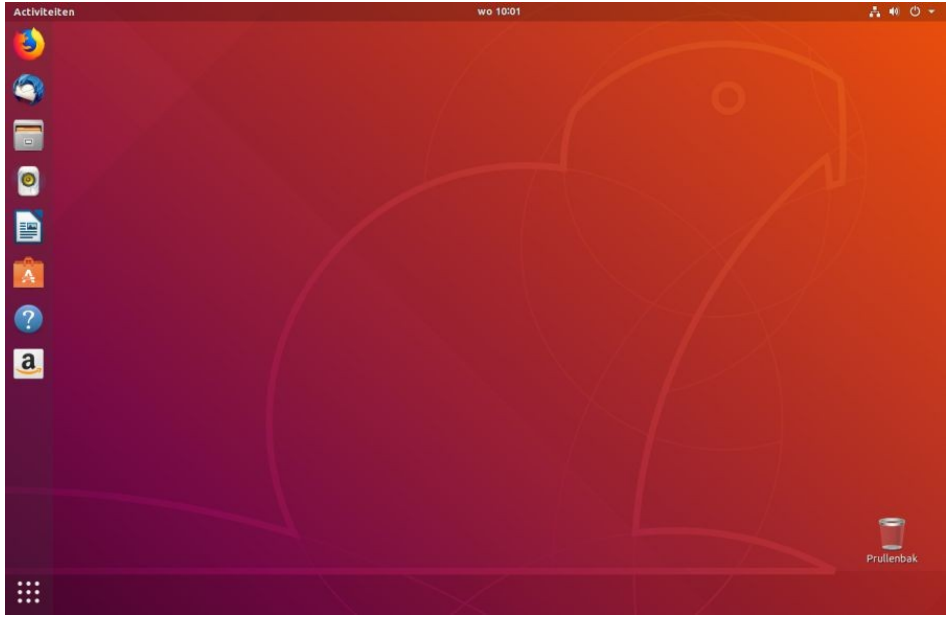
- GNOME
- KDE
- Mate
- Cinnamon
- LXDE
- Xfce

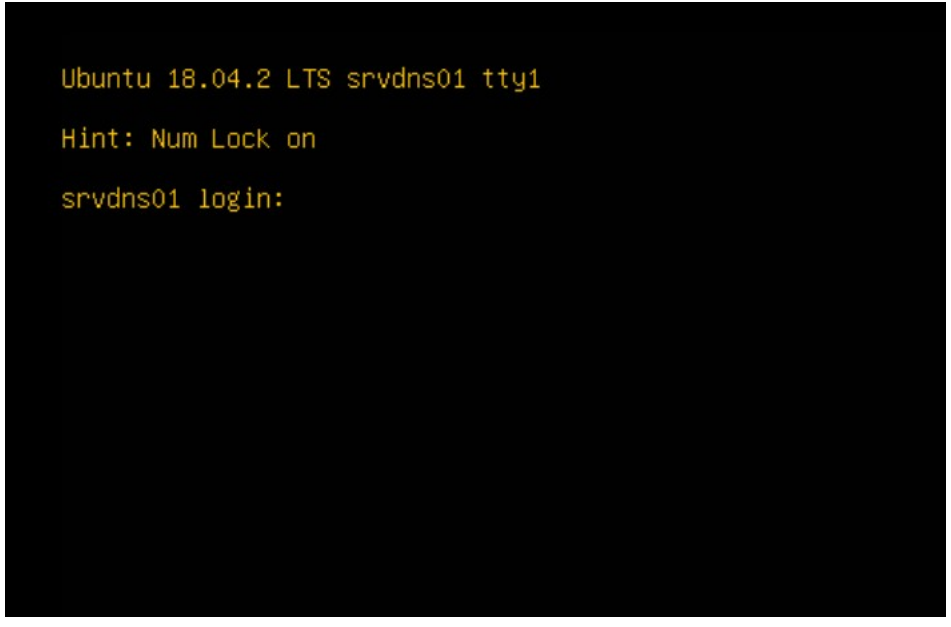
Install Linux

1. Download ISO
2. Make bootable usb (rufus, unetbootin,...)
3. Boot from usb
4. Follow installation wizard
5. Done



Ready to go


Activiteiten
wo 10:01
Prullenbak


Ubuntu 18.04.2 LTS srvdns01 tty1
Hint: Num Lock on
srvdns01 login:

Basic commands

Machine info

```
## Check current kernel
uname -a

## Check distribution information
cat /etc/*release

## Clear console
clear

## command history
history
```

File manipulation

• List files	ls, ls -alh
• Change directory	cd
• Present work directory	pwd
• Concatenate files	cat <file1> <file2>
• Type of file	type file.txt

File manipulation

- Copy file — cp <src> <dst>
- Move/rename file — mv <src> <dst>
- Create new file — touch <dst>
- Create directory — mkdir <dst>

View file

- Print file to console cat <file>
- Scrolable viewer less <file>
- ~~Scrolable viewer~~ ~~more <file>~~
- Pipe large output command | less
- Top of file head <file>
- Bottom of file tail <file>

Search – replace – extract

- Search on content — grep <item> file.txt
- Pipe search — cat f.txt | grep <item>
- Find file — find / -iname “file1”

Operations

• Word count	wc <file>
• Line count	wc -l <file>
• Print text to console	echo some-text
• Sort lines	sort <file>
• Unique lines	uniq <file>

stdin, stdout and stderr

- Write stdout to file — `command > out.txt`
- Append stdout to file — `command >> out.txt`
- Pipe stdout to stdin — `command | grep item`
- Redirect stderr to stdout — `command 2>&1`
- Write stderr to file — `command 2> error.txt`
- Display and save to file — `command | tee out.txt`

Edit file

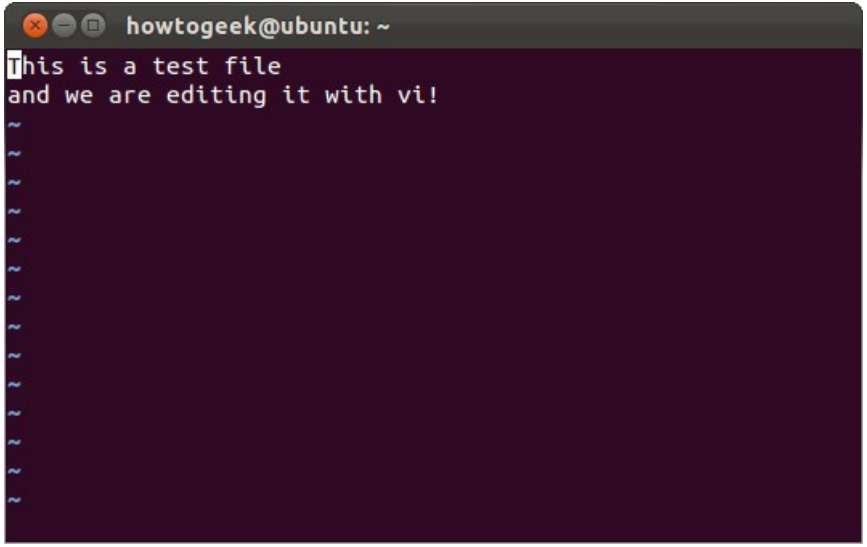
- Nano
- Vi (vim)
- Emacs
- Atom
- ...

Nano

```
bob@ubuntu: ~
  GNU nano 2.2.6              File: textfile.txt

"Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempo$

"Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempo$

"Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempo$

"Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempo$

                              [ Read 7 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

Vi

- Command mode (at start, esc)
  - Delete line → dd
  - Copy line → yy
  - Past underneth → p
  - Enter insert mode → i (o,a)
- Ex mode (after ':')
  - Save → :w
  - Quit → :q
- Insert mode



Remote management

SSH

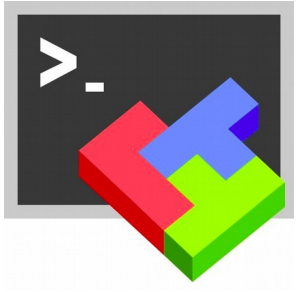
- Secure Shell
- Password or keypair
- Remote console
- tcp port 22
- Forward other ports

SSH

```
# Configure SSH keypair
## ssh client
ssh-keygen -t rsa
Enter file in which to save the key (/home/user/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
# /home/user/.ssh/id_rsa.pub        → public key
# /home/user/.ssh/id_rsa        → private key (never share!!!)

## ssh server
echo “public key” >> /home/user/.ssh/authorized_keys
```

SSH clients

- Putty
- MobaXterm
- ssh user@server.com

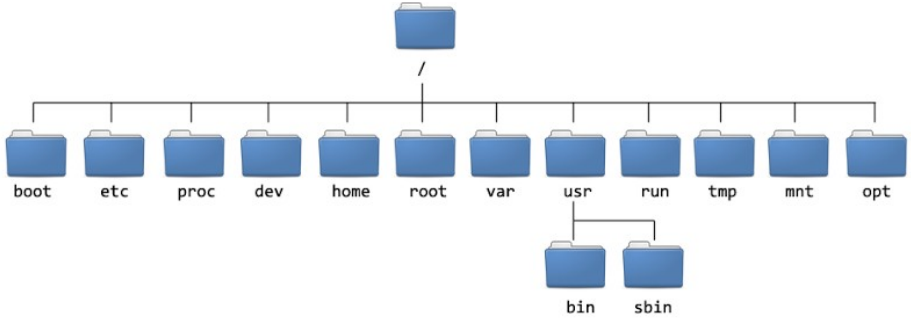


Lab

Storage and file system

FHS

- File-system Hierarchy Standard
- Directory structure
- Everything is a file
- Everything under ‘/’



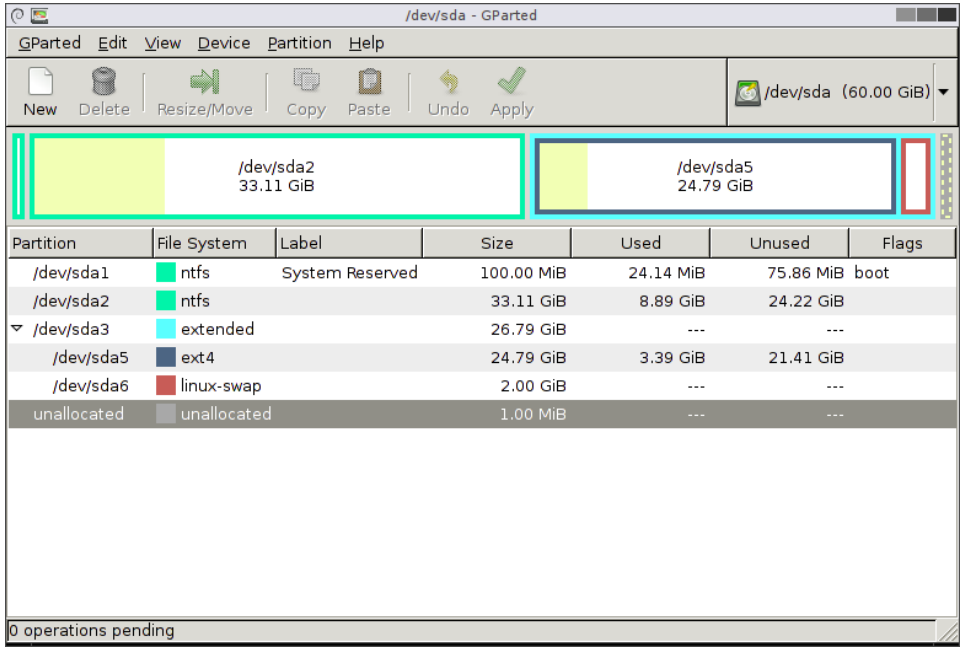
FHS

Path	Description
/	Root of file system
/bin /sbin	Binaries,
/boot	static files of boot loader
/dev	Device files (/dev/sda1, /dev/sr0)
/sys, /proc	System memory*
/etc	Host specific config
/usr	Sharable and read-only data

Path	Description
/opt	Addon application software
/tmp	Temporary data
/mnt	Mount for temporary filesystems
/mount	Long term mounts
/root	Home directory root user
/home	User home directories
/var	Variable data files (/var/www, /var/log,..)

Disks and partitions

- Disk → /dev/sda, /dev/sdb
- Partition → /dev/sda, /dev/sda1



Disks and partitions

```
## List disks
lsblk

## List disk-ID’s
blkid

## List filesystems
df
df -h       # Human readable
df -l       # local filesystems only

## Graphical tool
gparted
```

Disks and partitions

- Create partition

```
fdisk /dev/sda
#   m - print help
#   p - print the partition table
#   n - create a new partition
#   p - delete a partition
#   q - quit without saving changes
#   w - write the new partition table and exit
```

Partition format

- fat32
- ext2, ext3, ext4
- xfs
- btrfs
- zfs
- swap

Partition format

- Create partition

```
mkfs.ext4 /dev/sda1
mkfs -t xfs /dev/sdb5
mkfs.xfs /dev/sda
mkfs.ext4 -b 4096 /dev/sdc1
mkfs.fat /dev/
```

- Create swap partition

```
mkswap /dev/sdb
swapon /dev/sdb
swapoff /dev/sdb
```

Mount

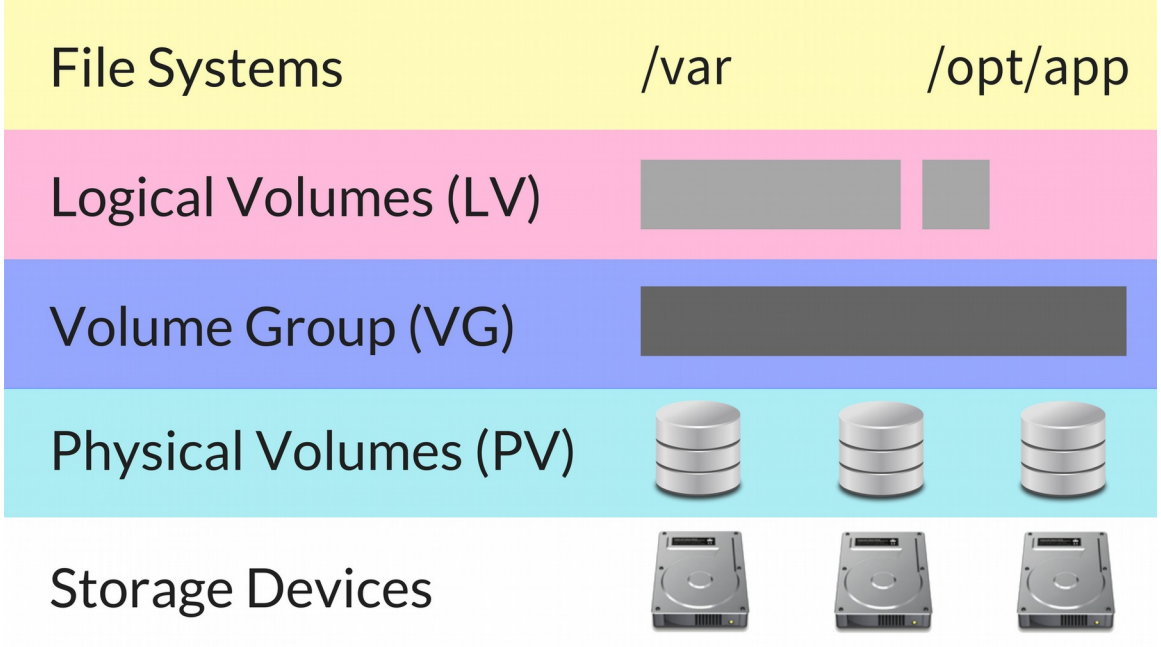
- Mount partition on folder
- /etc/fstab
  - ➔ [File System] [Mount Point] [File System Type] [Options] [Dump] [Pass]

Mount

```
mount /path/to/partition /path/to/mountpoint -t <type>
mount /dev/sda /mnt/tempdir
mount /dev/mapper/sys-var /var
mount /home/user1/dvd.iso /dev/mnt/dvd
```

LVM

- Logical volume management



LVM

```
# create a physical volume
pvcreate /dev/sda

# create a volume group
vgcreate sys /dev/sda

# add physical volume to volume group
vgextend sys /dev/sdb

# create logical volume
lvcreate -L 2G var sys

# extend logical volume and filesystem
lvextend -rL +1G /dev/mapper/sys-var
```

Extend iscsi disk (VMware)

```
### list scsi adapters
ls /sys/class/scsi_device/

### rescan scsi bus (modify the channel)
for i in $(ls /sys/class/scsi_device/); do echo 1 >
/sys/class/scsi_device/$i/device/rescan; echo "Rescan scsi_device
$i";done

### list scsi hosts
ls /sys/class/scsi_host/

### update all iscsi volumes
for i in $(ls /sys/class/scsi_host/); do echo "- - -" >
/sys/class/scsi_host/$i/scan; echo "rescan $i"; done
```

Users and Permissions

Users

- Unique identifier UID
- Users-file → /etc/passwd
- Password-file → /etc/shadow (…,SHA-512)

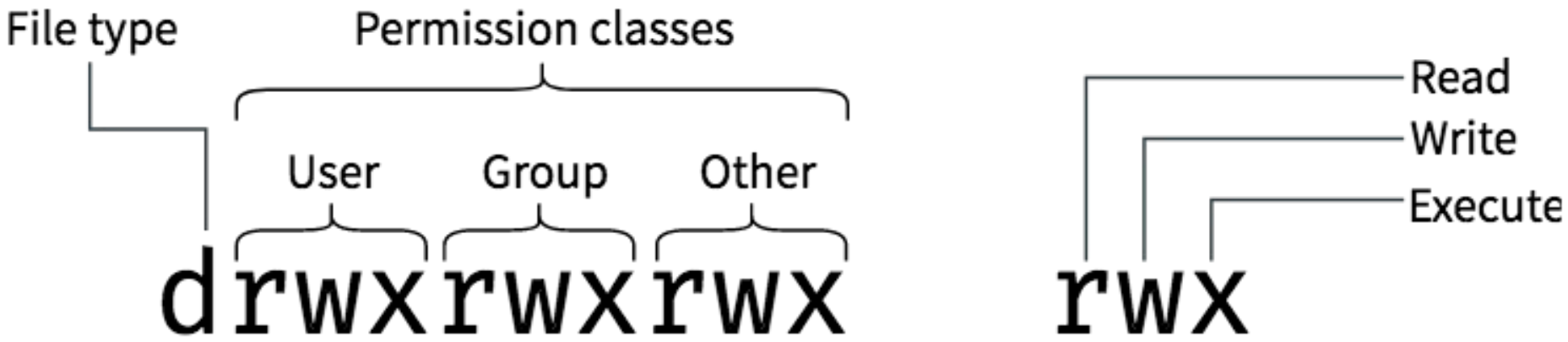
Groups

- Group file → /etc/group
- Unique identifier GID

Users and groups

```
## Add user
useradd bob
useradd -u 521 -m -g users -G print,fileshare bob

## Add group
addgroup users
addgroup --gid 124 users

## Delete user/group
userdel bob
groupdel users

## Reset passwoord
passwd          #current user
passwd bob      #reset password Bob
```

File permissions



File permissions

Mode | Owner | Group | File Size | Last Modified | Filename

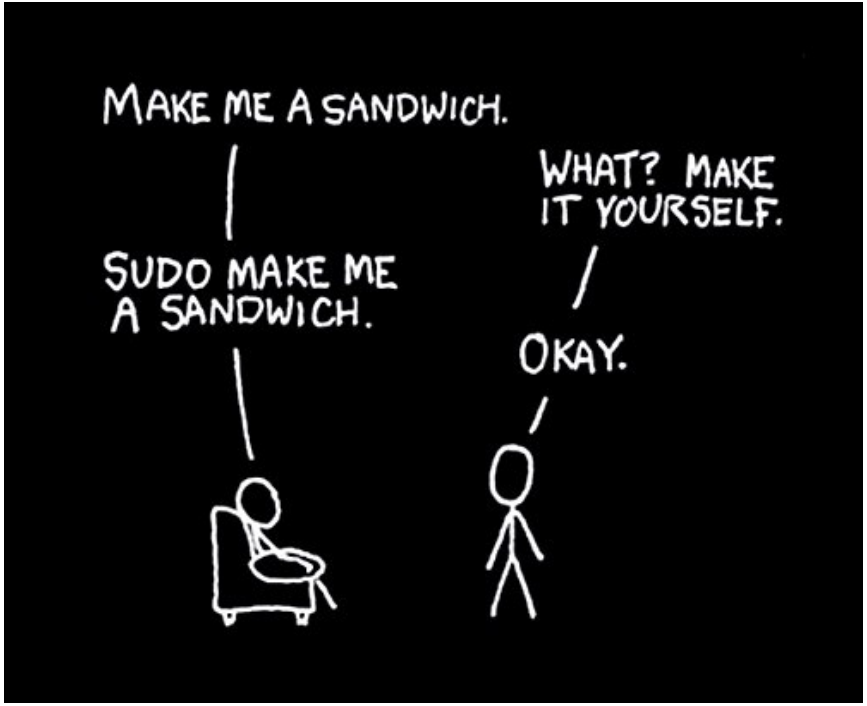
```
drwxrwxrwx 2 sammy sammy       4096 Nov 10 12:15 everyone_directory
drwxrwx--- 2 root  developers  4096 Nov 10 12:15 group_directory
-rw-rw---- 1 sammy sammy         15 Nov 10 17:07 group_modifiable
drwx------ 2 sammy sammy       4096 Nov 10 12:15 private_directory
-rw------- 1 sammy sammy        269 Nov 10 16:57 private_file
-rwxr-xr-x 1 sammy sammy      46357 Nov 10 17:07 public_executable
-rw-rw-rw- 1 sammy sammy       2697 Nov 10 17:06 public_file
drwxr-xr-x 2 sammy sammy       4096 Nov 10 16:49 publicly_accessible_directory
-rw-r--r-- 1 sammy sammy       7718 Nov 10 16:58 publicly_readable_file
drwx------ 2 root  root        4096 Nov 10 17:05 root_private_directory
```

File permissions

```
## Change owner
chown bob ./file.txt
chown alice:users /opt/file
chown bob:bob -R /home/bob

## Change group
chgrp bob file.txt

## Change permissions
chmod 400 /home/bob/key
chmod u=rwx,g=r -R ~/
chmod ug+x,o-x public.txt

## List folder with permissions and hidden files
ls -la
```

Sudo

- Super User Do
- /etc/sudoers
- /etc/sudoers.d/*
- visudo



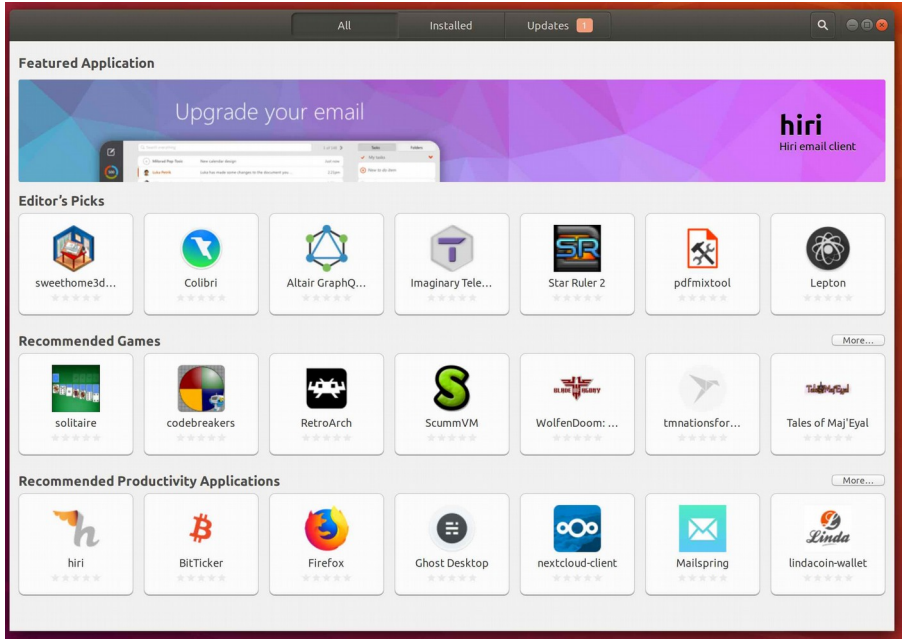
/etc/sudoers

```
## Allow root user to run any commands anywhere
root    ALL=(ALL)       ALL

## Allows people in group wheel to run all commands without a password
%wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to shutdown this system
%users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
```

Package manager

Package manager

- Ubuntu
  - Apt-get
  - Apt
  - Aptitude
- CentOS, Redhat
  - Yum
- Suse, opensuse
  - Zypper
  - yast, yast2



apt (Ubuntu)

```
apt update                    # update local repo cache
apt upgrade                   # update all packages
apt-get install htop          # install htop (old methode)
apt install htop              # install htop
apt remove htop               # remove htop
apt search <search term>      # search for package
apt info htop                 # get info about specific package
```

htop is an interactive process viewer for Unix systems.

yum (CentOS)

```
yum update                    # update cache and update packages
yum install sshd              # install sshd
yum remove sshd               # remove sshd
yum search <search term>      # search for package
yum info sshd                 # get info about specific package
```

zypper (SuSE)

```
zypper refresh              # refresh repositories
zypper update               # update cache and update packages
zypper install sshd         # install sshd
zypper remove sshd          # remove sshd
```

AXXES IT CONSULTANCY

(Remote) file operations

SCP

- Secure copy
- Copy data between machines

```
## copy to remote server
scp foo.txt username@remotehost.edu:~
scp foo.txt username@remotehost.edu:/home/username/
scp -r folder username@remotehost.edu:/some/remote/directory

# copy from remote host
scp username@remotehost.edu:foobar.txt /some/local/directory
scp username@rh1.edu:/remote/foobar.txt \username@rh2.edu:/remote/
```

SCP clients

- WinSCP
- Filezilla

rsync

- Syncing data
- Delta transfer algorithm

```
## Basic syntax
rsync options source destination
    -v, –verbose     Verbose output
    -q, –quiet       suppress message output
    -a, –archive     archive files and directory while synchronizing ( -a equal to -rlptgoD)
    -r, –recursive   sync files and directories recursively
    -b, –backup      take the backup during synchronization
    -u, –update      don’t copy the files if destination files are newer
    -l, –links       copy symlinks as symlinks during the sync
    -n, –dry-run     perform a trial run without synchronization
    -z, –compress    compress file data during the transfer
    -h, –human-readable  display the output numbers in a human-readable format
    –progress        show the sync progress during transfer
```

File compression

- tar
- gzip vs bzip2
- .zip

File compression

```
## Create tar archive
tar -cvf archive.tar /folder1 /folder2

## Extract tar archive
tar -xvf archive.tar

## Compress a folder(s)/file(s)
gzip archive.tar
tar -cvzf archive.tar.gz /home/user
tar -cvjf archive.tar.bz2 1.mp4 2.mp4

## Uncompress a archive
tar -xvf thumbnails.tar.gz
tar -xvf videos.tar.bz2
```

Hard an Soft links

- Hard link
  - pointer to a file
  - only inside partition
- Soft link (symbolic link, symlink)
  - file with path to another file
  - across multiple partitions
  - similar to shortcuts in Windows

Service, process and jobs

Service Manager (init)

- First service that boots (pid 1)
- Manages start/stop of other services
- Multiple implementations
  - SystemV init
  - Upstart
  - SystemD
  - ...

SysV vs SystemD

SystemV init

- Older
- Runlevels (0-6)
- Sequential boot

SystemD

- Newer
- Targets
- Dependency based

SysV

- /etc/init.d → startup services
- /etc/rcX.d → organized per runlevel
  → symlink to service in /etc/init.d
- /etc/rc5.d/S01rsyslog → runlevel 5, Start, order 1

SystemD

- /etc/systemd/system — Local configuration
- /run/systemd/system — Runtime units
- /usr/lib/systemd/system — Units of installed packages (CentOS)
- /lib/systemd/system — Units of installed packages (ubuntu)
- man systemd.service
- man systemd.unit

Services

- Services are defined in service manager
- Intended to start automatically
- Every service will start one or more processes
- Runs in the background

Process

- The instance of a computer program that is being executed by one or many threads.
- Defined by
  - State (runnig, waiting…)
  - Process ID (pid)
- Init is parent of every process
- ps -ef, top, htop

Jobs

- Command started at specific time/date
- Cron-job
- Background job / foreground job

```
sleep 1000 &          # run job in background
jobs                  # list all jobs in current terminal
fg %1                 # move job 1 to foreground
bg %2                 # move job 2 to background
Ctrl+z                # Stop foreground job and places it in
                        the background as a stopped job
```

Cron Job

- /etc/crontab

```
# ┌─────────────── minute (0 - 59)
# │ ┌─────────────── hour (0 - 23)
# │ │ ┌─────────────── day of the month (1 - 31)
# │ │ │ ┌─────────────── month (1 - 12)
# │ │ │ │ ┌─────────────── day of the week (0 - 6) (Sunday is 0 or 7)
# │ │ │ │ │
# │ │ │ │ │
# * * * * * <user>  <command>
 17 * * * * root    cd / && run-parts --report /etc/cron.hourly
 25 6 * * * root    python /opt/clean-logs.py
```

Cron Job

- /etc/cron.d/*
- /etc/cron.daily
- /etc/cron.weekly
- /etc/cron.monthly
- crontab -e

Screen

- Reconnect to a shell
- Commands
  - screen → start session
  - Ctrl+a, d → detach session
  - screen -ls → list all sessions
  - screen -r → reconnect to session
  - screen -r <name> → reconnect to session

Network

Network (Ubuntu)

- /etc/network/interfaces

```
auto eth0
iface eth0 inet static
    address 192.168.0.42
    network 192.168.0.0
    netmask 255.255.255.0
    broadcast 192.168.0.255
    gateway 192.168.0.1
```

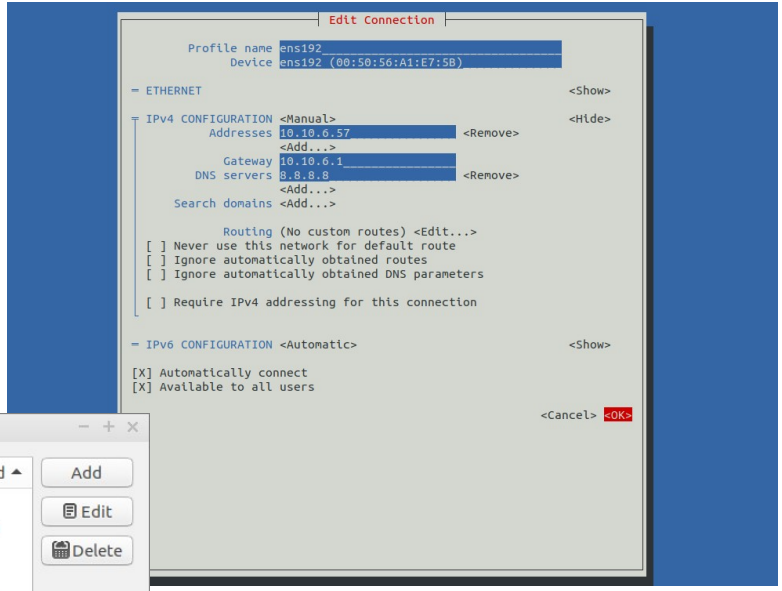
Network (CentOS)

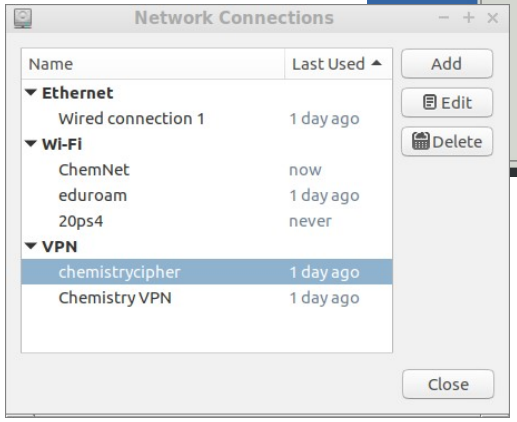
- /etc/sysconfig/network-scripts/ifcfg-*

```
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="dhcp"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="ens192"
UUID="92a2689a-2ccd-41c8-9dc5-67ff6793809f"
DEVICE="ens192"
ONBOOT="yes"
IPV6_PRIVACY="no"
```

Network-Manager

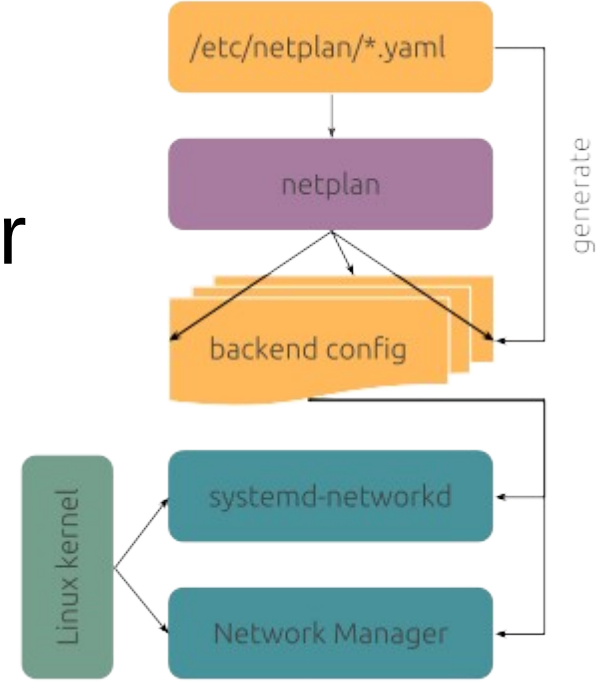
- User friendly
- Desktop oriented
- nmtui





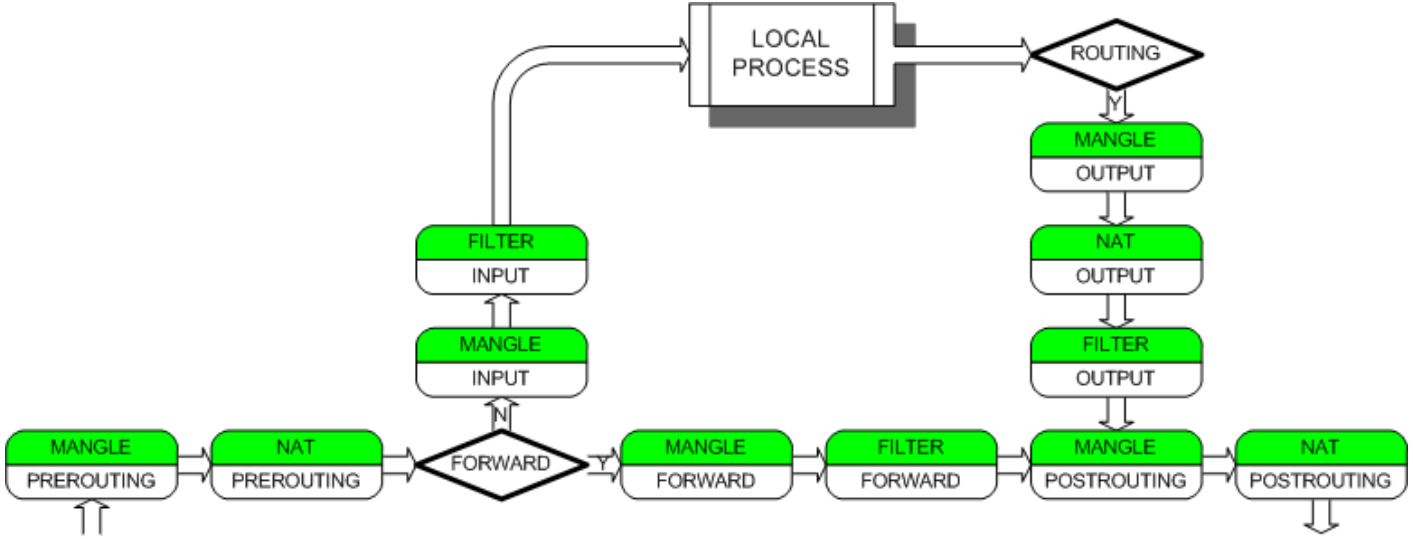
Netplan

- New in Ubuntu 18.04
- Config in yaml
- Networkd and Network-Manager
- /etc/netplan/*
- Future unknown



iptables

- Local firewall
- Disabled by default



selinux

- Security-Enhanced Linux
- Disable if not required
- /etc/selinux/config

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=disabled
```

AXXES
IT CONSULTANCY

Network

Troubleshooting

AXXES IT CONSULTANCY

- # List network info (old)

```
sander@LT1905:$ ifconfig
enp0s20f0u7: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.42.216  netmask 255.255.255.0  broadcast 192.168.42.255
        inet6 fe80::98f2:833a:5814:9a08  prefixlen 64  scopeid 0x20<link>
        ether fa:74:2f:92:3c:89  txqueuelen 1000  (Ethernet)
        RX packets 6227  bytes 2305098 (2.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6173  bytes 1079776 (1.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 716353  bytes 70015115 (70.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 716353  bytes 70015115 (70.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisi
```

- # List network info

```
[root@SRVGFS01 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
qlen 1000
    link/ether 00:50:56:a1:e7:5b brd ff:ff:ff:ff:ff:ff
    inet 10.10.6.127/24 brd 10.10.6.255 scope global noprefixroute dynamic ens192
       valid_lft 5939sec preferred_lft 5939sec
    inet6 fe80::c638:608e:e010:daca/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- # Show route table

```
sander@LT1905:~$ ip route
default via 172.16.10.1 dev wlp1s0 proto dhcp metric 600
169.254.0.0/16 dev wlp1s0 scope link metric 1000
172.16.10.0/24 dev wlp1s0 proto kernel scope link src 172.16.10.188 metric 600
```

- # Show arp table

```
[root@SRVGFS01 ~]# ip neigh
10.10.6.2 dev ens192 lladdr 00:50:56:a1:6c:83 STALE
10.10.6.1 dev ens192 lladdr 00:00:5e:00:01:01 REACHABLE
10.10.6.4 dev ens192 lladdr 00:50:56:a1:b7:46 REACHABLE
10.10.6.30 dev ens192  FAILED
10.10.6.3 dev ens192 lladdr 00:50:56:a1:8c:6c STALE
10.10.6.22 dev ens192 lladdr 00:50:56:a1:16:90 REACHABLE
10.10.6.21 dev ens192 lladdr 00:50:56:a1:bd:cb REACHABLE
10.10.6.5 dev ens192 lladdr 00:50:56:a1:c4:00 REACHABLE
```

- # Ping

```
sander@LT1905:$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=52 time=127 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=52 time=39.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=52 time=47.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=52 time=37.6 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=52 time=38.2 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 37.592/57.756/126.822/34.707 ms
```

- # Traceroute

```
sander@LT1905:$ traceroute 216.58.204.46
traceroute to 216.58.204.46 (216.58.204.46), 30 hops max, 60 byte packets
 1  _gateway (192.168.42.129)  1.068 ms  1.082 ms  1.139 ms
 2  * * *
 3  10.54.41.1 (10.54.41.1)  54.322 ms  54.322 ms  54.225 ms
(...)
13  209.85.143.66 (209.85.143.66)  78.065 ms 64.233.175.112 (64.233.175.112)  78.055 ms *
14  108.170.246.129 (108.170.246.129)  78.124 ms 108.170.246.161 (108.170.246.161)  45.778 ms  51.666
15  108.170.238.119 (108.170.238.119)  42.831 ms  62.462 ms 108.170.238.117 (108.170.238.117)  62.295
16  * * *
17  * * *
18  lhr25s12-in-f14.1e100.net (216.58.204.46)  61.969 ms *  37.295 ms
```

- # My Traceroute (real-time)

```
mtr google.com
                                My traceroute  [v0.71]
            example.lan                                Sun Mar 25 00:07:50 2007

                                          Packets                Pings
Hostname                               %Loss  Rcv  Snt  Last Best  Avg  Worst
 1. example.lan                           0%   11   11     1    1    1      2
 2. ae-31-51.ebr1.Chicago1.Level3.n      19%    9   11     3    1    7     14
 3. ae-1.ebr2.Chicago1.Level3.net         0%   11   11     7    1    7     14
 4. ae-2.ebr2.Washington1.Level3.ne      19%    9   11    19   18   23     31
 5. ae-1.ebr1.Washington1.Level3.ne      28%    8   11    22   18   24     30
 6. ge-3-0-0-53.gar1.Washington1.Le       0%   11   11    18   18   20     36
 7. 63.210.29.230                         0%   10   10    19   19   19     19
 8. t-3-1.bas1.re2.yahoo.com              0%   10   10    19   18   32    106
 9. p25.www.re2.yahoo.com                 0%   10   10    19   18   19     19
```

- # List listening ports (legacy)

```
sander@LT1905:~$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:41275         0.0.0.0:*               LISTEN      2886/cloud-c
(...)
tcp        0      0 127.0.0.1:1029          0.0.0.0:*               LISTEN      2967/cloud-da
tcp        0      0 127.0.0.1:46025         0.0.0.0:*               LISTEN      2893/cloud-co
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
(...)
udp6       0      0 :::48896                :::*                                -
```

- # List listening ports (new)

```
sander@LT1905:~$ ss -tulpn
Netid    State      Recv-Q     Send-Q       Local Address:Port            Peer Address:Port
udp      UNCONN     0          0            127.0.0.53%lo:53                   0.0.0.0:*
udp      UNCONN     0          0                  0.0.0.0:68                   0.0.0.0:*
udp      UNCONN     0          0                  0.0.0.0:631                  0.0.0.0:*
udp      UNCONN     0          0                  0.0.0.0:5353                 0.0.0.0:*
udp      UNCONN     0          0                  0.0.0.0:60789                0.0.0.0:*
udp      UNCONN     0          0                     [::]:5353                    [::]:*
udp      UNCONN     0          0                     [::]:48896                   [::]:*
tcp      LISTEN     0          128          127.0.0.53%lo:53                   0.0.0.0:*
tcp      LISTEN     0          5                127.0.0.1:631                  0.0.0.0:*
tcp      LISTEN     0          32               127.0.0.1:1024                 0.0.0.0:*   ...
tcp      LISTEN     0          128              127.0.0.1:1025                 0.0.0.0:*   ...
tcp      LISTEN     0          128              127.0.0.1:1026                 0.0.0.0:*   ...
tcp      LISTEN     0          128              127.0.0.1:1027                 0.0.0.0:*   ...
tcp      LISTEN     0          32               127.0.0.1:1028                 0.0.0.0:*   ...
tcp      LISTEN     0          128              127.0.0.1:1029                 0.0.0.0:*   ...
tcp      LISTEN     0          5                    [::1]:631                     [::]:*
```

AXXES IT CONSULTANCY

- # Port-scan

```
sander@LT1905:~$ nmap axxes.com
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-27 15:08 CEST
Nmap scan report for axxes.com (176.62.168.199)
Host is up (0.094s latency).
rDNS record for 176.62.168.199: 176.62.168.199.static.hosted.by.combell.com

PORT      STATE    SERVICE
9/tcp     open     discard
20/tcp    open     ftp-data
21/tcp    open     ftp
22/tcp    filtered ssh
23/tcp    open     telnet
25/tcp    open     smtp
110/tcp   open     pop3
143/tcp   open     imap
161/tcp   open     snmp
```

- Check if port is open

```
sander@LT1905:~$ telnet goolge.be 80
Trying 185.53.178.22...
Connected to goolge.be.
Escape character is '^]'.
^]
```

- DNS query (legacy)

```
sander@LT1905:~$ nslookup google.com
Server:         127.0.0.53
Address:  127.0.0.53#53

Non-authoritative answer:
Name:google.com
Address: 216.58.211.110
Name:google.com
Address: 2a00:1450:400e:809::200e
```

- # DNS query (new)

```
sander@LT1905:~$ dig google.com
; <<>> DiG 9.11.5-P1-1ubuntu2.5-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26407
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN    A

;; ANSWER SECTION:
google.com.       69    IN    A     216.58.211.110

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: wo aug 28 13:25:38 CEST 2019
;; MSG SIZE  rcvd: 55
```

- # Packet capture

```
sander@LT1905:~$ sudo tcpdump -i wlp1s0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp1s0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:38:44.038125 ARP, Request who-has 172.16.10.84 tell 172.16.10.70, length 46
13:38:44.040315 IP LT1905.49993 > 172.16.10.3.domain: 44022+ [1au] PTR? 84.10.16.172.in-addr.arpa. (54)
13:38:44.070708 IP 172.16.10.3.domain > LT1905.49993: 44022 NXDomain 0/1/1 (103)
13:38:44.071066 IP LT1905.49993 > 172.16.10.3.domain: 44022+ PTR? 84.10.16.172.in-addr.arpa. (43)
13:38:44.072680 IP 172.16.10.3.domain > LT1905.49993: 44022 NXDomain 0/1/0 (92)
13:38:44.074129 IP LT1905.44480 > 172.16.10.3.domain: 48968+ [1au] PTR? 70.10.16.172.in-addr.arpa. (54)
13:38:44.075331 IP LT1905.47984 > ec2-52-30-188-175.eu-west-1.compute.amazonaws.com.https: Flags [.], ack 1347930532, w
13:38:44.102439 IP LT1905.37066 > 172.16.10.3.domain: 7751+ [1au] PTR? 175.188.30.52.in-addr.arpa. (55)
13:38:44.115689 IP 172.16.10.3.domain > LT1905.37066: 7751 1/0/1 PTR ec2-52-30-188-175.eu-west-1.compute.amazonaws.com.
13:38:45.062138 ARP, Request who-has 172.16.10.84 tell 172.16.10.70, length 46
13:38:45.099322 IP LT1905.41802 > ec2-52-210-19-6.eu-west-1.compute.amazonaws.com.https: Flags [.], ack 2272216828, win
13:38:45.099401 IP LT1905.36580 > server-13-224-244-36.lhr62.r.cloudfront.net.https: Flags [.], ack 617216046, win 501,
13:38:45.103466 IP server-13-224-244-36.lhr62.r.cloudfront.net.https > LT1905.36580: Flags [.], ack 1, win 359, length
13:38:45.103467 IP ec2-52-210-19-6.eu-west-1.compute.amazonaws.com.https > LT1905.41802: Flags [.], ack 1, win 1024, le
13:38:45.983933 ARP, Request who-has 172.16.10.84 tell 172.16.10.70, length 46
```

- More
  - https://www.tecmint.com/linux-networking-commands/
  - google.com
  - ...

Logs and Troubleshooting

Logs

- /var/log/syslog (Ubuntu)
- /var/log/messages (CentOS)
- dmesg

journalctl

- Added in systemd
- Central logging system
- Also boot logs

journalctl

```
## List all logs
journalctl
## List all logs since boot
journalctl -b
journalctl -b -1
journalctl --list-boots
journalctl -b 13883d180dc0420db0abcb5fa26d6198
## Filter on logs
journalctl --since "2019-01-10 17:15:00"
journalctl --since "2019-01-10" --until "2019-01-11 03:00"
journalctl –since yesterday
journalctl -u nginx.service
journalctl -k           #kernel logs
# real-time logs
journalctl -f
```

Help

- -h, --help
- man
- Google
- unix.stackexchange.com
- askubuntu.com
- ...

Scripting

Bash

- Windows has Powershell, Linux has bash
- .sh file
- Start with Shebang (#!/bin/bash)

Basic

```
## Print line
echo “something to print”

## Variables
A=15
NAME="John"
C=$(ip a)
echo "Congratulations with your $A birthday ${NAME}!"
```

If-then-else

```
if [[ -z "$string" ]]; then
  echo "String is empty"
elif [[ -n "$string" ]]; then
  echo "String is not empty"
fi

#-----------------------------------------------------------------------

if ping -c 1 google.com; then
  echo "It appears you have a working internet connection"
fi
```

Loop

```
## for each number from 1 to 5 print “Welkom”
for i in {1..5}; do
    echo "Welcome $i"
done
```

```
while true; do
  ...
done
```

…

...

- https://devhints.io/bash

AXXES
IT CONSULTANCY

Config management

Tools

- Ansible
- Puppet
- Chef
- Salt (SaltStack)
- Terraform

Ansible

- Agent-less
- ssh, powershell,….
- yml-files
- Simple
- Playbook → Play → Roles → Tasks → Modules

Puppet

- Agent – Master
- Declarative
- …

Chef

- Master - Slave
- Ruby and Erlang
- ...

SaltStack

- Master – Minion
- …

Terraform

- Infrastructure as code
- Declarative

Reflection

- Kernel, distro’s, ssh, disks, partitions, users, permissions, package manager, init, networking,…
- Don’t be afraid. Just try it.

Evaluation

- https://forms.office.com/Pages/ResponsePage.aspx?id=tsPR7Ye-u0OS1HqRHFzuFxuX3eVGfXtFoOzIyh2dgltUOERVRjU3RFZZM0NDU0VFWDBNUUhEMFpSNy4u

The end

Thank you!

email: sander.descamps@axxes.com
email: sander_descamps@hotmail.com