Contents

[Tools and tricks: 3](#_Toc520365868)

[NANO editor 3](#_Toc520365869)

[mc 3](#_Toc520365870)

[history 3](#_Toc520365871)

[SYSTEM BOOT 3](#_Toc520365872)

[Runlevels/Targets 3](#_Toc520365873)

[init 3](#_Toc520365874)

[systemd 3](#_Toc520365875)

[Runlevels 3](#_Toc520365876)

[Targets 4](#_Toc520365877)

[Start services: 5](#_Toc520365878)

[DISK management 5](#_Toc520365879)

[Add new volume to the system (AWS) 5](#_Toc520365880)

[LVM 5](#_Toc520365881)

[Create a volume group 6](#_Toc520365882)

[Extend existing volume group 6](#_Toc520365883)

[Reducing disk space 6](#_Toc520365884)

[Network configuration 8](#_Toc520365885)

[Configure static IP 8](#_Toc520365886)

[SETUP FIREWALLS with iptables 9](#_Toc520365887)

[IDENTIFY NETWORK ISSUES 9](#_Toc520365888)

[Packets analyzing 10](#_Toc520365889)

[Command route 10](#_Toc520365890)

[Protocol SSH 11](#_Toc520365891)

[SYSTEM TROUBLESHOOTING 12](#_Toc520365892)

[CPU check: 12](#_Toc520365893)

[DEVICES: 12](#_Toc520365894)

[Memory check 12](#_Toc520365895)

[Disk usage 12](#_Toc520365896)

[Monitoring tools 12](#_Toc520365897)

[LOG files 13](#_Toc520365898)

[Running jobs 13](#_Toc520365899)

[Network File System 15](#_Toc520365900)

[Users and Groups management 16](#_Toc520365901)

[Create user 16](#_Toc520365902)

[Create group 16](#_Toc520365903)

[User disk quota 16](#_Toc520365904)

[Change root password 17](#_Toc520365905)

[Interview Questions 17](#_Toc520365906)

# Tools and tricks:

## NANO editor

* String search - ^w
* Exit: ^x

## mc

(midnight commander, like Northon (nc))

* delete line from the history:

## history

history –d <line number>

To make command not to be saved in history

>HISTCONTROL=ignorespace

Commands started with space will not be saved in history

# SYSTEM BOOT

## Runlevels/Targets

* preset operating state
* have a set of active processes
* combination of services

## init

* the first daemon process to start
* pid=1
* starts the other processes ***serially***

## systemd

/lib/systemd

* the first daemon process to start
* pid=1
* starts the process in ***parallel***

## Runlevels

* runlevel **0** is halt
* runlevel **1** is single user – root (rescue mode)
* runlevels **2-4** are multiuser
* runlevel **5** - graphical
* runlevel **6** is reboot

ubuntu@ip-172-31-47-11:/lib/systemd/system$ ls -ld runlevel\*target

lrwxrwxrwx 1 root root 15 Mar 8 17:51 runlevel0.target -> poweroff.target

lrwxrwxrwx 1 root root 13 Mar 8 17:51 runlevel1.target -> rescue.target

lrwxrwxrwx 1 root root 17 Mar 8 17:51 runlevel2.target -> multi-user.target

lrwxrwxrwx 1 root root 17 Mar 8 17:51 runlevel3.target -> multi-user.target

lrwxrwxrwx 1 root root 17 Mar 8 17:51 runlevel4.target -> multi-user.target

lrwxrwxrwx 1 root root 16 Mar 8 17:51 runlevel5.target -> graphical.target

lrwxrwxrwx 1 root root 13 Mar 8 17:51 runlevel6.target -> reboot.target

Current runlevel:

>runlevel

N 3

To change runlevel use command init or telinit

ec2-user@karalov01:/lib>telinit 4

ec2-user@karalov01:/lib>runlevel

3 4

Previous was 3 , current 4

The default runlevel is defined in file /etc/inittab (RedHat, Centos, Debian) or /etc/init/rc-sysinit.conf in Ubuntu

Services that will be started for RL 2 immediately after boot (Ubuntu) or killed before shutdown. S – start, K - kill

**S**<NUM> - priority

(ubuntu)root@ip-172-31-47-11:/etc/rc**2**.d$ls -l .

total 4

-rw-r--r-- 1 root root 677 Feb 5 2016 README

lrwxrwxrwx 1 root root 16 May 22 10:55 S01apport -> ../init.d/apport

lrwxrwxrwx 1 root root 22 May 22 10:55 S01lvm2-lvmetad -> ../init.d/lvm2-lvmetad

lrwxrwxrwx 1 root root 23 May 22 10:55 S01lvm2-lvmpolld -> ../init.d/lvm2-lvmpolld

lrwxrwxrwx 1 root root 13 May 22 10:55 S01lxd -> ../init.d/lxd

lrwxrwxrwx 1 root root 23 May 22 10:55 S01open-vm-tools -> ../init.d/open-vm-tools

lrwxrwxrwx 1 root root 17 May 22 10:54 S01rsyslog -> ../init.d/rsyslog

…

Check rsyslog for all run levels:

(ubuntu)root@ip-172-31-47-11:~$ls -1 /etc/rc?.d/\*rsyslog

/etc/rc0.d/K04rsyslog

/etc/rc1.d/K04rsyslog

/etc/rc2.d/S01rsyslog

/etc/rc3.d/S01rsyslog

/etc/rc4.d/S01rsyslog

/etc/rc5.d/S01rsyslog

/etc/rc6.d/K04rsyslog

To disable booting/killing process at specific run level, delete link from rc<N> for this server. To delete links from all run levels for specific service (e.g. apache2), use command

***>update-rc.d –f apache2 remove***

To restore links:

***>update-rc.d apache2 defaults***

File /etc/init.d/apache2 should be present

Another way to disable apache2 at start:

***>update-rc.d apache2 disable***

To restore, use “enable”

To disable/enable for specific run level (e.g enable for RL 3)

***>update-rc.d apache2 enable 3***

To change priority – rename link to change name with required priority

***>/mv etc/rc3.d/S01rsyslog /etc/rc3.d/S90rsyslog***

## Targets

Used on Ubuntu. For redhat use runlevel. Ubuntu can use both

To get default target:

***>systemctl get-default***

graphical.target

To set default to multi-user

***(ubuntu)root@ip-172-31-47-11:~$systemctl set-default multi-user.target***

Created symlink from /etc/systemd/system/default.target to /lib/systemd/system/multi-user.target.

(ubuntu)root@ip-172-31-47-11:~$runlevel

N 5

(ubuntu)root@ip-172-31-47-11:~$systemctl isolate multi-user.target

(ubuntu)root@ip-172-31-47-11:~$runlevel

5 3

## Start services:

(ubuntu)>systemctl (start/stop/enable/status) apache2

(redhat)> service httpd (stop/start/status)

(redhat)>chkconfig httpd on -> enable to be started on boot

# DISK management

## Add new volume to the system (AWS)

1. Available disks:

ec2-user@karalov01:/home/ec2-user>lsblk

NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT

xvda 202:0 0 8G 0 disk

└─xvda1 202:1 0 8G 0 part /

xvdf 202:80 0 100G 0 disk

2. Check if disk has FS on it

[ec2-user ~]$ **sudo file -s /dev/xvdf**

/dev/xvdf: data

Data – means no FS, should be created

3. Create a new FS (All data will be erased)

>mkfs -t ext4 /dev/xvdf

4. Create a mount point

>mkdir /dima

5. mount new device to the mount point

>mount /dev/xvdf /dima

6. To mount this EBS volume on every system reboot, add an entry for the device to the /etc/fstab file.

*#device\_name* *mount\_point* *file\_system\_type* *fs\_mntops* *fs\_freq* *fs\_passno*

/dev/xvdf /dima ext4 defaults,nofail 0 2

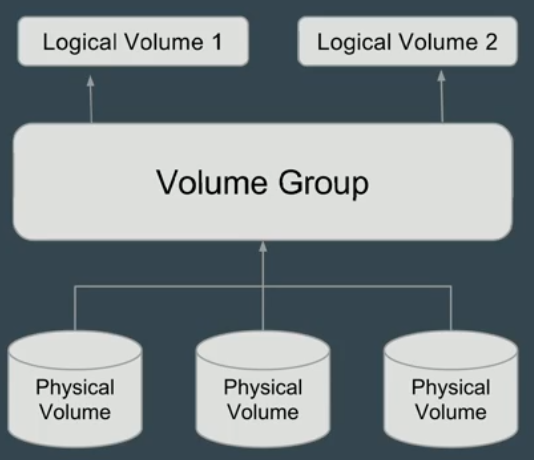
Run to check that no errors in fstab

>mount -a

## LVM

Logical volume manager

* simple to use
* on the fly changes
* online relocation
* flexible storage
* disk stripping
* the package needed for using LVM is lvm2



## Create a volume group

1. Add a new hard drive on the virtual machine
2. Create a partition on the hard drive
3. Create a physical volume (PV) of the partition previously created
4. Create a volume group (VG)
5. Create a logical volume (LV) and the file system
6. Add entry in /etc/fstab file for mounting at boot

## Extend existing volume group

1. Run steps 1-3 from above
2. Assign the PV to an existing VG
3. Extend the logical volume (LV)
4. Resize the file system

## Reducing disk space

1. Check disk for errors
2. Resize the filesystem on the desired size
3. Reduce the LV to the desired size
4. Check to see if the disk can be removed
5. If disk is not free, then move data from the disk to another
6. Reduce the VG with the disk you wish to delete
7. Remove the physical volume
8. Re-check that disk was removed
9. Increase the LV if there’s any free space left on the last disk
10. Resize the file system
11. Remove the disks from virtual machine



# Network configuration

Change the hostname: /etc/hostname

Or use command

>hostname <new name>

File /etc/resolv.conf – important information about resolving servernames

Header file /usr/include/resolv.h

File have IP address of the server (nameserver entry) that will resolve server names

ec2-user@karalov01:~>cat /etc/resolv.conf

options timeout:2 attempts:5

; generated by /sbin/dhclient-script

search us-east-2.compute.internal

nameserver **172.31.0.2**

ec2-user@karalov01:~>nslookup google.com

Server: **172.31.0.2**

Address: 172.31.0.2#53

Non-authoritative answer:

Name: google.com

Address: 216.58.216.206

Another command:

>dig google.com

It will resolve name and will show more details, including time that took to nameserver to resolve the name.

Local names resolving: **/etc/hosts**

Restart network:

/**etc/init.d/networking restart** (ubuntu)

File **/etc/nsswitch.conf** - order of resolving server names.

Entry: **hosts**

Fitst files(/etc/hosts), then dns (nameserver)

**hosts: files dns**

## Configure static IP

****

To set instant IP for the server instead to be dynamically assigned by DHCP server, modify file /etc/network/interfaces (ubuntu) for your interface

Comment dhcp resolving and add inet entry

#iface eth0 inet dhcp

iface eth0 inet static

address 192.168.12.132

netmask 255.255.255.0

gateway 192.168.12.2

Restart networking after changing

**Ifdown eth0** – to stop etch0 iface

**Ifstart eth0** – start it again

Another tool: ip

ip a - list interfaces

ip link set etho0 (down/up) – stop/start iface

Add interface alias :

ip a add 192.168.1.119 dev eth0:0

Routing table:

ip route show

route

route –n – numeric IP display

## SETUP FIREWALLS with iptables



## IDENTIFY NETWORK ISSUES

1. To check if network card (NIC) was found at boot:

>dmesg | grep eth (interface name)

2. check that you have assigned Ip: ifconfig

3. ping another server in the local network (ping command)

4. ping server outside of the network, ping router ip address

5. check firewall (iptables –L) - if yes, use iptables –F to delete all rules

6. if you can ping ip, but server name is not resolved – check file /etc/resolv.conf

Command ***traserout -*** shows all hops from source to destination

Command netstat – all current network connections

Netstat –ta (TCP, all LISTENING and ESTABLISHED)

Netstat –ua (UDP)

Netstat –tan (Numeric IPs instead of server names)

Add “p” to display process ID and name (root only)

Netstat –s details about received/sent packets

Another command similar to netstat is “ss”

## Packets analyzing

>tcpdump

>tcpdump -i any – for all interfaces

>tcpdump –D -list all interfaces

>tcpdump -i eth0 – analyze specific interface

>tcpdump –i eth0 -w data.pcap – dump to file data.pcap



## Command route

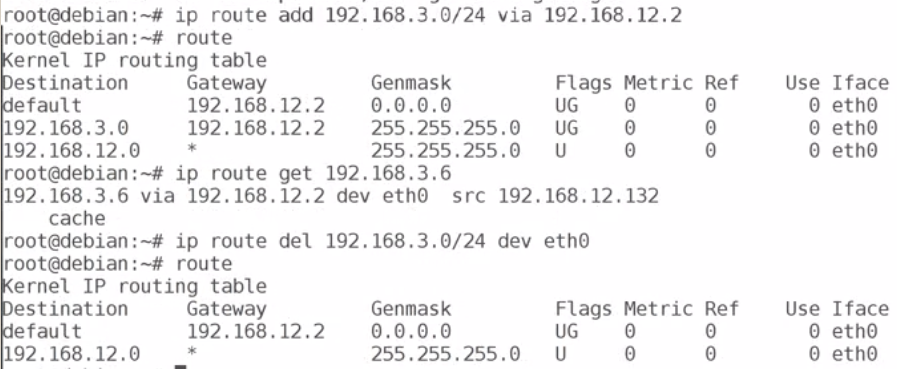
>route - current routing



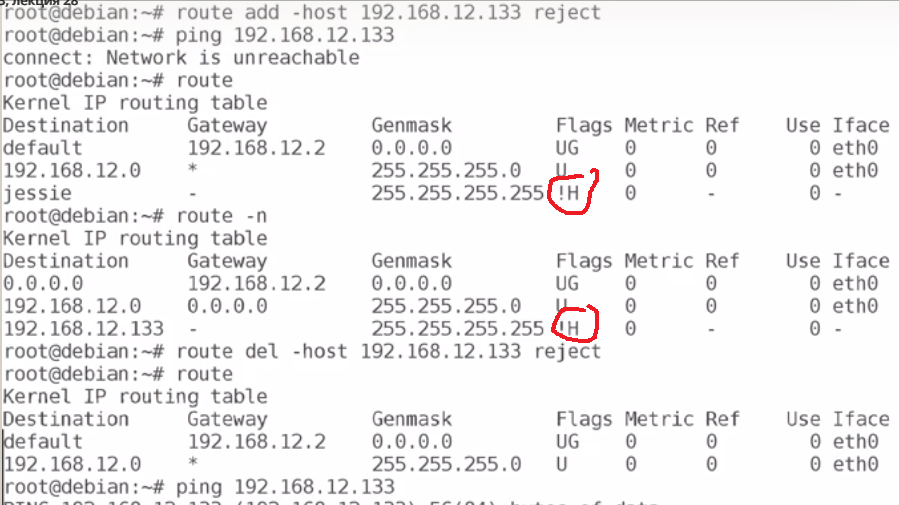




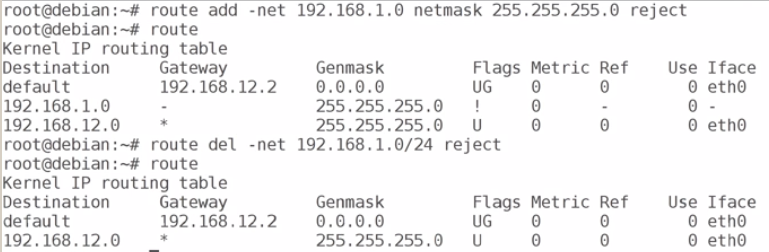




Block IPs



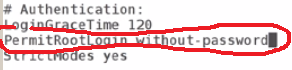
Reject whole network range



## Protocol SSH

Configuration file: /etc/ssh/sshd\_config

To change root login options via ssh change parameter



If “yes” – root from another server will be able to login as root.

If “no” or “without-password” – no root login enabled, means you have to login first as regular user and then change user to root.

Generate public key:



To copy public key to remote server:



# SYSTEM TROUBLESHOOTING

## CPU check:

>lscpu

>cat /proc/cpuinfo

## DEVICES:

>lspci - list of PCI devices

>lsusb – usb devices

File systems (block devices)

>lsblk –list of block devices

>blkid – detailed info

## Memory check

>free –m (mBytes

>cat /proc/meminfo

## Disk usage

du -h - human readable – all folders recursively

du –h –max-depth 1 – maximum depth of the recursivity (subfolders)

du –h –time –to see when the file was last modified-

## Monitoring tools

>***watch*** - will run any command every 2 seconds

>watch df –h

>watch iptables –nvL

>**iostat** – disk usage and cpu stats

>iostat 5 2 – display report every 5 sec 2 times

>iostat –p sda –x - display info for sda devices, in e**x**tended format

>top

>**uptime** - how long system was up and running and avg load

>**vmstat** – memory usage

>vmstat –s detailed memory report

>vmstat -s -S M – display in Mb

>vmstat –S M 2 3 – every 2 seconds for 3 times

>iotop – io usage (should be istalled)

>iotop --only - display io only

***Use arrows to switch columns for sorting***

r – to reverse sorting order

>sar – display historical usage of resources (CPU by default)

>sar –r -> memory usage

>sar –S – swap

>sar –b – I/O

>sar –r 2 2 > every 2 seconds 2 outputs

Statistics files are stored under /var/log/sysstat with day number

>sar –f /var/log/sysstat/sa08 - display stats for day 08

>sar –r –f /var/log/sysstat/sa08 –q –s 11:00:00 – memory report from day 8 after 11:00 only

To enable stats collection update file /etc/default/sysstat

>ps –eo pcpu,pid,user, args | sort –k 1 –r : display processes with cpu usage, username, with it’s agrs, sorted first column in reverse order

>ps aux – all running processes, cpu, memory, started time etc

>lsof – opened files

>lsof /var/log/syslog - to check who opened this file.

>lsof –c rsyslogd - list all files opened by process rsyslogd

>lsof –u carmen - list all files opened by user carmen



## LOG files

System logs – syslog

Configuration file /etc/rsyslog.conf

## RULES ##

user.\* /var/log/user.log #- all user logs of all priorities written to file

/dev/console – write to console

@log.server.com - to the server

mail.info /var/log/mail.info - info priority and up (war,err, critical) write to file

mail.=warn /var/log/mail.warn - only warning priority

mail.!error /var/log/mail.error - all priorities below error

Log files are located under /var/log

/var/log/dmesg - log file of the boot time

>lastlog list of users and their last login time

>lastlog –u carmen – last log for the user carmen

>less syslog - system log

/var/log/apt/history.log - log of installed packages

Log rotation utility

/etc/logrotate.d - for applications

/etc/logrotate.conf - general

## Running jobs

Schedule one-time job run at specific time:

>at 13:30

>atq - print queue of the at scheduled jobs

>at –c 34 - display command scheduled for at job #34

>atrm 34 - remove job #34

>at 9:00 AM Sun - schedule 9am on Sunday

>at 9:00 Apr 20

>at 9:00 next month - same day next month

>at 9:00 tomorrow

>at now + 1 hour

>at now + 1 year

> at midnight

Send output to terminal

>tty

/dev/pts/1

>at now + 2 minutes

At> echo “Hello” > /dev/pts/1

>

Cron:

/etc/crontab – system jobs only

M h dom mon dow user command

17,18,30 \* \* \* \* root echo ‘this will run every 17,18 and 30 min)

17-30 \* \* \* \* root echo ‘this will run every minute starting from 17 ending 10 included

Mon can be number or word, the same day of week dow

\*/17 \* \* \* \* - run job every 17 minutes

If you want to run some job daily/monthly/hourly – put it to the folder /etc/cron.<period>

User crontab files are stored under /var/spool/cron/crontabs

Anacron

Configuration: /etc/anacrontab

First field – to run evey # of days (1 – daily, 7 – weekly, @monthly - monthly)

Second field – delay before executing the command (min)

>anacron –T – test for errors

Spool for anacron: /var/spool/anacron

It stores date when job was lastly executed

To force run anacron:

>anacron –d –f

# Network File System

NFS services:

* Portmap/portmapper – what port NFS is running
* Rpc.idmapd – maps users
* Rpc.mountd – controls mount requests from clients
* Rpc.nfsd – user level part of NFS service
* Rpc.statd – announce clients when server reboots

NFS processes running in background:

>ps aux | grep rpc

On the server:

The package form NFS installation is nfs-kernel-server

>mkdir /var/nfs

Update file /etc/exports

Add shared dir and ip’s of clients + options in brackets

/var/nfs 192.168.12.133(rw,sync,no\_subtree\_check, root\_squash)

Run

>exportfs –a

To check exported folders:

>exportfs

On the client:

Install package nfs-common

>mkdir /nfs

>mount 192.168.12.132:/var/nfs /nfs

To make it permanent, update /etc/fstab on client

First, check nfs version on server

>nfsstat | less

In the /etc/fstab

For nfs v4

192.168.12.132:/var/nfs /nfs nfs4 hard,intr,rsize=32768,wsize=32768 0 0

for options check man nfs

# Users and Groups management

## Create user

>useradd john - Create user

>passwd john

>mkdir /home/john - create home directory

>chown john:john /home/john

>useradd –m karla - will create homedir automatically

For all options check man adduser

Remove user:

>userdel john

Lock user:

>passwd –l karla - unable to connect to this user from outside, but local root can connect

Unlock: passwd –u karla

Expire user:

>chage –E -0 karla (restore –E -1)

## Create group

>groupadd sysadmin

Append user john to group sysadmin

>usermod –a –G sysadmin john

>grep sysadmin /etc/group

Remove user from group:

>gpasswd –d john sysadmin

## User disk quota

>apt install quota

In the file /etc/fstab, for the required FS add option usrquota and grpquota (for group)

UUID=AAAA ext4 errors=remount-ro,usrquota,grpquota

Then remount FS

>mount –o remount /

Create quota files, check user files, no remount

>quotacheck –cum /

>quotaon / – enable quota on /

>quotaoff /

>edquota maks - edit quota for user

>quota maks - check current quota

>repquota –a - report for all users

>edquota –t – edit grace period, for all users only

# Change root password



## Interview Questions

