Kernel

- Ubuntu deposundaki kaynaktan derlemece
    - kernel/compiler-from-apt-source.sh
    - compile-from-kernel-source/compile-from-kernel-source.sh

menuconfig ekranındaki menülerle ilgili açıklama

General Setup Miscellaneous and fairly high-level options appear in this category, including many that relate to how the
Enable the Block Layer This short category includes some obscure options related to disk devices and how the kernel manages input/output (I/O) scheduling. Select the defauloptions unless you have specific reason to do otherwise.
Processor Type and Features This section includes options that control how Linux manages the CPU, including several options that are CPU- specifi c. The Paravirtualized
Guest Support subsection includes options that are important if you want to run certain types of virtualization software, which enables you to run another OS within your Linux system. (See also the Virtualization section, described shortly.)
Power Management and ACPI Options Options in this area relate to hardware features
designed to minimize power use, including support for suspend-to- RAM and suspend-todisk (or hibernation) features that are particularly important on laptop computers.

Bus Options (PCI, etc.) Over the course of Linux' s history, several computer busses have been
popular and then faded away. Old busses include the Industry Standard Architecture (ISA), the
Extended ISA (EISA), the VESA Local Bus (VLB), Micro Channel Architecture (MCA), and
NuBus. Depending on your platform, many of these obsolete busses may be available. You can
trim your kernel size by removing them, if you' re certain your hardware doesn't use them. This
section also includes options related to PC Card (commonly used on laptops).
Executable File Formats/Emulations Your kernel should almost certainly support the Executable and Linkable Format (ELF) file format for binaries. Support for the older a.out
format is seldom necessary today unless you have some extremely old binary programs you

need to run. Including support for miscellaneous binaries is usually a good idea. On x86 - 64
systems, including support for IA32 is usually wise.
Networking Support This kernel configuration area is huge and includes a large number
of options that can be confusing to the uninitiated. Note that low-level network hardware
drivers do not reside in this area, but in the next one. You can usually greatly reduce compilation time and kernel (or at least module) size by perusing the options and removing
unnecessary features. For instance, you' re unlikely to need obscure networking stacks such
as AppleTalk, DECnet, or IPX. On the other hand, if your local network uses one of these
protocols, be sure it ' s installed!
Device Drivers This configuration area is enormous. It includes options to support most of the hardware devices managed directly by the kernel, including hard disk controllers, network hardware drivers, multimedia devices (TV tuner cards and Webcams), video card framebuffer drivers, sound cards, and low-level USB devices. Many other options in this area relate to obscure or obsolete hardware. Follow the recommendations for specific devices or elect to compile the driver, at least as a module,
if you ' re uncertain what to do.
File Systems This category is extremely important, since it provides support for the filesystem used on your Linux boot device. Be sure to activate the appropriate filesystem,
which is typically ext2fs, ext3fs, ext4fs, ReiserFS, XFS, JFS, or Btrfs on modern systems.
CD - ROM, non - Linux, and other miscellaneous fi lesystems are listed in their own subcategories.
The Partition Types subcategory is also important, since it controls what partitioning systems
the kernel supports. On most systems, the PC BIOS (MS-DOS Partition Tables) Support option
is most critical; this activates support for the Master Boot Record (MBR) system used on most
x86 and x86-64 systems. The EFI GUID Partition Support option is important on Intel-based
Macintoshes and is becoming important on other systems.
Kernel Hacking You can set options that are mostly of interest to kernel developers in this section. Occasionally even a non-developer will need to adjust options in this area, particularly if you' re using an older kernel patch. (The Enable __deprecated Logic option,

for instance, is required by some third-party drivers.)
Security Options
A handful of security features can be controlled in this area.
Cryptographic API Some kernel features and non-kernel software require cryptographic
modules to be present in the kernel. You can enable or disable them here.

Virtualization This category provides support for certain virtualization features, used to
run another OS while Linux is running on the system.
Library Routines This section includes a handful of features that are used by other kernel
modules or by user- space programs. Stick with the default settings unless you know they
should be changed.

Bazı kernel menü ayarları:

General Setup -> Local Version You can add a string to the kernel version number using
this option. This feature can be handy if you need to experiment with kernel options; you
can build different kernels with different local version strings to signify different feature sets, thus keeping the kernels' module directories separated and producing different kernel
identifiers when using uname or similar utilities.
General Setup -> Initial RAM Filesystem and RAM Disk (initramfs/initrd) Support Be
sure to activate this support if you intend to use an initial RAM disk (described shortly, in
"Preparing an Initial RAM Disk").
General Setup -> Enable Loadable Module Support Be sure this option is enabled, unless
you intend to build a kernel with nothing but built-in drivers— a strange configuration with
serious drawbacks on typical desktop or server configurations today.
Processor Type and Features -> Symmetric Multi- Processing Support This option enables
support for more than one CPU or CPU core. Most modern computers have two or more
cores, so activating this support makes sense unless you're certain that your CPU has just
one core.

Processor Type and Features Processor Family If you're building a kernel for a specific
computer, or for a set of identical computers, you can eke out a bit of extra performance by
setting the correct CPU model in this option.
Processor Type and Features -> High Memory Support This option is available for x86
CPUs, but not for x86-64 CPUs. You can use it to optimize performance based on how much RAM your computer has. If you have less than 1 GiB of RAM, select Off; if you have
between 1 GiB and 4 GiB of RAM, select 4GB; and if you have more than 4 GiB of RAM,
select 64GB. An incorrect selection can result in an inability to use all your system' s memory.

Networking Support -> Networking Options -> TCP/IP Networking Almost all modern
computers need this option, since the Transmission Control Protocol/Internet Protocol

TCP/IP) is the basis of the Internet. This option contains a large number of suboptions. Peruse them and follow the suggestions or your judgment based on your knowledge of your
ocal network and the computer' s role in it. Note in particular the IPv6 Protocol suboption,
which controls support for the next-generation version of TCP/IP, which is becoming a necessity in some areas.
Networking Support -> Networking Options -> Network Packet Filtering Framework This option is critical if you want to configure a router or enable fi rewall rules on your computer.
Networking Support -> Networking Options -> Wireless
 Be sure to enable this option if
your computer uses a wireless network adapter.
Device Drivers -> SCSI Device Support The Small Computer Systems Interface (SCSI)
tandard is a high- end disk interface. (It' s also used by some scanners, printers, and other devices.) Although it ' s rare in modern computers, Linux uses a SCSI emulation layer or many devices, including drivers for the more common Serial Advanced Technology Attachment (SATA) disk interface and USB storage devices. Therefore, you must enable SCSI support, including support for SCSI disks and, usually, SCSI CD-ROMs, on most systems. If your system lacks true SCSI devices, though, you can usually uncheck the SCSI
Low- Level Drivers section, omitting the large number of SCSI drivers from your build.
Device Drivers Serial ATA and Parallel ATA Drivers This section includes drivers for

most modern and many older SATA and PATA disk controllers. Enable the overall section
and peruse it until you find your disk controller. Note that many controller chipsets include
both SATA and PATA support, but these are often listed separately in this driver section.
Thus, you may need to enable both SATA and PATA drivers. If you're building a kernel for
a specific computer with a known chipset, I recommend building these drivers directly into the kernel, rather than as modules.

Device Drivers -> Multiple Devices Driver Support This section includes options for Redundant Array of Independent Disks (RAID) and Logical Volume Manager (LVM) confi gurations, which are advanced disk management tools described in Chapter 4, " Advanced Disk Management. "

Device Drivers -> Graphics Support On most x86 and x86-64 systems, the features in his section are optional; however, enabling framebuffer support for your video chipset and ramebuffer console support will provide you with advanced options for adjusting text-
mode consoles. On some other platforms, you must include framebuffer support to get a
ext-mode console, and sometimes even for X.

Device Drivers -> USB Support This area includes both drivers for low-level USB hardware (typically built into the motherboard or on a plug-in card) and for a few USB devices or device categories, such as USB Mass Storage Support, which is used to interface with USB flash drives and other plug-in media. Many USB devices require support in other areas of the kernel, too.

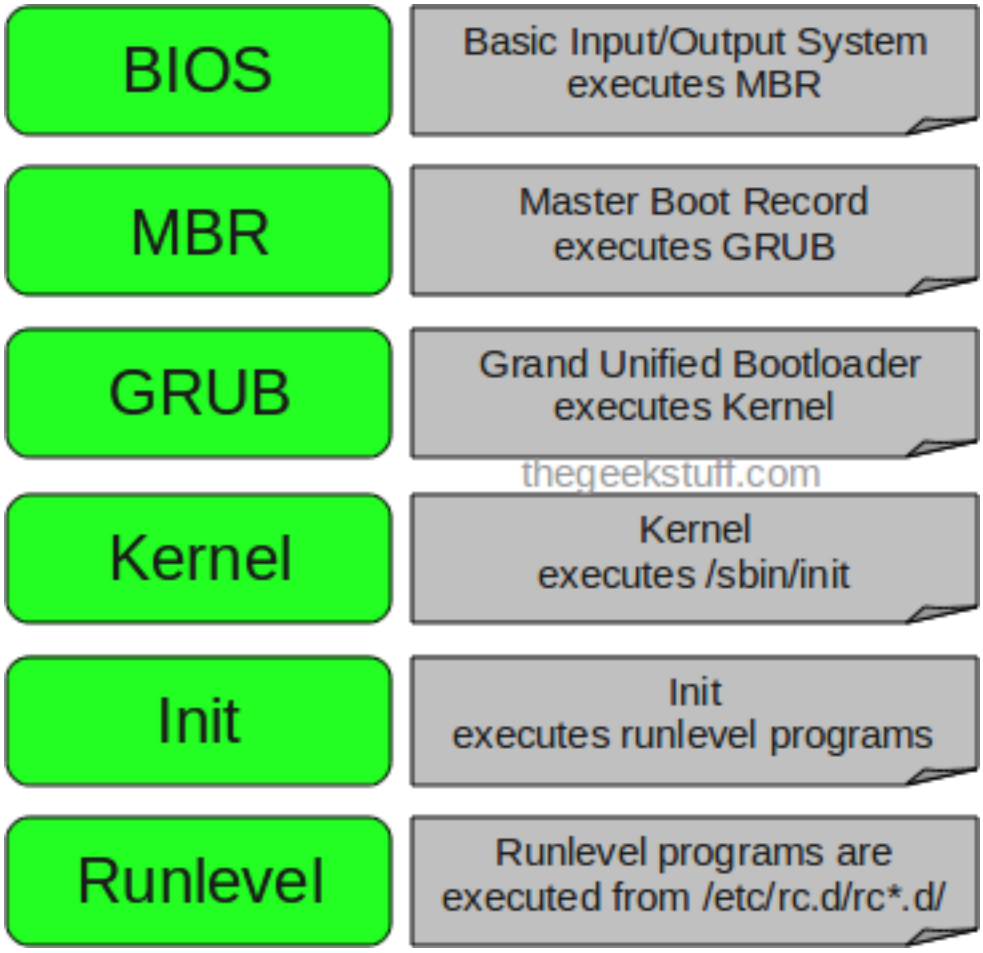
What is Initramfs

An initial RAM disk (aka an initial RAM fi lesystem) is a collection of critical kernel modules and a handful of system utilities that the boot loader reads from disk and passes to the kernel at boot time. The kernel accesses them in memory as if they were on disk, loading modules and running scripts and programs from the RAM disk in order to mount

Sürücü yüklemece:

lsmod
modinfo snd_intel8x0
insmod /lib/modules/3.17.6RC1/kernel/drivers/mmc/card/mmc_block.ko
modinfo mmc_block
modprobe mmc_block
rmmod soundcore

rmmod: ERROR: Module soundcore is in use by: snd
modprobe -r soundcore



patch

iki dosya oluşturuldu
diff -uNar ile patch oluştur
patch -p0 < my.patch
patch -R -p0 < my.patch

for kernel

Once a patch is downloaded to your local system, place it in the directory containing the folder of your kernel's source code. Ensure that the kernel and patch are compatible, meaning, they

must be the same version. Patches are applied to the uncompressed source code before the kernel is configured.

patch -p1 < ../PATCH

Startup

Runlevels

0 -> shutdown, transition from one state to another, powerff
1 -> single user mode, çalışan servisler dağıtıma göre değişiyor ama partition resizing, low-level system maintanence
2 -> Debian and its derivatives, full multi-user mode with X

komut satırında
runlevel

3 -> Fedora, Mandriva, Red Hat diğer pekçok dağıtımda full multi-user mode with console login
4-> Undefined, good for customization
5 -> 3 + graphical support, XDM for login
6 -> reboot

SystemV veya Upstart olarak tanımlanan yaklaşımda

1. yöntem /etc/inittab girdilerini değiştirmek

id:runlevels:action:process

id	This field consists of a sequence of one to four characters that identifies the entry ’s function.
runlevels	This field consists of a list of runlevels for which this entry applies. For instance, 345 means the entry is applicable to runlevels 3, 4, and 5.
action	Specific codes in this field tell init how to

	treat the process. For instance, wait tells init to start the process once when entering a runlevel and to wait for the process's termination, and respawn tells init to restart the process whenever it terminates (which is great for login processes). Several other actions are available; consult the man page for inittab for details.
process	This field specifies the process to run for this entry, including any options and arguments that are required.

/etc/rc./rcx.d veya /etc/init.d/rcx.d veya /etc/rcx.d altında sistem açılırkenki betikleri görebiliriz

Bu betiklerin çalışmasında S ile başlayanlara start parametresi gönderirken
durdurma sırasında K ile başlayanlar stop arametresi gider

S10network
K10smb

sayısal olarak önde olan ilk başlar

Ubuntu için

update-rc.d

update-rc.d [options] name action

update-rc.d samba defaults

Creates links to start the service in runlevels 2, 3, 4, and 5, and to
stop it in runlevels 0, 1, and 6.

update-rc.d gdm disable 234

sudo update-rc.d foo defaults
sudo update-rc.d foo disable

sudo update-rc.d -f remove

changing runlevel

init 0
init 6

shutdown now
 shutdown -h +2 “system going down for maintenance” # 2 minutes lates
shutdown -c “never mind”
shutdown -r +10

halt (without power off), reboot, and poweroff.

upstart

Bilgisayarın açılışı sırasında olanlar

1. The server boots
2. The **init** process runs (usually as PID 1)
3. A predefined set of startup tasks activate in sequence

Bu ardışıl init süreçlerindeki sıkıntı dinamik olmaması, belli bir zaman almaları, değişiklikleri algılamalarında sıkıntı olması

Bunları çözmek için Upstart yaklaşımı getirilmiş

Upstart ile servis tanımları yaparken “job” tanımlamaları yapmamız gerekiyor.

job tanımlamalarındaki genel kurallar

- debian sistemlerde varsayılan “job” tanımlarının olduğu dizin /etc/init altıdır
- ls /etc/init: burada gördüğümüz conf dosya isimleri “job” isimleri
- initctl list komutunu veriyorum, burada gördüğüm job isimleri buradaki dosya isimleri ile aynıdır
- bir job ın olabileceği durumlar şu şekilde
- waiting: the initial state of processing
- **starting: where a job is about to start**
- **pre-start: where the pre-start section is loaded**
- **spawned: where a script section is about to run**
- **post-start: where post-start operations take place**
- **running: where the job is fully operational**

- **pre-stop: where pre-stop operations take place**
- **stopping: where the job is being stopped**
- **killed: where the job is stopped**
- **post-stop: where post-stop operations take place - to clean up**

bunların sıralamasını görebileceğimiz grafik
http://people.canonical.com/~jhunt/upstart/upstart-states-new.png veya
http://upstart.ubuntu.com/cookbook/ adresinde

burada üst kısımda detaylı olarak anlatıyor

- Her job tanımında exec veya sript ifadsi olmalı

exec /bin/foo --opt -xyz foo bar

```
script
   # do some stuff
   if [ ... ]; then
      ...
   fi
end script
```

script -> /bin/sh altında çalışacak betikleri içerir
pre-start script specifies the shell code to be run before the main process, as with script any command that fails will terminate the script and it is terminated with “end script”

```
pre-start script
   # prepare environment
   mkdir -p /var/run/foo
end script
```

post-stop script specifies the shell code to be run after the main process terminates or is killed, as with script and post-start script any command that fails will terminate the script and it is terminated with “end script”

```
post-stop script
   # clean up
   rm -rf /var/run/foo
end script
```

- start on ve stop on tanımlamaları ile ne zaman başlayıp öldürüleceğini söylüyoruz
    - hangi runlevellarda
    - yeniden başlatılırken napayım

örnek iki conf dosyası testjob.conf ve testjobadvanced.conf

bu örnekleri anlatırken init-checkconf komutunu çalıştırıp syntax hatası var mı diye kontrol etmekte fayda var

ssh servicine bakalım
respawn:
Bu ifade olmadan bir süreç sonlanınca, nasıl sonladığıdan bağımsız stop/waiting durumuna geçer
bunu yazınca eğer 0 döndürerek sonlanmazsa, tekrar başlatırlı
respawn 10 5
respawn the job up to 10 times within a 5 second period.
If the job exceeds these values, it will be stopped and
marked as failed.

umask
default umask : umask
default umask for files: 666
default umask for dir: 777

touch hede

systemd

ubuntu 14.04 upstart kullanıyor ve wiki sayfasındaki ppa deposunda trusty için durdurulmuş. Ubuntu systemd için 14.10 dan sonrasını önermiş. Dolayısı ile burada 14.10 kurmuş olmaları lazım

açıldıktan sonra

apt-get install systemd systemd libpam-systemd systemd-ui (sonuncusu şart değil)

/etc/default/grub içinde
GRUB_CMDLINE_LINUX_DEFAULT="init=/lib/systemd/systemd"
şeklinde bir değişiklik yapıyoruz

update-grub2

sonrasında açıldıktan sora dmesg | grep mtab ile oluşan hata durumunu görüyoruz

ln -fs /proc/self/mounts /etc/mtab

ile bunu düzeltiyoruz

sonrasında systemd1.sh dakileri sırası ile deneyebiliriz.

systemctl komutu sonrası

target, socket, service diye 3 tipte systemde tanımlamak mümkün

service: .service ile biten unit dosyaları, süreç kontrolü amaçlı
socket: .socket ile biten ve IPC, network socket ve FIFO kontrolleri için
target: grouping units

targetle ilgili aşağıda bir tablo var

systemctl komutunun altında da LOAD, ACTIVE ve SUB için açıklamalar var

systemctl list-unit-files

enabled: açılışta çalışsın
disabled: açılışta çalışmasın
masked: /dev/null a yönlendirilmiş dosyalar, bu sayede o servici hiç bir şekilde çalıştırmıyoruz
static: bağımlılık olarak tanımlanan servis

journalctl kullanımı ile ilgili systemdd2.sh

Örnek servis
/lib/systemd/system altına testjobadvanced.service olarak konulacak
bunu açıp okuyunca gerekli bazı bilgiler aşağıda var
ssh.service i açıp okuyalım
If set to process, only the main process itself is killed.
If set to mixed, the SIGTERM signal (see below) is sent to the main process while the subsequent SIGKILL signal (see below) is sent to all remaining processes of the unit's control group.
If set to none, no process is killed.

http://www.freedesktop.org/software/systemd/man/systemd.service.html

stanza

https://wiki.ubuntu.com/SystemdForUpstartUsers

Service types:

- Type=simple (default): *systemd* considers the service to be started up **immediately**. The **process must not fork**. Do not use this type if other services need to be ordered on this service, unless it is socket activated.
- Type=forking: *systemd* considers the service started up once the process forks and the parent has exited. **For classic daemons** use this type unless you know that it is not necessary. You should specify PIDFile= as well so *systemd* can keep track of the main process.
- Type=oneshot: this is useful for scripts that do a **single job and then exit**. You may want to set RemainAfterExit=yes as well so that *systemd* still considers the service as active after the process has exited.
- Type=notify: **identical to Type=simple, but with the stipulation that the daemon will send a signal to *systemd* when it is ready**. The reference implementation for this notification is provided by *libsystemd-daemon.so*.
- Type=dbus: the service is considered ready when the specified BusName appears on DBus's system bus.
- Type=idle: b**ehavior of idle is very similar to Type=simple; however, actual execution of the service binary is delayed until all jobs are dispatched**. This may be used to avoid interleaving of output of shell services with the status output on the console.

target table

SysV Runlevel	systemd Target	Notes
0	runlevel0.target, poweroff.target	Halt the system.
1, s, single	runlevel1.target, rescue.target	Single user mode.
2, 4	runlevel2.target, runlevel4.target,	User-defined/Site-specific runlevels. By default, identical to 3.

	multi-user.target	
3	runlevel3.target, multi-user.target	Multi-user, non-graphical. Users can usually login via multiple consoles or via the network.
5	runlevel5.target, graphical.target	Multi-user, graphical. Usually has all the services of runlevel 3 plus a graphical login.
6	runlevel6.target, reboot.target	Reboot
emergency	emergency.target	Emergency shell

Monitoring

top

top - 15:49:02 up 7 min, 1 user, load average: 0.01, 0.07, 0.05

ilk satır

aslında uptime ile gördüğümüz ve 5, 10,15 dakikalık load durumları

l ye basarak bu satırın kaybolup gözükmesini sağlıyoruz

%Cpu(s): 0.0 us, 1.6 sy, 0.0 ni, 98.4 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st

- Percentage of the CPU for user processes (0.3%**us**)
- Percentage of the CPU for system processes (0.0%**sy**)
- Percentage of the CPU processes with priority upgrade *nice* (0.0%**ni**)
- Percentage of the CPU not used (99,4%**id**)
- Percentage of the CPU processes waiting for I/O operations(0.0%**wa**)
- Percentage of the CPU serving hardware interrupts (0.3% **hi** — Hardware IRQ
- Percentage of the CPU serving software interrupts (0.0% **si** — Software Interrupts
- The amount of CPU ‘stolen’ from this virtual machine by the hypervisor for other tasks (such as running another virtual machine) this will be 0 on desktop and server without Virtual machine. (0.0%**st** — Steal Time)

cpu ekranı t ile açılıp kapatılabiliyor

memory kısmı
KiB Mem: 1017452 total, 261956 used, 755496 free, 36320 buffers
KiB Swap: 1045500 total, 0 used, 1045500 free. 164412 cached Mem

ilk satır free komutu çıktısı

varsayılan kb gösteriyor
free -m ile daha anlamlı bilgiye ulaşmak mümkün
ya da free -h

takas alanı kullanmıyor olmanız kullanıyorsanız o zaman bellekte bir arttırıma gitmeniz gerekiyor

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
36	root	20	0	0	0	0	S	0.3	0.0	0:00.34	kworker/1:1
37	root	20	0	0	0	0	S	0.3	0.0	0:01.45	kworker/0:1

- **PID** – l'ID of the process(4522)
- **USER** – The user that is the owner of the process (root)
- **PR** – priority of the process (15)
- **NI** – The "NICE" value of the process (0)
- **VIRT** – virtual memory used by the process (132m)
- **RES** – physical memory used from the process (14m)
- **SHR** – shared memory of the process (3204)
- **S** – indicates the status of the process: **S**=sleep **R**=running **Z**=zombie (S)
- **%CPU** – This is the percentage of CPU used by this process (0.3)
- **%MEM** – This is the percentage of RAM used by the process (0.7)
- **TIME+** –This is the total time of activity of this process (0:17.75)
- **COMMAND** – And this is the name of the process (bb_monitor.pl)

D - uninterruptible sleep
R - running
S - sleeping
T - traced or stopped
Z - zombie

diğer kullanım özellikleri

space veya enter ile refresh yapmak
ne kadar sıklıkla refresh yapacağını aslında h ye basarak görüyoruz varsayılan 3 snye
shift A ile 4 tipe göre sıralamayı göster
w ve a ile geçişler yap
veya g ile herhangi birine git

saniye refseh aralığını belirtmek için
s ve d ile değiştir

f ile seçilecek yeni alanları belirle

seçmek için d ye basıyoruz

sıralamak için sağ ok s ve sonrasında taşıyoruz

c ile full path gösterme ve saklama

Z ile yan seç enter de

küçük z ile toggle
x ile sort key belirlemece
y ile running process on off

u ile sadece belli bir kullanıcınınkileri gösterme

lsof

lsof -i

lsof -Pni
netstat -pantu ile hemen hemen aynı
lsof -iTCP
lsof -iUDP

lsof -i :22

lsof -i :20-100

belli bir ipden yapılan bağlantılar
lsof -i @10.0.2.2

oguzun eriştiği dosyalar
lsof -u oguz

negate - root olmayan kullanıcıların eriştiği dosyalar
lsof -u ^root

/var/log/ dizini altındaki dosyalara erişen tüm süreçleri listelemek için +d paramertesi kullanılabilir:

lsof +d /var/log

var log altındaki dizinlere ve tüm alt dizinlere erien dosyaların listesi
lsof +d /var/log

belli bir sürecin açtığı tüm dosyalar
lsof -p surec_no

buraya ps -efl grep ssh deyip ssh ın sürecini yaz

belli bir komutu çalıştıran tüm süreçlerin listesi

lsof -c bash

and ile birden fazla kriteri birleştirmek
lsof -i @10.0.2.2 -a -i :22

netstat

netstat -a

tüm tcp, udp ve unix socket bağlantılarını gösteriyor

sadece tcp bağlantılarını göster
netstat -at

sadece udp bağlantılarını göster
netstat -au

hostname çözümlemesi yapma

netstat -ant

sadece listen durumunda olan bağlantıları göster
netstat -ntl

surec numaralarını da göster
bu ne zaman işinize yarar? (80 de dinleyen var mı)
netstat -pntl

lsof ile nasıl yapardık?

add user name
netstat -ltpe

netstat -s
bağlantı yoğun sistemlerde established connection sayısı önemli olabilir

netstat -rn
route -n ile aynı

netstat -atnp | grep ESTA

sor bu nedir?
watch -d -n2 "netstat -atnp | grep ESTA"

check if a service is running
netstat -aple | grep ntp

sar

sudo apt-get install sysstat

sar -V

sar servisi için /etc/default/sysstat ayarı yapılıyor
/etc/cron.d/sysstat için de her 2 dakikada ayarı yapıp restart diyoruz

the system CPU statistics 3 times (with 1 second interval).
sar 1 3

sar -u

Linux 3.17.6RC1 (ab2015) 01/03/2015 _x86_64_ (2 CPU)

All the sar command will have the following as the 1st line in its output.

- Linux 2.6.18-194.el5PAE – Linux kernel version of the system.
- (dev-db) – The hostname
- 03/26/2011 – The date when the sar data was collected.
- _i686_ – The system architecture
- (8 CPU) – Number of CPUs available on this system. On multi core systems, this indicates the total number of cores.

sar komutunun bu istatikstkleri

- **sar -u** Displays CPU usage for the current day that was collected until that point.

bu istatistikler /etc/cron.d/sysstat altından alıyoruz

./sa1 1 1 çalıştırıp /var/log/sysstat altındaki dosyanın değiştiğini görelim

If you have 4 Cores on the machine and would like to see what the individual cores are doing, do the following.
sar -P ALL 1 1

sar -P ALL 1 1 1
sar -P 1 1 3 Displays real time CPU usage for core number 1, every 1 second for 3 times.

This reports the memory statistics. “1 3″ reports for every 1 seconds a total of 3 times. Most likely you’ll focus on “kbmemfree” and “kbmemused” for free and used memory.
sar -r 1 3

This reports the swap statistics. “1 3″ reports for every 1 seconds a total of 3 times. If the “kbswpused” and “%swpused” are at 0, then your system is not swapping.
sar -S 1 3

load average
sar -q 1 3

starting from 10 a.m, if you want to see 7 entries, you have to pipe the above output to “head -n 10″.i
sadd - dd indicates the day of the month

sar -q -f /var/log/sysstat/sa03 -s 10:00:01 | head -n 10

iostat

iostat

tek başına sadece cpu ve disk bilgisini gösteriyor tps: transferred per second

iostat -c
iostat -d
iostat -m
By default iostat displays I/O data for all the disks available in the system. To view statistics for # a specific device (For example, /dev/sda), use the option -p as shown below.
iostat -p sda
iostat 2 3
iostat 2

vmstat

vmstat

```
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so        bi        bo   in   cs us sy id wa st
 1  0      0 822944  34648 102480      0         0         70        5   19   35  0  0 98  2  0
```

- Procs – r: Total number of processes waiting to run
- Procs – b: Total number of busy processes
- Memory – swpd: Used virtual memory
- Memory – free: Free virtual memory
- Memory – buff: Memory used as buffers
- Memory – cache: Memory used as cache.
- Swap – si: Memory swapped from disk (for every second)
- Swap – so: Memory swapped to disk (for every second)
- IO – bi: Blocks in. i.e blocks received from device (for every second)
- IO – bo: Blocks out. i.e blocks sent to the device (for every second)
- System – in: Interrupts per second
- System – cs: Context switches
- CPU – us, sy, id, wa, st: CPU user time, system time, idle time, wait time

vmstat 2

vmstat 2 3

vmstat -s
tüm disk istatistikleri
vmstat -d
bir disk bölümüne ait istatistik
vmstat -p sda1

mpstat

by default cpu statistcis
mpstat

tüm işlemcilere ait istatistikler
mpstat -P ALL

mpstat -P 0
mpstat -P 1

w

$ w
 14:15:53 up 0 min, 1 user, load average: 0.96, 0.28, 0.09
USER TTY   FROM   LOGIN@   IDLE   JCPU   PCPU WHAT
oguz pts/1 10.0.2.2   14:15   1.00s 0.14s 0.00s w

1. **USER** - User name.
2. **TTY** - Terminal type such as pts/0 or console.
3. **FROM** - The remote host name or IP address.
4. **LOGIN@** - Login time.
5. **IDLE** - Idel time.
6. **JCPU** - The JCPU time is the time used by all processes attached to the tty.
7. **PCPU** - The PCPU time is the time used by the current process displayed in WHAT field.
8. **WHAT** - The command line of USER's current process.

#header surpress
w -h

#short output
w -s

display information about oguz
w oguz

ps

#The following command will give a full list of processes
ps -ef
for bsd style
ps ax

display processes for a special user
ps -f -u oguz

search process with a keyword and diplay the process id
ps -C bash

filter with process id
ps -f -p 1, 853

ps -ef | grep ssh

sort according to cpu or mem usage
ps aux --sort=-pmem | head -5

ps aux --sort=-pmem,+pcpu | head -5

display the process tree by searching a keyword
ps -f --forest -C apache2

filtering the columns
ps -o pid,uname,comm -C sshd
ps -o pid,uname,comm, time -C sshd

ps -p 1
all processes forked from the process id #1
ps --ppid 1

man ps ile standart format specifiers kısmından
ps -e -o pid,uname,pcpu,pmem,comm | less

elapsed time

ps -e -o pid,uname,pcpu,pmem,comm,etime | less

sor bunu
watch -n 1 'ps -e -o pid,uname,cmd,pmem,pcpu --sort=-pmem,-pcpu | head -15'

pstree

pstree

show parameters
pstree -a

show process ids
pstree -p

sort according to the procss id
pstree -np

display the user runningt the command
pstree -u

highlight the current process
pstree -h

highlight the process with this pid
pstree -H 865

add either username or process id to display that user or process' tree
pstree oguz
pstree 395

nagios3

commands.cfg -> makrolar http://nagios.sourceforge.net/docs/3_0/macrolist.html#hostname
contacts_nagios2.cfg:

contacts.cfg:

service_notification_options **w** = notify on WARNING service states, **u** = notify on UNKNOWN service states, **c** = notify on CRITICAL service states, **r** = notify on service recoveries (OK states), and **f** = notify when the service starts and stops flapping. If you specify **n** (none) as an option, the contact will not receive any type of service notifications

host_notification_options: **d** = notify on DOWN host states, **u** = notify on UNREACHABLE host states, **r** = notify on host recoveries (UP states), **f** = notify when the host starts and stops flapping, and **s** = send notifications when host or service scheduled downtime starts and ends. If you specify **n** (none) as an option, the contact will not receive any type of host notifications

flapping: flapping occurs when a service or host changes state too frequently

change email settings to myfancyemailtest@gmail.com

generic-host.cfg:
notification_interval: This directive is used to define the number of "time units" to wait before re-notifying a contact that this service is *still* down or unreachable
notification_period: http://nagios.sourceforge.net/docs/3_0/objectdefinitions.html#timeperiod
performancedata:

PING ok - Packet loss = 0%, RTA = 0.80 ms | percent_packet_loss=0, rta=0.80

When Nagios sees this plugin output format it will split the output into two parts:

1. Everything before the pipe character is considered to be the "normal" plugin output and will be stored in either the $HOSTOUTPUT$ or $SERVICEOUTPUT$ macro
2. Everything after the pipe character is considered to be the plugin-specific performance data and will be stored in the $HOSTPERFDATA$ or $SERVICEPERFDATA$ macro

networking

edit /etc/network/interfaces
sudo ifdown eth1 && sudo ifup eth0
ping -c 1 www.google.com

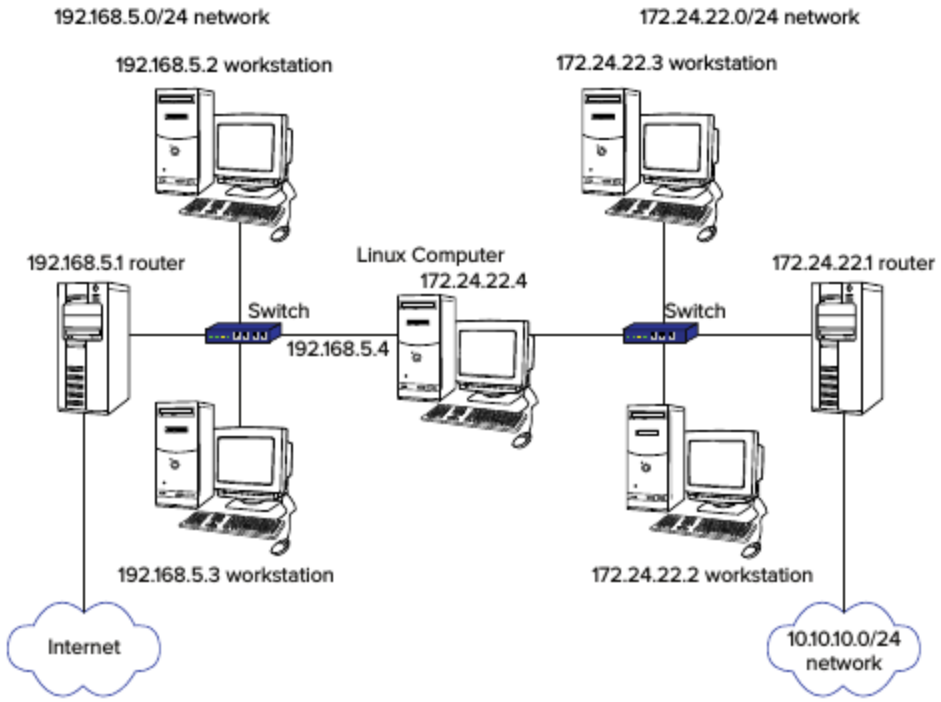
sudo cat /etc/resolv.conf
sudo route -n

konsolda yapmak isteseydik ayni şeyleri

sudo ifconfig eth1 address 192.168.156.110 netmask 255.255.255.0
sudo route add default gw 192.168.56.1

sudo ifconfig
sudo ifconfig eth0
sudo ifconfig eth1

hostname
deiştirmek için hostname yenisi
restart atıldığında set eidlmesi için /etc/hosts dosyası ve /etc/hostname dosyaları ellenmeli



burada 172 li ağdaki iki workstation varsayılan olarak internete çıkarken 192.168 .5.1 i gateway olarak görürken 10.10 içinse 172.24.22.1 i gw olarak görmektedir

burada yazılacak komut:

route add -net 10.10.10.0 netmask 255.255.255.0 gw 172.24.22.1

man route da kullanımına bakalım

Link computer farklı networkler arasında paket geçişine izin vermesi gerekiyor

echo “1” > /proc/sys/net/ipv4/ip_forward

/etc/sysctl.conf:

dosyasında
net.ipv4.ip_forward = 1

değeri değiştirilip sysctl -p /etc/sysctl.conf ile reload edilebilr

sudo sysctl -a ile konttol edilebilir

ALLINONE Command

ip addr show
veya ip a

sudo ip addr del 192.168.56.102/24 dev eth1
sudo ip addr add 192.168.56.110/24 dev eth1

sudo ip route show

route ekleme
sudo ip route add 10.10.20.0/24 via 192.168.50.110 dev eth1
sudo ip route del 10.10.20.0/24
sudo ip route add default via 192.168.50.110

make it static

interfaces dosyasının sonuna
up ip route add 10.10.20.0/24 via 192.168.50.110 dev eth1

network traffic monitoring

netcat

apt-get install netcat

random telnet type command sending, testing port connectivity

netcat -vz www.google.com 80
netcat -vt www.google.com 80
GET / HTTP/1.0
nc -l 9000
lsof -i :9000
nc localhost 9000
deneme

sending file

at the server side
nc -l 9000 > test
at the client side
cat testfile | nc localhost 9000

define v4 v6

nc -4 -l 9000
#lsof -i :9000

nc -6 -l 9000
#lsof -i :9000

keep up the server even the client is disconnected

nc -l 9000
nc localhost 9000
ctrl + c

then
#nc -k -l 9000
#nc localhost 9000
ctrl + c

udp

nc -u -4 -l 9000
lsof -i :9000

tcpdump

tcpdump -i eth0
tcpdump -i eth0 -nn
http://en.wikipedia.org/wiki/Transmission_Control_Protocol

IP ve TCP header başlıklarındaki ip,port, flag data kısımları

tcpdump -nn -i eth0 -c 5
filtering
tcpdump -nn -i eth0 -c 5 port 22
tcpdump -nn -i eth0 -c 5 host 10.0.2.2
tcpdump -nn -i eth0 -c 5 dst host 10.0.2.15
tcpdump -nn -i eth0 -c 5 host 10.0.2.2 -w tump.pcap

print header in hex format and tcp data in ascii
tcpdump -XX -nn -i eth1 -c 5 port 80

other protocols
tcpdump -nvvv -i any -c 2 icmp
test with ping

tcpdump -nnvvv -i any -c 2 udp
hping3 -2 192.168.56.102

udo hping3 -S 192.168.56.102 -p 80
hping3 -S www.google.com -p 80

nmap

nmap 192.168.56.1
nmap 192.168.56.1-10
nmap 192.168.56.0/24
nmal -iL iplistesi.txt

nmap -sP 192.168.56.1 - ping sweep, ping atarak sistemlerin açık ya da kapalılığını
nmap -PS 192.168.56.0/24 - TCP SYN ile ayakta olup olmadığına - port bilgisi de geldi
nmap -PA 192.168.56.0/24 - TCP ACK ile sistemlerin ayakta olup olmadığına
nmap -PU 192.168.56.0/24 - UDP paketleri ile ayakta olup olmadığına

SYN scan
nmap -sS 192.168.56.1 - gelen yanıt SYN + ACK ise port açık
nmap -sT - handshake kurulur

nmap -sU 192.168.56.1 - UDP scan

herhangi bir parametre vermezsek ilk 1000 portu kullanır

nmap -sS -F 192.168.56.1 - en yaygın 100 portu kullanır

nmap -sS -p80 192.168.56.1 - just port 80
nmap -sS -p80-150 192.168.56.1 - range
nmap -sS -p22,80,110 192.168.56.1 - 22 and 80 and 110
nmap -sS -p U:53,T:22 192.168.56.1 - udp 53, tcp 22
nmap -sS --top-ports 10 192.168.56.1 - en sık kullanılan 10 port

nmap -sS -sV --top-ports 10 192.168.56.1 - servis surumü
nmap -sS -O --top-ports 10 192.168.56.1 - işletim sistemi analizi
nmap -sS -A --top-ports 10 192.168.56.1 - işletim sistemi ve os analizi

problem çözme

tracepath -n ip_adresi - just display targets ip adress
netstat -ap | grep smtp
lsof -i
lsof -i :port numarası
logların incelenmesi
hostname -f
host www.google.com

dig @8.8.8.8 www.google.com - use server 8.8.8.8 and return ns records for www.google.com
dig www.google.com - use default dns and return ip adress of www.google.com

route -n
ifconfig
ip a