

Born2beroot detayına kadar öğrenme vol2

#####

<https://www.techtarget.com/searchnetworking/definition/TCP>

TCP (Transmission Control Protocol) İletim Kontrol Protokolü, Bağlantıya yönelik güvenli bir protokol. İletilecek veriler önce uygulama tarafından bir veri akışı olarak gönderilir, ardından işletim sistemi tarafından uygun biçime dönüştürülür.

TCP, verileri sunucu ve istemci arasında güvenli iletimi sağlayacak şekilde düzenlemek için kullanılır. Ağ üzerinden gönderilen verilerin, miktarı ne olursa olsun bütünlüğünü garanti eder. Bu nedenle, iletilen tüm verilerin ulaşmasını gerektiren diğer üst düzey protokollerden veri iletmek için kullanılır.

> Bu protokollerin örnekleri şunlardır:

> Güvenli Kabuk(**Secure Shell**) (SSH), Dosya Aktarım Protokolü(**File Transfer Protocol**) (FTP), Telnet: Eşler arası dosya paylaşımı ve Telnet'in durumunda, bir dosyaya erişmek için başka bir kullanıcının bilgisayarında oturum açmak için.

> Basit Posta Aktarım Protokolü(**Simple Mail Transfer Protocol**) (SMTP), Postane Protokolü(**Post Office Protocol**) (POP), İnternet İleti Erişim Protokolü(**Internet Message Access Protocol**) (IMAP): E-posta göndermek ve almak için.

> HTTP: Web erişimi için.

Bu örneklerin tümü, TCP/IP yığınının uygulama katmanında bulunur ve taşıma katmanındaki TCP'ye aşağı doğru veri gönderir.

TCP neden önemlidir?

> TCP önemlidir çünkü bilgilerin internet üzerinden iletilme şekline ilişkin kuralları ve standart prosedürleri belirler. Mevcut haliyle internetin temelidir ve ilgili yer, donanım veya yazılımdan bağımsız olarak veri iletiminin tek tip olarak yapılmasını sağlar.

> TCP esnektir ve yüksek düzeyde ölçeklenebilir, yani ona yeni protokoller eklenebilir ve bunları barındırır. Aynı zamanda tescilli değildir, yani hiç kimse veya şirket ona sahip değildir.

Location in the TCP/IP stack (TCP/IP yığınınındaki konum)

> TCP/IP yığını, verilerin TCP/IP protokolü kullanılarak ağlar üzerinden nasıl düzenlendiğini ve değiş tokuş edildiğini temsil eden bir modeldir. İstemciden sunucuya ve tersi yönde ilerlerken, verilerin bir dizi protokol tarafından işleme ve paketlenme biçimini temsil eden bir dizi katmanı tasvir eder.

> TCP, UDP gibi diğer protokollerle birlikte taşıma katmanında bulunur. Bu katmandaki protokoller, daha sınırlı hata kontrol kabiliyetine sahip olduğu için UDP

hariç, verilerin kaynağa hatasız iletimini sağlar.

Kurulan toplam bağlantı sayısını bulmamız isteniyor bu yüzden TCP insune değeri elde edilecektir.

- Aktif bağlantı sayısı.

```
ctcp=$(cat /proc/net/sockstat | awk '$1 == "TCP:" {print $3}')
```

```
#Connexions TCP: $ctcp ESTABLISHED
```

Aktif TCP bağlantılarına bakmak için bu kullanılabilir.

```
akaraca@akaraca42:~$ cat /proc/net/sockstat
sockets: used 80
TCP: inuse 2 orphan 0 tw 0 alloc 3 mem 1
UDP: inuse 1 mem 0
UDPLITE: inuse 0
RAW: inuse 0
FRAG: inuse 0 memory 0
```

Bağlantı sayısını bulmak için;

```
akaraca@akaraca42:~$ cat /proc/net/sockstat | awk '$1 == "TCP:" {print $3}'
2
```

TCP inuse, kurulan toplam bağlantı sayısını temsil ediyor.

TCP orphan(kimsesiz bırakılan, yetim, öksüz vs), artık,öksüz,yetim tcp bağlantıları temsil ediyor. (herhangi bir kullanıcı dosyası tanıtıcısına eklenmemiş)

TCP tw, TIME_WAIT bağlantıları

TCP alloc, Alloc: Ayrılan TCP soketleri (tüm türler) (allow types)

TCP mem, ??????????????

Ya da bu komut ilede bakılabilir.

```
akaraca@akaraca42:/usr/local/bin$ ss -s
Total: 80
TCP:    3 (estab 1, closed 0, orphaned 0, timewait 0)
```

Transport	Total	IP	IPv6
RAW	0	0	0
UDP	1	1	0
TCP	3	2	1
INET	4	3	1
FRAG	0	0	0

```
akaraca@akaraca42:/usr/local/bin$ ss -s | awk '$1 == "TCP" {print $3}'
2
```

Eğerki sadece sunucu üzerinden bağlantı kurarsam tek bir bağlantı olduğunu göreceğiz.

```
root@akaraca42:~# ss -s
Total: 74
TCP:    2 (estab 0, closed 0, orphaned 0, timewait 0)
```

Transport	Total	IP	IPv6
RAW	0	0	0
UDP	1	1	0
TCP	2	1	1
INET	3	2	1
FRAG	0	0	0

```
root@akaraca42:~# ss -s | awk '$1 == "TCP" {printf $3}'
1root@akaraca42:~# _
```

```
root@akaraca42:~# bash /usr/local/bin/monitoring.sh
Broadcast message from root@akaraca42 (tty1) (Thu Mar 24 06:03:14 2022):

    #Architecture: Linux akaraca42 5.10.0-12-amd64 #1 SMP Debian 5.10.103-1 (2022-03-07) x86_64
GNU/Linux
    #CPU physical: 1
    #vCPU: 2
    #Memory Usage: 72/1982MB (3.64%)
    #Disk Usage: 1590/28Gb (6%)
    #CPU load: 3.2%
    #Last boot: 2022-03-24 04:59
    #LVM use: yes
    #Connexions TCP: 1 ESTABLISHED
    #User log: 1
    #Network: IP 10.0.2.15 (08:00:27:ee:c6:71)
    #Sudo: 272 cmd
```

#####

- Sunucuyu kullanan kullanıcı sayısı.

```
u$log=$(users | wc -w)
```

```
#User log: $u$log
```

Kullanıcı sayısını bulmak için;

```
akaraca@akaraca42:~$ users
akaraca
akaraca@akaraca42:~$ users | wc
      1      1      8
akaraca@akaraca42:~$ users | wc -l
1
akaraca@akaraca42:~$ users | wc -w
1

Broadcast message from root@akaraca42 (somewhere) (Thu Mar 24 06:00:01 2022):

    #Architecture: Linux akaraca42 5.10.0-12-amd64 #1 SMP Debian 5.10.103-1 (2022-03-07) x86_64 GNU/Linux
    #CPU physical: 1
    #vCPU: 2
    #Memory Usage: 73/1982MB (3.71%)
    #Disk Usage: 1590/28Gb (6%)
    #CPU load: 3.2%
    #Last boot: 2022-03-24 04:59
    #LVM use: yes
    #Connexions TCP: 2 ESTABLISHED
    #User log: 1
    #Network: IP 10.0.2.15 (08:00:27:ee:c6:71)
    #Sudo: 270 cmd
```

Sunucu üzerinden root kullanıcısına girerek artış gerçekleşiyor mu kontrol ettim.

```
akaraca@akaraca42:~$ users
akaraca root
akaraca@akaraca42:~$ users | wc
  1    2   13
akaraca@akaraca42:~$ users | wc -l
1
akaraca@akaraca42:~$ users | wc -w
2

Broadcast message from root@akaraca42 (somewhere) (Thu Mar 24 06:02:01 2022):

    #Architecture: Linux akaraca42 5.10.0-12-amd64 #1 SMP Debian 5.10.103-1 (2022-03-07) x86_64 GNU/Linux
    #CPU physical: 1
    #vCPU: 2
    #Memory Usage: 77/1982MB (3.91%)
    #Disk Usage: 1590/28Gb (6%)
    #CPU load: 3.2%
    #Last boot: 2022-03-24 04:59
    #LVM use: yes
    #Connexions TCP: 2 ESTABLISHED
    #User log: 2
    #Network: IP 10.0.2.15 (08:00:27:ee:c6:71)
    #Sudo: 271 cmd
```

#####

- Sunucunun IPv4 ve MAC (Media Access Control) adresleri.

```
ip=$(hostname -I)
```

```
mac=$(ip link show | awk '$1 == "link/ether" {print $2}')
```

```
#Network: IP $ip ($mac)
```

Sunucunun IP adresini çekmek için;

```

akaraca@akaraca42:~$ hostname
akaraca42
akaraca@akaraca42:~$ hostname --help
Usage: hostname [-b] {hostname|-F file}      set host name (from file)
        hostname [-a|-A|-d|-f|-i|-I|-s|-y]    display formatted name
        hostname                               display host name

        {yp,nis,}domainname {nisdomain|-F file} set NIS domain name (from file)
        {yp,nis,}domainname                  display NIS domain name

        dnsdomainname                        display dns domain name

        hostname -V|--version|-h|--help      print info and exit

Program name:
        {yp,nis,}domainname=hostname -y
        dnsdomainname=hostname -d

Program options:
        -a, --alias                alias names
        -A, --all-fqdns            all long host names (FQDNs)
        -b, --boot                 set default hostname if none available
        -d, --domain               DNS domain name
        -f, --fqdn, --long         long host name (FQDN)
        -F, --file                 read host name or NIS domain name from given file
        -i, --ip-address           addresses for the host name
        -I, --all-ip-addresses     all addresses for the host
        -s, --short                short host name
        -y, --yp, --nis            NIS/YP domain name

```

"hostname -I" komutu ile tüm ip adreslerini görüntülemek için;

```

akaraca@akaraca42:~$ hostname -I
10.0.2.15

```

MAC adreslerini görüntülemek için;

```

akaraca@akaraca42:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
   link/ether 08:00:27:ee:c6:71 brd ff:ff:ff:ff:ff:ff

```

```
akaraca@akaraca42:~$ ip addr show
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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:ee:c6:71 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 82057sec preferred_lft 82057sec
    inet6 fe80::a00:27ff:feee:c671/64 scope link
        valid_lft forever preferred_lft forever
```

lo, geri döngü arabirimidir(**loopback interface**). Bu, sistemin kendi kendisiyle iletişim kurmak için kullandığı özel bir ağ arabirimidir.

ether: Bir ağa bağlanmak için kimlik doğrulama prosedürünün bir parçası olarak gerekli olabilecek arayüzünüzün donanım adresi "ether" ile işaretlenmiştir.

Mac ve **IP adresleri**, ağa bağlı olan cihazı tanımlar. **Mac**, bilgisayarın ev adresimiz gibi fiziksel adresidir. Böylece bir ağda, bir **Mac adresi** kullanılarak çeşitli cihazlar tanımlanabilir. **IP adresi** ise ağ bağlantısını bir sayı vererek tanımlar.

MAC adresini çekmek için;

```
akaraca@akaraca42:~$ ip link show | awk '$1 == "link/ether" {print $2}'
08:00:27:ee:c6:71
```

#####

- sudo ile çalıştırılmış komut sayısı.

```
cmds=$(journalctl _COMM=sudo | grep COMMAND | wc -l)
```

```
#Sudo: $cmds cmd"
```

journalctl, systemd'nin günlük kaydı hizmeti olan Journald'den günlükleri sorgulamak ve görüntülemek için bir yardımcı programdır. Journald, günlük verilerini düz metin biçimi yerine ikili biçimde sakladığından, Journalctl, Journald tarafından işlenen günlük mesajlarını okumanın standart yoludur.

```

akaraca@akaraca42:~$ journalctl
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
-- Journal begins at Thu 2022-03-17 07:05:10 EDT, ends at Thu 2022-03-24 06:06:45 EDT. --
Mar 17 07:05:10 akaraca42 su[544]: (to root) akaraca on tty1
Mar 17 07:05:10 akaraca42 su[544]: pam_unix(su:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 07:05:25 akaraca42 su[544]: pam_unix(su:session): session closed for user root
Mar 17 07:06:17 akaraca42 su[552]: pam_unix(su:auth): authentication failure; logname=akaraca uid=1000 euid=0 tty=tty1 ruser=akaraca
Mar 17 07:06:20 akaraca42 su[552]: FAILED SU (to root) akaraca on tty1
Mar 17 07:06:28 akaraca42 su[554]: (to root) akaraca on tty1
Mar 17 07:06:28 akaraca42 su[554]: pam_unix(su:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 07:36:21 akaraca42 su[554]: pam_unix(su:session): session closed for user root
Mar 17 07:38:01 akaraca42 sudo[679]: akaraca : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/visudo
Mar 17 07:38:01 akaraca42 sudo[679]: pam_unix(sudo:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 07:42:56 akaraca42 sudo[679]: pam_unix(sudo:session): session closed for user root
Mar 17 07:58:15 akaraca42 sudo[697]: pam_unix(sudo:auth): authentication failure; logname=akaraca uid=1000 euid=0 tty=/dev/tty
Mar 17 07:58:23 akaraca42 sudo[697]: akaraca : 3 incorrect password attempts ; TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sb
Mar 17 08:07:42 akaraca42 sudo[704]: pam_unix(sudo:auth): authentication failure; logname=akaraca uid=1000 euid=0 tty=/dev/tty
Mar 17 08:07:52 akaraca42 sudo[704]: akaraca : 3 incorrect password attempts ; TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sb
Mar 17 08:08:04 akaraca42 sudo[706]: pam_unix(sudo:auth): authentication failure; logname=akaraca uid=1000 euid=0 tty=/dev/tty
Mar 17 08:08:12 akaraca42 sudo[706]: akaraca : 3 incorrect password attempts ; TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sb
Mar 17 08:11:36 akaraca42 sudo[710]: pam_unix(sudo:auth): authentication failure; logname=akaraca uid=1000 euid=0 tty=/dev/tty
Mar 17 08:11:44 akaraca42 sudo[710]: akaraca : TTY=tty1 ; PWD=/var/log ; USER=root ; TSID=000001 ; COMMAND=/usr/bin/mkdir sudo

```

sudo ile ilgili yapılan işlemleri sıralar.

```

Mar 17 08:26:17 akaraca42 sudo[813]: akaraca : TTY=tty1 ; PWD=/ ; USER=root ; TSID=000008 ; COMMAND=/usr/bin/apt-get install vim
Mar 17 08:26:17 akaraca42 sudo[813]: pam_unix(sudo:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 08:26:22 akaraca42 sudo[813]: pam_unix(sudo:session): session closed for user root
Mar 17 08:27:13 akaraca42 sudo[933]: akaraca : TTY=tty1 ; PWD=/ ; USER=root ; TSID=000009 ; COMMAND=/usr/bin/apt-get install vim
Mar 17 08:27:13 akaraca42 sudo[933]: pam_unix(sudo:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 08:27:14 akaraca42 sudo[933]: pam_unix(sudo:session): session closed for user root
Mar 17 08:28:13 akaraca42 sudo[939]: akaraca : TTY=tty1 ; PWD=/ ; USER=root ; TSID=00000A ; COMMAND=/usr/bin/vim /etc/pam.d/common-password
Mar 17 08:28:13 akaraca42 sudo[939]: pam_unix(sudo:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 08:29:51 akaraca42 sudo[939]: pam_unix(sudo:session): session closed for user root
Mar 17 08:31:29 akaraca42 sudo[945]: akaraca : TTY=tty1 ; PWD=/ ; USER=root ; TSID=00000B ; COMMAND=/usr/bin/apt-get install libpam-pwquality
Mar 17 08:31:29 akaraca42 sudo[945]: pam_unix(sudo:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 08:31:31 akaraca42 sudo[945]: pam_unix(sudo:session): session closed for user root
Mar 17 08:32:28 akaraca42 sudo[1090]: akaraca : TTY=tty1 ; PWD=/ ; USER=root ; TSID=00000C ; COMMAND=/usr/bin/apt-get install libpam-pwquality
Mar 17 08:32:28 akaraca42 sudo[1090]: pam_unix(sudo:session): session opened for user root(uid=0) by akaraca(uid=1000)
Mar 17 08:32:29 akaraca42 sudo[1090]: pam_unix(sudo:session): session closed for user root
Mar 17 08:33:32 akaraca42 sudo[1096]: akaraca : TTY=tty1 ; PWD=/ ; USER=root ; TSID=00000D ; COMMAND=/usr/bin/vim /etc/pam.d/common-password
Mar 17 08:33:32 akaraca42 sudo[1096]: pam_unix(sudo:session): session opened for user root(uid=0) by akaraca(uid=1000)

```

Komut satırı içerisinde sudo ile yapılan işlemleri sıralar.

```

akaraca@akaraca42:~$ journalctl _COMM=sudo | grep COMMAND
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.
Mar 17 07:38:01 akaraca42 sudo[679]: akaraca : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/visudo
Mar 17 07:58:23 akaraca42 sudo[697]: akaraca : 3 incorrect password attempts ; TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/visudo
Mar 17 08:07:52 akaraca42 sudo[704]: akaraca : 3 incorrect password attempts ; TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/groupadd user42
Mar 17 08:08:12 akaraca42 sudo[706]: akaraca : 3 incorrect password attempts ; TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/visudo
Mar 17 08:11:44 akaraca42 sudo[710]: akaraca : TTY=tty1 ; PWD=/var/log ; USER=root ; TSID=000001 ; COMMAND=/usr/bin/mkdir sudo
Mar 17 08:11:56 akaraca42 sudo[715]: akaraca : TTY=tty1 ; PWD=/var/log ; USER=root ; TSID=000002 ; COMMAND=/usr/bin/mkdir sudo
Mar 17 08:13:27 akaraca42 sudo[726]: akaraca : TTY=tty1 ; PWD=/var/log/sudo ; USER=root ; TSID=000003 ; COMMAND=/usr/bin/cat sudo.log
Mar 17 08:13:46 akaraca42 sudo[731]: akaraca : TTY=tty1 ; PWD=/var/log ; USER=root ; TSID=000004 ; COMMAND=/usr/bin/rm -rf sudo

```

Kaç komut kullanıldığı görüntülenir.

```

akaraca@akaraca42:~$ journalctl _COMM=sudo | grep COMMAND | wc -l
Hint: You are currently not seeing messages from other users and the system.
      Users in groups 'adm', 'systemd-journal' can see all messages.
      Pass -q to turn off this notice.

```


sudo systemctl status ssh nedir?

> Yönetici izni sistem hizmet bilgilerini kullanarak güvenli kabuk hakkında bilgileri çekmeyi amaçlar.

systemctl nedir?

> Systemctl, systemd ve hizmetleri kontrol etmek ve yönetmek için kullanılan bir Linux komut satırı yardımcı programıdır. Systemctl'yi Systemd init hizmeti için bir kontrol arayüzü olarak düşünebilirsiniz, systemd ile iletişim kurmanıza ve işlemleri gerçekleştirmenize izin verir. Systemctl, Init'in halefidir.

```
akaraca@akaraca42:~$ systemctl
```

UNIT	LOAD	ACTIVE	SUB	DESCRIPTION
proc-sys-fs-binfmt-misc.automount	loaded	active	waiting	Arbitrary Executable File Formats File System Auto
sys-devices-pci0000:00-0000:00:01.1-ata2-host2-target2:0:0-2:0:0:0-block-sr0.device	loaded	active	plugged	VBOX_CD-ROM
sys-devices-pci0000:00-0000:00:03.0-net-enp0s3.device	loaded	active	plugged	82540EM Gigabit Ethernet Controller (PRO/1000 MT DS
sys-devices-pci0000:00-0000:00:05.0-sound-card0-controlC0.device	loaded	active	plugged	/sys/devices/pci0000:00/0000:00:05.0/sound/card0/cs
sys-devices-pci0000:00-0000:00:0d.0-ata3-host1-target1:0:0-1:0:0:0-block-sda-sda1.device	loaded	active	plugged	VBOX_HARDDISK 1
sys-devices-pci0000:00-0000:00:0d.0-ata3-host1-target1:0:0-1:0:0:0-block-sda-sda2.device	loaded	active	plugged	VBOX_HARDDISK 2
sys-devices-pci0000:00-0000:00:0d.0-ata3-host1-target1:0:0-1:0:0:0-block-sda-sda5.device	loaded	active	plugged	VBOX_HARDDISK 5
sys-devices-pci0000:00-0000:00:0d.0-ata3-host1-target1:0:0-1:0:0:0-block-sda.device	loaded	active	plugged	VBOX_HARDDISK
sys-devices-platform-serial8250-tty-ttyS0.device	loaded	active	plugged	/sys/devices/platform/serial8250/tty/ttyS0
sys-devices-platform-serial8250-tty-ttyS1.device	loaded	active	plugged	/sys/devices/platform/serial8250/tty/ttyS1
sys-devices-platform-serial8250-tty-ttyS2.device	loaded	active	plugged	/sys/devices/platform/serial8250/tty/ttyS2
sys-devices-platform-serial8250-tty-ttyS3.device	loaded	active	plugged	/sys/devices/platform/serial8250/tty/ttyS3
sys-devices-virtual-block-dm\x2d0.device	loaded	active	plugged	/sys/devices/virtual/block/dm-0
sys-devices-virtual-block-dm\x2d1.device	loaded	active	plugged	/sys/devices/virtual/block/dm-1
sys-devices-virtual-block-dm\x2d2.device	loaded	active	plugged	/sys/devices/virtual/block/dm-2
sys-devices-virtual-block-dm\x2d3.device	loaded	active	plugged	/sys/devices/virtual/block/dm-3
sys-devices-virtual-block-dm\x2d4.device	loaded	active	plugged	/sys/devices/virtual/block/dm-4
sys-devices-virtual-block-dm\x2d5.device	loaded	active	plugged	/sys/devices/virtual/block/dm-5
sys-devices-virtual-block-dm\x2d6.device	loaded	active	plugged	/sys/devices/virtual/block/dm-6
sys-devices-virtual-block-dm\x2d7.device	loaded	active	plugged	/sys/devices/virtual/block/dm-7
sys-module-configfs.device	loaded	active	plugged	/sys/module/configfs
sys-module-fuse.device	loaded	active	plugged	/sys/module/fuse
sys-subsystem-net-devices-enp0s3.device	loaded	active	plugged	82540EM Gigabit Ethernet Controller (PRO/1000 MT DS
-.mount	loaded	active	mounted	Root Mount
boot.mount	loaded	active	mounted	/boot
dev-hugepages.mount	loaded	active	mounted	Huge Pages File System

```

akaraca@akaraca42:~$ systemctl status
● akaraca42
   State: running
   Jobs: 0 queued
   Failed: 0 units
   Since: Fri 2022-03-25 03:20:27 EDT; 4min 18s ago
   CGroup: /
└─user.slice
    └─user-1000.slice
        └─user@1000.service
            └─init.scope
                └─598 /lib/systemd/systemd --user
                └─599 (sd-pam)
            └─session-1.scope
                └─595 sshd: akaraca [priv]
                └─608 sshd: akaraca@pts/0
                └─609 -bash
                └─612 systemctl
                └─613 pager
                └─615 systemctl status
                └─616 pager
                └─624 systemctl
                └─625 pager
                └─628 systemctl status
                └─629 pager
    └─init.scope
        └─1 /sbin/init
    └─system.slice
        └─systemd-udevd.service
            └─339 /lib/systemd/systemd-udevd
        └─cron.service
            └─550 /usr/sbin/cron -f
        └─systemd-journald.service
            └─317 /lib/systemd/systemd-journald
        └─ssh.service
            └─593 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
        └─rsyslog.service
            └─554 /usr/sbin/rsyslogd -n -iNONE
        └─ifup@enp0s3.service
            └─540 /sbin/dhclient -4 -v -i -pf /run/dhclient.enp0s3.pid -lf /var/lib/dhcp/dhclient.enp0s3.leases -I -df /var/lib/dhcp/dhclient6.enp0s3.leases enp0s3
        └─dbus.service
            └─551 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
        └─systemd-timesyncd.service
            └─532 /lib/systemd/systemd-timesyncd
        └─system-getty.slice
            └─getty@tty1.service
                └─592 /sbin/agetty -o -p -- \u --noclear tty1 linux
        └─systemd-logind.service
            └─555 /lib/systemd/systemd-logind

```

```

akaraca@akaraca42:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-03-25 03:20:31 EDT; 4min 30s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 590 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 593 (sshd)
    Tasks: 1 (limit: 2336)
   Memory: 6.1M
      CPU: 68ms
   CGroup: /system.slice/ssh.service
           └─593 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Warning: some journal files were not opened due to insufficient permissions.

```

```
akaraca@akaraca42:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-03-25 03:20:31 EDT; 4min 46s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 590 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 593 (sshd)
    Tasks: 1 (limit: 2336)
   Memory: 6.1M
      CPU: 68ms
  CGroup: /system.slice/ssh.service
          └─593 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Mar 25 03:20:31 akaraca42 systemd[1]: Starting OpenBSD Secure Shell server...
Mar 25 03:20:31 akaraca42 sshd[593]: Server listening on 0.0.0.0 port 4242.
Mar 25 03:20:31 akaraca42 sshd[593]: Server listening on :: port 4242.
Mar 25 03:20:31 akaraca42 systemd[1]: Started OpenBSD Secure Shell server.
Mar 25 03:20:52 akaraca42 sshd[595]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.2.2 user=akaraca
Mar 25 03:20:54 akaraca42 sshd[595]: Failed password for akaraca from 10.0.2.2 port 53289 ssh2
Mar 25 03:20:58 akaraca42 sshd[595]: Accepted password for akaraca from 10.0.2.2 port 53289 ssh2
Mar 25 03:20:58 akaraca42 sshd[595]: pam_unix(sshd:session): session opened for user akaraca(uid=1000) by (uid=0)
```