

- Part 1. Установка ОС
- Part 2. Создание пользователя
- Part 3. Настройка сети ОС
- Part 4. Обновление ОС
- Part 5. Использование команды sudo
- Part 6. Установка и настройка службы времени
- Part 7. Установка и использование текстовых редакторов
- Part 8. Установка и базовая настройка сервиса SSHD
- Part 9. Установка и использование утилит top, htop
- Part 10. Использование утилиты fdisk
- Part 11. Использование утилиты df
- Part 12. Использование утилиты du
- Part 13. Установка и использование утилиты ncdu
- Part 14. Работа с системными журналами
- Part 15. Использование планировщика заданий CRON

## Part 1. Установка ОС

---

- Команда для вывода версии Ubuntu:

```
~$ cat /etc/issue.net
```

```
cranbero@winvairu:~$ cat /etc/issue.net
Ubuntu 20.04.6 LTS
cranbero@winvairu:~$ _
```

## Part 2. Создание пользователя

---

Создание пользователя, отличного от созданного при установке и добавление его в группу **adm**:

1. Создаем нового пользователя с помощью команды **useradd**. В качестве примера создадим пользователя с именем **newuser**:

```
~$ sudo useradd -m newuser
```

Параметр **-m** указывает на то, что домашняя директория пользователя должна быть создана автоматически.

2. Добавляем нового пользователя в группу **adm**:

```
~$ usermod -aG adm newuser
```

Параметр **-a** указывает на то, что пользователь должен быть добавлен в группу, даже если он уже входит в эту группу. Параметр **-G** используется для добавления пользователя в одну или несколько групп.

3. Проверяем, был ли пользователь успешно добавлен в группу **adm**:

```
~$ cat /etc/passwd
```

```
cranbero@winvairu:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:112:/:run/uidd:/usr/sbin/nologin
tcpdump:x:108:113:/:nonexistent:/usr/sbin/nologin
landscape:x:109:115:/:var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:/:var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
cranbero:x:1000:1000:cranbero:/home/cranbero:/bin/bash
lxd:x:998:100:/:var/snap/lxd/common/lxd:/bin/false
newuser:x:1001:1001:,,,:/home/newuser:/bin/bash
cranbero@winvairu:~$ _
```

## Part 3. Настройка сети ОС

1. Изменение название машины вида user-1:

```
~$ hostnamectl set-hostname winvairu-1
```

```

newuser:x:1001:1001:,,,:/home/newuser:/bin/bash
cranbero@winvairu:~$ hostnamectl
  Static hostname: winvairu
        Icon name: computer-vm
        Chassis: vm
        Machine ID: 49c7ad599b0f4a5ca883dce1da474ab5
        Boot ID: 47d8a7ad0a664c86b4365067f3912419
        Virtualization: oracle
        Operating System: Ubuntu 20.04.6 LTS
        Kernel: Linux 5.4.0-186-generic
        Architecture: x86-64
cranbero@winvairu:~$ hostnamectl set-hostname winvairu-1
==== AUTHENTICATING FOR org.freedesktop.hostname1.set-static-hostname ====
Authentication is required to set the statically configured local host name, as well as the pretty host name.
Authenticating as: cranbero
Password: Could not set property: Method call timed out
cranbero@winvairu:~$ polkit-agent-helper-1: pam_authenticate failed: Authentication failure
hostnamectl set-hostn^C
cranbero@winvairu:~$ hostnamectl set-hostname winvairu-1
==== AUTHENTICATING FOR org.freedesktop.hostname1.set-static-hostname ====
Authentication is required to set the statically configured local host name, as well as the pretty host name.
Authenticating as: cranbero
Password:
==== AUTHENTICATION COMPLETE ====
cranbero@winvairu:~$ hostnamectl
  Static hostname: winvairu-1
        Icon name: computer-vm
        Chassis: vm
        Machine ID: 49c7ad599b0f4a5ca883dce1da474ab5
        Boot ID: 47d8a7ad0a664c86b4365067f3912419
        Virtualization: oracle
        Operating System: Ubuntu 20.04.6 LTS
        Kernel: Linux 5.4.0-186-generic
        Architecture: x86-64
cranbero@winvairu:~$

```

## 2. Установка временной зоны, по моему местоположению:

~\$timedatectl set-timezone Europe/Moscow

```

cranbero@winvairu-1:~$ timedatectl
  Local time: Thu 2024-06-20 07:08:46 UTC
  Universal time: Thu 2024-06-20 07:08:46 UTC
        RTC time: Thu 2024-06-20 07:08:47
        Time zone: Etc/UTC (UTC, +0000)
System clock synchronized: yes
        NTP service: active
        RTC in local TZ: no
cranbero@winvairu-1:~$ sudo timedatectl set-timezone Europe/Moscow
[sudo] password for cranbero:
Sorry, try again.
[sudo] password for cranbero:
Sorry, try again.
[sudo] password for cranbero:
cranbero@winvairu-1:~$ timedatectl
  Local time: Thu 2024-06-20 10:12:13 MSK
  Universal time: Thu 2024-06-20 07:12:13 UTC
        RTC time: Thu 2024-06-20 07:12:13
        Time zone: Europe/Moscow (MSK, +0300)
System clock synchronized: yes
        NTP service: active
        RTC in local TZ: no
cranbero@winvairu-1:~$ _

```

## 3. Консольная команда для вывода сетевых интерфейсов:

~\$ip link

```
cranbero@winvairu-1:~$ 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 fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:c9:b3:2e brd ff:ff:ff:ff:ff:ff
cranbero@winvairu-1:~$ _
```

- **lo** - это loopback интерфейс, который используется для обращения к самому себе внутри системы;
- **enp0s3** - это Ethernet интерфейс, подключенный к сети.

4. Консольная команда для получения ip адреса моего рабочего устройства от DHCP сервера:

- **~\$ip a**

```
cranbero@winvairu-1:~$ 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c9:b3:2e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 80627sec preferred_lft 80627sec
    inet6 fe80::a00:27ff:fec9:b32e/64 scope link
        valid_lft forever preferred_lft forever
cranbero@winvairu-1:~$ _
```

- В данном примере IP-адрес 10.0.2.15 был получен устройством через DHCP для интерфейса enp0s3.

DHCP - это сокращение от Dynamic Host Configuration Protocol, что в переводе с английского означает "протокол динамической конфигурации хостов". Это стандартный протокол, используемый в компьютерных сетях для автоматического назначения IP-адресов подключенным устройствам.

Протокол DHCP работает следующим образом: когда устройство подключается к сети, оно отправляет запрос на специальный сервер DHCP, который назначает ему IP-адрес, маску подсети, адрес шлюза по умолчанию и другие необходимые параметры. После этого устройство может полноценно участвовать в работе сети.

Преимущество использования DHCP заключается в том, что администраторам сетей не нужно вручную настраивать каждое устройство, чтобы оно могло работать в сети. Кроме того, DHCP

позволяет легко управлять IP-адресами в сети, переназначая их при необходимости.

## 5. Определение и вывод на экран внешнего ip-адреса шлюза (ip) и внутреннего IP-адреса шлюза, он же ip-адрес по умолчанию (gw):

- получения внешнего IP-адреса шлюза

```
~$curl ip.me
```

```
cranbero@winvairu-1:~$ curl ip.me
178.207.154.253
cranbero@winvairu-1:~$ _
```

- получение внутреннего IP-адреса шлюза (IP-адрес по умолчанию)

```
~$ip route show default
```

```
cranbero@winvairu-1:~$ ip route show default
default via 10.0.2.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 100
cranbero@winvairu-1:~$
```

## 6. Статичные (заданные вручную, а не полученные от DHCP сервера) настройки ip, gw, dns (используются публичные DNS серверы, например 1.1.1.1 или 8.8.8.8).

Настроить все сетевые параметры можно 2-мя способами:

- командами;
- редактированием конфигурационных файлов.

При использовании команд все настройки удаляются после перезагрузки системы. Поэтому, если нет необходимости держать выставленные настройки в течении долгого времени, то лучше воспользоваться командами.

Рассмотрим вариант настройки сети в конфигурационном файле:

- редактируем файл `etc/netplan/*.yaml`, после редактирования файл выглядит так:

```
# This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses:
        - 10.0.2.15/24
      routes:
        - to: default
          via: 10.0.2.2
      nameservers:
        search: [ya.ru]
        addresses: [1.1.1.1, 8.8.8.8]
```

- Применяем изменения, выполнив команду:

```
~$sudo netplan apply
```

- Перезагружаем виртуальную машину.
- Успешно пропингуем удаленные хосты 1.1.1.1 и ya.ru:

```
~$ping -c 4 1.1.1.1
```

```
~$ping -c 4 ya.ru
```

`-c 4` указывает отправить 4 пакета (некоторые реализации позволяют указать количество пакетов до бесконечности, используя `-c -1`).

`ya.ru` - это имя хоста, которое будет преобразовано в IP-адрес с помощью DNS.

```
cranbero@winvairu-1:~$ ping -c 4 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=63 time=24.2 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=63 time=24.0 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=63 time=23.5 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=63 time=23.4 ms

--- 1.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 23.376/23.764/24.154/0.314 ms
cranbero@winvairu-1:~$ ping -c 4 ya.ru
PING ya.ru (5.255.255.242) 56(84) bytes of data.
64 bytes from ya.ru (5.255.255.242): icmp_seq=1 ttl=63 time=29.1 ms
64 bytes from ya.ru (5.255.255.242): icmp_seq=2 ttl=63 time=17.8 ms
64 bytes from ya.ru (5.255.255.242): icmp_seq=3 ttl=63 time=17.9 ms
64 bytes from ya.ru (5.255.255.242): icmp_seq=4 ttl=63 time=17.8 ms

--- ya.ru ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 17.822/20.652/29.065/4.857 ms
cranbero@winvairu-1:~$
```

## Part 4. Обновление ОС

- Консольная команда для обновления системных пакетов:

```
~$sudo apt update && sudo apt full-upgrade -y
```

```
cranbero@winvairu-1:~$ sudo apt update && sudo apt full-upgrade -y
Hit:1 http://ru.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://ru.archive.ubuntu.com/ubuntu focal-updates InRelease [128 kB]
Hit:3 http://ru.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu focal-security InRelease
Get:5 http://ru.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [3,361 kB]
Get:6 http://ru.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [2,996 kB]
Get:7 http://ru.archive.ubuntu.com/ubuntu focal-updates/restricted Translation-en [419 kB]
Get:8 http://ru.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [1,194 kB]
Get:9 http://ru.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 Packages [27.1 kB]
Get:10 http://ru.archive.ubuntu.com/ubuntu focal-updates/multiverse Translation-en [7,936 B]
Fetched 8,132 kB in 2s (3,880 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
cranbero@winvairu-1:~$
```

## Part 5. Использование команды sudo

---

1. Разрешаем пользователю **newuser** выполнять команду **sudo**:

```
~$usermod -aG sudo newuser
```

Команда **sudo** в **Linux** используется для предоставления пользователям возможности выполнять команды от имени другого пользователя, обычно с правами суперпользователя **root**. Это позволяет пользователям решать задачи, требующие административных привилегий, без необходимости работать напрямую под учетной записью **root**. Использование **sudo** помогает ограничить права пользователей и снизить риски безопасности, связанные с работой с правами суперпользователя. Правила, определяющие, какие пользователи могут использовать **sudo** и какие команды они могут выполнять, хранятся в файле **/etc/sudoers**.

2. Меняем **hostname** ОС от имени пользователя **newuser** (используя **sudo**);

```
~$hostnamectl set-hostname winvairu-2
```

```

newuser@winvairu-1:~$ hostnamectl
  Static hostname: winvairu-1
    Icon name: computer-vm
  Chassis: vm
  Machine ID: 49c7ad599b0f4a5ca883dce1da474ab5
  Boot ID: c4f4f6e0c9ce4a859a193a903b0d146d
  Virtualization: oracle
  Operating System: Ubuntu 20.04.6 LTS
    Kernel: Linux 5.4.0-186-generic
  Architecture: x86-64
newuser@winvairu-1:~$ hostnamectl set-hostname winvairu-2
=== AUTHENTICATING FOR org.freedesktop.hostname1.set-static-hostname ===
Authentication is required to set the statically configured local host name, as well as the pretty host name.
Multiple identities can be used for authentication:
 1. cranbero
 2. ,, (newuser)
Choose identity to authenticate as (1-2): 2
Password:
=== AUTHENTICATION COMPLETE ===
newuser@winvairu-1:~$ hostnamectl
  Static hostname: winvairu-2
    Icon name: computer-vm
  Chassis: vm
  Machine ID: 49c7ad599b0f4a5ca883dce1da474ab5
  Boot ID: c4f4f6e0c9ce4a859a193a903b0d146d
  Virtualization: oracle
  Operating System: Ubuntu 20.04.6 LTS
    Kernel: Linux 5.4.0-186-generic
  Architecture: x86-64
newuser@winvairu-1:~$

```

## Part 6. Установка и настройка службы времени

1. Если нам нужно узнать текущее время в локальном часовом поясе:

~\$**date +%T**

```

cranbero@winvairu-2:~$ date +%T
13:42:33
cranbero@winvairu-2:~$ _

```

2. ~\$**timedatectl show**

```

cranbero@winvairu-2:~$ timedatectl show
Timezone=Europe/Moscow
LocalRTC=no
CanNTP=yes
NTP=yes
NTPSynchronized=yes
TimeUSec=Fri 2024-06-21 13:47:29 MSK
RTCTimeUSec=Fri 2024-06-21 13:47:30 MSK
cranbero@winvairu-2:~$ _

```

3. Переход с timesyncd на ntpd:

- отключаем timesyncd ~\$**sudo timedatectl set-ntp no**
- устанавливаем ntp ~\$**sudo apt install ntp**



Демон **ntpd** запускается автоматически после установки. Запрашиваем состояние **ntpd**:

**~\$ntpq -p**

```
cranbero@winvairu-2:~$ ntpq -p
      remote               refid              st t when poll reach  delay  offset  jitter
=====
0.ubuntu.pool.n .POOL.          16 p   -   64    0   0.000   0.000   0.000
1.ubuntu.pool.n .POOL.          16 p   -   64    0   0.000   0.000   0.000
2.ubuntu.pool.n .POOL.          16 p   -   64    0   0.000   0.000   0.000
3.ubuntu.pool.n .POOL.          16 p   -   64    0   0.000   0.000   0.000
ntp.ubuntu.com .POOL.          16 p   -   64    0   0.000   0.000   0.000
time.cloudflare 10.136.8.4      3 u  27   64    1  15.197 127.693 596.064
+ntp.ix.ru       .GLN.           1 u   7   64   37  15.379 126.814 569.585
+time-e-b.nist.g .NIST.          1 u   1   64   37 169.602 129.164 574.186
217.26.24.119 .STEP.          16 u   -  256    0   0.000   0.000   0.000
any.yandex.ru .STEP.          16 u   -  256    0   0.000   0.000   0.000
#213.33.141.134 85.21.78.8      3 u  27   64    1  21.610 509.789 327.893
+95-31-7-160.sta 82.209.210.87   2 u  23   64    1  15.774 133.093 537.104
+ntp.truenetwork 80.242.83.227   2 u  24   64    1  41.070 127.424 536.092
+Time100.Stupi.S .PPS.           1 u  20   64    1  34.178 138.865 536.263
#212.20.46.199 ( 46.254.241.74  2 u  18   64    1  46.794 914.270 538.912
+rnis-app2.rnis6 10.0.10.101     2 u  24   64    1  28.669 120.073 536.101
#ntp1.doorhan.ru 194.190.168.1   2 u  25   64    1  16.219 905.018 529.014
+time.cloudflare 10.158.8.5      3 u  24   64    1  27.657 128.414 536.145
+195.239.232.102 129.6.15.28     2 u  23   64    1  32.121 910.751 531.235
*lemonbro.ru     .PPS.           1 u  25   64    1  27.146 137.639 522.055
+mx1.user3849.ru 89.109.251.22   2 u  20   64    1  32.076 123.779 547.514
+home.ostankin.n 89.109.251.23   2 u  23   64    1  27.361 907.175 527.823
+62.105.144.90  128.10.252.6    2 u  25   64    1  45.053 331.685 373.859
alphyn.canonica 132.163.96.1    2 u 139   64   34 126.204 125.365 333.240
cranbero@winvairu-2:~$ _
```

**ntpq** – это инструмент запросов для **ntpd**. Флаг **-p** запрашивает данные о серверах NTP, к которым подключается **ntpd**. Ваш вывод будет отличаться, но в нём всё равно должен быть стандартный пул Ubuntu и несколько других серверов.

На установку соединения **ntpd** потребуется несколько минут.

## Part 7. Установка и использование текстовых редакторов

### 1. VIM:

```
cranbero
~
~
```

- Команда для выхода с сохранением изменений: **:wq**
- Команда для выхода без изменений: **:q!**

```
cranbero@winvairu-2:~$ cat test_vim.txt
cranbero
cranbero@winvairu-2:~$
```

- Поиска слова и его замена на другое в редакторе Vim:

```
:s/\<cranbero\>/winvairu/
```

[illegible]

2. nano:

```
GNU nano 4.8 test_nano.txt
cranbero
```

- Команда для выхода с сохранением изменений: **^S, ^X**
- Команда для выхода без изменений: **^X, N**

```
cranbero@winvairu-2:~$ cat test_nano.txt
cranbero
cranbero@winvairu-2:~$
```

- Для поиска и замены текста используется команда **Option+R**.

GNU nano 4.8test\_nano.txtModified

cranbero

Search (to replace) [winvairu]: cranbero

^G Get Help

^C Cancel

M-C Case Sens

M-R Regexp

M-B Backwards

^R No Replace

^P Older

^N Newer

GNU nano 4.8test\_nano.txtModified

cranbero

Replace with: winvairu\_

^G Get Help

^C Cancel

^P Older

^N Newer

```
GNU nano 4.8      test_nano.txt      Modified
winvairu

[ Replaced 1 occurrence ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line  M-E Redo
```

3. joe:

```
  IW  test_joe.txt      Row 2  Col 1
cranbero
```

- Команда для выхода с сохранением изменений: **^KX**
- Команда для выхода без изменений: **^KQ**

```
cranbero@winvairu-2:~$ cat test_joe.txt
cranbero
cranbero@winvairu-2:~$
```

- Для выполнения поиска и замены файл должен содержать более одного слова, поэтому добавляем:

```
  IW  test_joe.txt      Row 1  Col 1
hi cranbero
```

- Вводим **^K F**. Нам будет предложено ввести строку, которую мы хотим найти, в данном случае **cranbero**:

```
IW test_joe.txt Row 1 Col 1
hi cranbero

Find (^K H for help) [winvairu]: cranbero_
```

- Затем нам будет предложено указать параметры типа поиска, но в этом простом случае просто нажимаем клавишу **R**;
- Далее вводим слово для замены и подтверждаем клавишей **Y**:

```
IW test_joe.txt (Modified) Row 1 Col 12
hi winvairu
```

## Part 8. Установка и базовая настройка сервиса SSHD

1. Установка службы SSHd:

```
~$sudo apt install openssh-server
```

2. Добавляем автостарт службы при загрузке системы:

```
~$sudo systemctl enable ssh
```

3. Перенастройка службы SSHd на порт 2022. Все настройки сервера SSH хранятся в конфигурационном файле **sshd\_config**, который находится в папке **/etc/ssh**. Перед тем как вносить изменения в этот конфигурационный

файл рекомендуется сделать его резервную копию, для этого используем такую команду:

```
~$sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.factory-defaults
```

Переходим к настройке конфигурационного файла:

```
~$sudo vim /etc/ssh/sshd_config
```

```
#      $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.
# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 2022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

Перезапускаем службу SSH:

```
~$sudo systemctl restart ssh
```

4. Находим наличие процесса sshd:

```
~$ps -ax | grep sshd
```

Флаг **-a** обозначает все процессы, а **-x** — выводит все процессы, даже те, которые не связаны с текущим ТТУ.

```
cranbero@winvairu-2:~$ ps -ax | grep sshd
 3089 ?        Ss      0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
 3301 tty1    S+      0:00 grep --color=auto sshd
cranbero@winvairu-2:~$ _
```

5. ~\$**netstat -tan**:

```
cranbero@winvairu-2:~$ netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2022            0.0.0.0:*               LISTEN
tcp6       0      0 :::2022                 :::*                    LISTEN
cranbero@winvairu-2:~$ _
```

Команда **netstat -tan** в консоли Ubuntu показывает список всех активных сетевых соединений на вашем компьютере. Каждая строка вывода содержит

следующую информацию:

- **Proto** - Протокол, используемый для данного соединения. Обычно это TCP или UDP.
- **Recv-Q** - Количество байт данных, которые были получены от удаленного хоста, но еще не были прочитаны процессом, использующим соединение.
- **Send-Q** - Количество байт данных, которые были отправлены местным процессом, но еще не были доставлены удаленному хосту.
- **Local Address** - Локальный адрес и порт, используемые для данного соединения.
- **Foreign Address** - Удаленный адрес и порт, используемые для данного соединения.
- **State** - Состояние соединения. Возможные состояния включают ESTABLISHED (соединение установлено), LISTEN (процесс ожидает входящих соединений), CLOSE\_WAIT (удаленный хост закрыл соединение, но локальный процесс еще не завершил его), TIME\_WAIT (соединение было закрыто, но оно остается открытым некоторое время для обработки возможных повторных передач пакетов) и другие.

**netstat** — это утилита командной строки в Unix-подобных операционных системах, которая отображает информацию о сетевых соединениях, включая открытые порты и статистику по ним.

Ключи имеют следующие значения:

**-t**: Показывает все TCP-соединения.

**-a**: Показывает все соединения (активные и неактивные).

**-n**: Отключает разрешение имен для хостов и портов, то есть вместо имён используются числовые IP-адреса и номера портов. Это может быть полезно, если DNS не работает или нужно избежать лишних запросов к DNS-серверу.

Значение **0.0.0.0** в столбцах **Local Address** и **Foreign Address** при выполнении команды **netstat -tan** указывает на то, что IP-адрес не определен или не назначен. Это обычно происходит, когда приложение или

служба слушает все IP-адреса на сетевом интерфейсе, не конкретизируя какой-либо определенный IP-адрес.

Однако стоит отметить, что **0.0.0.0** также может указывать на проблемы с конфигурацией сети или приложения, поэтому если вы видите это значение и не уверены, что оно должно быть там, рекомендуется обратиться к документации соответствующего приложения или службы для уточнения.

## Part 9. Установка и использование утилит top, htop

### 1. Утилита top.

```
top - 02:46:34 up 9:28, 1 user, load average: 0.00, 0.00, 0.00
Tasks: 104 total, 1 running, 103 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni, 100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 3920.0 total, 3320.7 free, 162.5 used, 436.8 buff/cache
MiB Swap: 2296.0 total, 2296.0 free, 0.0 used. 3525.4 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
2807	root	20	0	0	0	0	I	0.3	0.0	0:10.10	kworker/1:2-events
3426	cranbero	20	0	9248	3968	3308	R	0.3	0.1	0:00.04	top
1	root	20	0	103944	13040	8532	S	0.0	0.3	0:03.16	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.03	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par_gp
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/0:0H-kblockd
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_percpu_wq
9	root	20	0	0	0	0	S	0.0	0.0	0:00.19	ksoftirqd/0
10	root	20	0	0	0	0	I	0.0	0.0	0:23.54	rcu_sched
11	root	rt	0	0	0	0	S	0.0	0.0	0:01.22	migration/0
12	root	-51	0	0	0	0	S	0.0	0.0	0:00.00	idle_inject/0
14	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/0
15	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/1
16	root	-51	0	0	0	0	S	0.0	0.0	0:00.00	idle_inject/1
17	root	rt	0	0	0	0	S	0.0	0.0	0:01.87	migration/1
18	root	20	0	0	0	0	S	0.0	0.0	0:00.13	ksoftirqd/1
20	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/1:0H-kblockd
21	root	20	0	0	0	0	S	0.0	0.0	0:00.01	kdevtmpfs
22	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
23	root	20	0	0	0	0	S	0.0	0.0	0:00.00	rcu_tasks_kthre
24	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kauditd
25	root	20	0	0	0	0	S	0.0	0.0	0:00.02	khungtaskd
26	root	20	0	0	0	0	S	0.0	0.0	0:00.00	oom_reaper
27	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	writeback
28	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kcompactd0
29	root	25	5	0	0	0	S	0.0	0.0	0:00.00	ksmd
30	root	39	19	0	0	0	S	0.0	0.0	0:00.00	khugepaged
77	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kintegrityd
78	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kblockd



```
top - 02:46:46 up 9:28, 1 user, load average: 0.00, 0.00, 0.00
Tasks: 104 total, 1 running, 103 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni,100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 3920.0 total, 3320.7 free, 162.5 used, 436.8 buff/cache
MiB Swap: 2296.0 total, 2296.0 free, 0.0 used. 3525.4 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
699	root	20	0	1320308	30304	19580	S	0.0	0.8	0:03.01	snapd
372	root	19	-1	60332	22544	21508	S	0.0	0.6	0:00.43	systemd-journal
792	root	20	0	107920	20632	12964	S	0.0	0.5	0:00.07	unattended-upgr
688	root	20	0	29644	18452	10420	S	0.0	0.5	0:00.11	networkd-dispat
579	root	rt	0	280200	18000	8208	S	0.3	0.4	0:16.85	multipathd
1	root	20	0	103944	13040	8532	S	0.0	0.3	0:03.16	systemd
667	systemd+	20	0	24688	12316	8252	S	0.0	0.3	0:00.19	systemd-resolve
703	root	20	0	393264	12304	10436	S	0.0	0.3	0:00.11	udisksd
752	root	20	0	315104	11288	9580	S	0.0	0.3	0:00.07	ModemManager
3278	cranbero	20	0	19088	9848	8268	S	0.0	0.2	0:00.06	systemd
1329	root	20	0	249468	9472	8324	S	0.0	0.2	0:00.09	upowerd
700	root	20	0	17536	7916	7024	S	0.0	0.2	0:00.31	systemd-logind
665	systemd+	20	0	19080	7604	6740	S	0.0	0.2	0:00.26	systemd-network
678	root	20	0	235680	7428	6536	S	0.0	0.2	0:02.02	accounts-daemon
692	root	20	0	232732	6844	6152	S	0.0	0.2	0:00.02	polkitd
3089	root	20	0	12188	6812	5968	S	0.0	0.2	0:00.00	sshd
407	root	20	0	22508	6060	4128	S	0.0	0.2	0:00.83	systemd-udev
3290	cranbero	20	0	8264	5128	3416	S	0.0	0.1	0:00.03	bash
693	syslog	20	0	224492	5044	3980	S	0.0	0.1	0:00.06	rsyslogd
682	message+	20	0	7708	4924	4040	S	0.0	0.1	0:00.44	dbus-daemon
3284	cranbero	20	0	105160	4660	12	S	0.0	0.1	0:00.00	(sd-pam)
3426	cranbero	20	0	9248	3968	3308	R	0.0	0.1	0:00.05	top
3101	root	20	0	5972	3892	3112	S	0.0	0.1	0:00.01	login
686	root	20	0	81828	3788	3488	S	0.0	0.1	0:01.44	irqbalance
681	root	20	0	6816	3036	2772	S	0.0	0.1	0:00.15	cron
714	daemon	20	0	3796	2120	1948	S	0.0	0.1	0:00.00	atd
1531	root	20	0	5828	1792	1676	S	0.0	0.0	0:00.00	agetty
2	root	20	0	0	0	0	S	0.0	0.0	0:00.03	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par_gp

- uptime: **9:28**
- количество авторизованных пользователей: **1**
- общую загрузку системы: **0**
- общее количество процессов: **104**
- загрузку сри: **0**
- загрузку памяти **162.5**
- pid процесса занимающего больше всего памяти: **699**
- pid процесса, занимающего больше всего процессорного времени: **2807**

## 2. Утилита htop.

- Сортировка по PID:

```

1  [                                0.0%]   Tasks: 27, 31 thr; 1 running
2  [                                0.0%]   Load average: 0.00 0.00 0.00
Mem[|||||]                        164M/3.83G   Uptime: 10:08:27
Swp[                               ]          0K/2.24G

```

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
1	root	20	0	101M	13040	8532	S	0.0	0.3	0:03.17	/sbin/init splash noprompt noshell
372	root	19	-1	60332	22592	21556	S	0.0	0.6	0:00.44	/lib/systemd/systemd-journald
407	root	20	0	22508	6060	4128	S	0.0	0.2	0:00.83	/lib/systemd/systemd-udevd
579	root	RT	0	273M	18000	8208	S	0.0	0.4	0:18.06	/sbin/multipathd -d -s
580	root	RT	0	273M	18000	8208	S	0.0	0.4	0:01.53	/sbin/multipathd -d -s
581	root	RT	0	273M	18000	8208	S	0.0	0.4	0:00.00	/sbin/multipathd -d -s
582	root	RT	0	273M	18000	8208	S	0.0	0.4	0:00.24	/sbin/multipathd -d -s
583	root	RT	0	273M	18000	8208	S	0.7	0.4	0:11.56	/sbin/multipathd -d -s
584	root	RT	0	273M	18000	8208	S	0.0	0.4	0:00.00	/sbin/multipathd -d -s
585	root	RT	0	273M	18000	8208	S	0.0	0.4	0:00.00	/sbin/multipathd -d -s
665	systemd-n	20	0	19080	7604	6740	S	0.0	0.2	0:00.27	/lib/systemd/systemd-networkd
667	systemd-r	20	0	24688	12316	8252	S	0.0	0.3	0:00.19	/lib/systemd/systemd-resolved
678	root	20	0	230M	7428	6536	S	0.0	0.2	0:02.16	/usr/lib/accountsservice/accounts-d
681	root	20	0	6816	3036	2772	S	0.0	0.1	0:00.16	/usr/sbin/cron -f
682	messagebu	20	0	7708	4924	4040	S	0.0	0.1	0:00.44	/usr/bin/dbus-daemon --system --add
686	root	20	0	81828	3788	3488	S	0.0	0.1	0:01.56	/usr/sbin/irqbalance --foreground
688	root	20	0	29644	18452	10420	S	0.0	0.5	0:00.11	/usr/bin/python3 /usr/bin/networkd-
692	root	20	0	227M	6844	6152	S	0.0	0.2	0:00.02	/usr/lib/policykit-1/polkitd --no-d
693	syslog	20	0	219M	5044	3980	S	0.0	0.1	0:00.06	/usr/sbin/rsyslogd -n -iNONE
699	root	20	0	1289M	30304	19580	S	0.0	0.8	0:03.12	/usr/lib/snapd/snapd
700	root	20	0	17536	7916	7024	S	0.0	0.2	0:00.32	/lib/systemd/systemd-logind
703	root	20	0	384M	12304	10436	S	0.0	0.3	0:00.12	/usr/lib/udisks2/udisksd
708	root	20	0	230M	7428	6536	S	0.0	0.2	0:02.08	/usr/lib/accountsservice/accounts-d
714	daemon	20	0	3796	2120	1948	S	0.0	0.1	0:00.00	/usr/sbin/atd -f
720	root	20	0	81828	3788	3488	S	0.0	0.1	0:00.00	/usr/sbin/irqbalance --foreground
721	root	20	0	227M	6844	6152	S	0.0	0.2	0:00.00	/usr/lib/policykit-1/polkitd --no-d
728	root	20	0	384M	12304	10436	S	0.0	0.3	0:00.00	/usr/lib/udisks2/udisksd
732	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.99	/usr/lib/snapd/snapd
736	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.00	/usr/lib/snapd/snapd

F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice -F8Nice +F9Kill F10Quit

- Сортировка по PERCENT\_CPU:

```

1  [                                0.0%]   Tasks: 27, 31 thr; 1 running
2  [                                0.0%]   Load average: 0.00 0.00 0.00
Mem[|||||]                        164M/3.83G   Uptime: 10:08:54
Swp[                               ]          0K/2.24G

```

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
3444	cranbero	20	0	8024	3964	3228	R	0.7	0.1	0:00.17	htop
1	root	20	0	101M	13040	8532	S	0.0	0.3	0:03.17	/sbin/init splash noprompt noshell
372	root	19	-1	60332	22592	21556	S	0.0	0.6	0:00.44	/lib/systemd/systemd-journald
407	root	20	0	22508	6060	4128	S	0.0	0.2	0:00.83	/lib/systemd/systemd-udevd
579	root	RT	0	273M	18000	8208	S	0.0	0.4	0:18.08	/sbin/multipathd -d -s
580	root	RT	0	273M	18000	8208	S	0.0	0.4	0:01.53	/sbin/multipathd -d -s
581	root	RT	0	273M	18000	8208	S	0.0	0.4	0:00.00	/sbin/multipathd -d -s
582	root	RT	0	273M	18000	8208	S	0.0	0.4	0:00.24	/sbin/multipathd -d -s
583	root	RT	0	273M	18000	8208	S	0.0	0.4	0:11.56	/sbin/multipathd -d -s
584	root	RT	0	273M	18000	8208	S	0.0	0.4	0:00.00	/sbin/multipathd -d -s
585	root	RT	0	273M	18000	8208	S	0.0	0.4	0:00.00	/sbin/multipathd -d -s
665	systemd-n	20	0	19080	7604	6740	S	0.0	0.2	0:00.27	/lib/systemd/systemd-networkd
667	systemd-r	20	0	24688	12316	8252	S	0.0	0.3	0:00.19	/lib/systemd/systemd-resolved
678	root	20	0	230M	7428	6536	S	0.0	0.2	0:02.16	/usr/lib/accountsservice/accounts-d
681	root	20	0	6816	3036	2772	S	0.0	0.1	0:00.16	/usr/sbin/cron -f
682	messagebu	20	0	7708	4924	4040	S	0.0	0.1	0:00.44	/usr/bin/dbus-daemon --system --add
686	root	20	0	81828	3788	3488	S	0.0	0.1	0:01.56	/usr/sbin/irqbalance --foreground
688	root	20	0	29644	18452	10420	S	0.0	0.5	0:00.11	/usr/bin/python3 /usr/bin/networkd-
692	root	20	0	227M	6844	6152	S	0.0	0.2	0:00.02	/usr/lib/policykit-1/polkitd --no-d
693	syslog	20	0	219M	5044	3980	S	0.0	0.1	0:00.06	/usr/sbin/rsyslogd -n -iNONE
699	root	20	0	1289M	30304	19580	S	0.0	0.8	0:03.12	/usr/lib/snapd/snapd
700	root	20	0	17536	7916	7024	S	0.0	0.2	0:00.32	/lib/systemd/systemd-logind
703	root	20	0	384M	12304	10436	S	0.0	0.3	0:00.12	/usr/lib/udisks2/udisksd
708	root	20	0	230M	7428	6536	S	0.0	0.2	0:02.08	/usr/lib/accountsservice/accounts-d
714	daemon	20	0	3796	2120	1948	S	0.0	0.1	0:00.00	/usr/sbin/atd -f
720	root	20	0	81828	3788	3488	S	0.0	0.1	0:00.00	/usr/sbin/irqbalance --foreground
721	root	20	0	227M	6844	6152	S	0.0	0.2	0:00.00	/usr/lib/policykit-1/polkitd --no-d
728	root	20	0	384M	12304	10436	S	0.0	0.3	0:00.00	/usr/lib/udisks2/udisksd
732	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.99	/usr/lib/snapd/snapd

F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice -F8Nice +F9Kill F10Quit

- Сортировка по PERCENT\_MEM:

1	[	0.0%	Tasks: 27, 31 thr; 1 running
2	[	0.0%	Load average: 0.00 0.00 0.00
Mem	[     ]	164M/3.83G	Uptime: 10:09:41
Swp	[	0K/2.24G	

  

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
732	root	20	0	1289M	30304	19580	S	0.0	0.8	0:01.00	/usr/lib/snapd/snapd
699	root	20	0	1289M	30304	19580	S	0.0	0.8	0:03.12	/usr/lib/snapd/snapd
736	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.00	/usr/lib/snapd/snapd
737	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.53	/usr/lib/snapd/snapd
739	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.00	/usr/lib/snapd/snapd
775	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.38	/usr/lib/snapd/snapd
776	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.45	/usr/lib/snapd/snapd
777	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.23	/usr/lib/snapd/snapd
778	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.42	/usr/lib/snapd/snapd
372	root	19	-1	60332	22592	21556	S	0.0	0.6	0:00.44	/lib/systemd/systemd-journald
792	root	20	0	105M	20632	12964	S	0.0	0.5	0:00.07	/usr/bin/python3 /usr/share/unatten
828	root	20	0	105M	20632	12964	S	0.0	0.5	0:00.00	/usr/bin/python3 /usr/bin/networkd-
688	root	20	0	29644	18452	10420	S	0.0	0.5	0:00.11	/usr/bin/python3 /usr/bin/networkd-
583	root	RT	0	273M	18000	8208	S	0.0	0.4	0:11.58	/sbin/multipathd -d -s
579	root	RT	0	273M	18000	8208	S	0.0	0.4	0:18.11	/sbin/multipathd -d -s
582	root	RT	0	273M	18000	8208	S	0.0	0.4	0:00.25	/sbin/multipathd -d -s
580	root	RT	0	273M	18000	8208	S	0.0	0.4	0:01.53	/sbin/multipathd -d -s
581	root	RT	0	273M	18000	8208	S	0.0	0.4	0:00.00	/sbin/multipathd -d -s
584	root	RT	0	273M	18000	8208	S	0.0	0.4	0:00.00	/sbin/multipathd -d -s
585	root	RT	0	273M	18000	8208	S	0.0	0.4	0:00.00	/sbin/multipathd -d -s
1	root	20	0	101M	13040	8532	S	0.0	0.3	0:03.17	/sbin/init splash noprompt noshell
667	systemd-r	20	0	24688	12316	8252	S	0.0	0.3	0:00.19	/lib/systemd/systemd-resolved
703	root	20	0	384M	12304	10436	S	0.0	0.3	0:00.12	/usr/lib/udisks2/udisksd
728	root	20	0	384M	12304	10436	S	0.0	0.3	0:00.00	/usr/lib/udisks2/udisksd
749	root	20	0	384M	12304	10436	S	0.0	0.3	0:00.01	/usr/lib/udisks2/udisksd
769	root	20	0	384M	12304	10436	S	0.0	0.3	0:00.00	/usr/lib/udisks2/udisksd
818	root	20	0	384M	12304	10436	S	0.0	0.3	0:00.00	/usr/lib/udisks2/udisksd
752	root	20	0	307M	11288	9580	S	0.0	0.3	0:00.07	/usr/sbin/ModemManager
760	root	20	0	307M	11288	9580	S	0.0	0.3	0:00.00	/usr/sbin/ModemManager

  

F1	Help	F2	Setup	F3	Search	F4	Filter	F5	Tree	F6	SortBy	F7	Nice -	F8	Nice +	F9	Kill	F10	Quit
----	------	----	-------	----	--------	----	--------	----	------	----	--------	----	--------	----	--------	----	------	-----	------

- Сортировка по TIME:

```
1 [ 0.0%] Tasks: 27, 31 thr: 1 running
2 [ 0.0%] Load average: 0.00 0.00 0.00
Mem[|||||] 164M/3.83G Uptime: 10:10:03
Swp[ ] 0K/2.24G

PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
579 root RT 0 273M 18000 8208 S 0.0 0.4 0:18.12 /sbin/multipathd -d -s
583 root RT 0 273M 18000 8208 S 0.0 0.4 0:11.59 /sbin/multipathd -d -s
1 root 20 0 101M 13040 8532 S 0.0 0.3 0:03.17 /sbin/init splash noprompt noshell
699 root 20 0 1289M 30304 19580 S 0.0 0.8 0:03.12 /usr/lib/napd/napd
678 root 20 0 230M 7428 6536 S 0.0 0.2 0:02.18 /usr/lib/accountsservice/accounts-d
708 root 20 0 230M 7428 6536 S 0.0 0.2 0:02.10 /usr/lib/accountsservice/accounts-d
686 root 20 0 81828 3788 3488 S 0.0 0.1 0:01.56 /usr/sbin/irqbalance --foreground
580 root RT 0 273M 18000 8208 S 0.0 0.4 0:01.53 /sbin/multipathd -d -s
732 root 20 0 1289M 30304 19580 S 0.0 0.8 0:01.00 /usr/lib/napd/napd
407 root 20 0 22508 6060 4128 S 0.0 0.2 0:00.83 /lib/systemd/systemd-udev
737 root 20 0 1289M 30304 19580 S 0.0 0.8 0:00.53 /usr/lib/napd/napd
776 root 20 0 1289M 30304 19580 S 0.0 0.8 0:00.45 /usr/lib/napd/napd
372 root 19 -1 60332 22592 21556 S 0.0 0.6 0:00.44 /lib/systemd/systemd-journald
682 messagebu 20 0 7708 4924 4040 S 0.0 0.1 0:00.44 /usr/bin/dbus-daemon --system --add
778 root 20 0 1289M 30304 19580 S 0.0 0.8 0:00.42 /usr/lib/napd/napd
775 root 20 0 1289M 30304 19580 S 0.0 0.8 0:00.38 /usr/lib/napd/napd
3444 cranbero 20 0 8024 3964 3228 R 0.0 0.1 0:00.33 htop
700 root 20 0 17536 7916 7024 S 0.0 0.2 0:00.32 /lib/systemd/systemd-logind
665 systemd-n 20 0 19080 7604 6740 S 0.0 0.2 0:00.27 /lib/systemd/systemd-networkd
582 root RT 0 273M 18000 8208 S 0.0 0.4 0:00.25 /sbin/multipathd -d -s
777 root 20 0 1289M 30304 19580 S 0.0 0.8 0:00.23 /usr/lib/napd/napd
667 systemd-r 20 0 24688 12316 8252 S 0.0 0.3 0:00.19 /lib/systemd/systemd-resolved
681 root 20 0 6816 3036 2772 S 0.0 0.1 0:00.16 /usr/sbin/cron -f
703 root 20 0 384M 12304 10436 S 0.0 0.3 0:00.12 /usr/lib/udisks2/udisksd
688 root 20 0 29644 18452 10420 S 0.0 0.5 0:00.11 /usr/bin/python3 /usr/bin/networkd-
1329 root 20 0 243M 9472 8324 S 0.0 0.2 0:00.09 /usr/lib/upower/upowerd
792 root 20 0 105M 20632 12964 S 0.0 0.5 0:00.07 /usr/bin/python3 /usr/share/unatten
752 root 20 0 307M 11288 9580 S 0.0 0.3 0:00.07 /usr/sbin/ModemManager
3278 cranbero 20 0 19088 9848 8268 S 0.0 0.2 0:00.06 /lib/systemd/systemd --user
F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice - F8Nice + F9Kill F10Quit
```

- Фильтрация для процесса sshd:

```
1 [ 0.0%] Tasks: 27, 31 thr: 1 running
2 [ 0.0%] Load average: 0.00 0.00 0.00
Mem[|||||] 164M/3.83G Uptime: 10:14:46
Swp[ ] 0K/2.24G

PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
3089 root 20 0 12188 6812 5968 S 0.0 0.2 0:00.00 | sshd: /usr/sbin/sshd -D [listene

F1Help F2Setup F3Search F4Filter F5Sorted F6Collap F7Nice - F8Nice + F9Kill F10Quit
```

- Процесс syslog, найденный, используя поиск:

1	[	0.0%	Tasks: 27, 31 thr; 1 running
2	[	0.0%	Load average: 0.00 0.00 0.00
Mem	[     ]	164M/3.83G	Uptime: 10:17:36
Swp	[	0K/2.24G	

  

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
3290	cranbero	20	0	8264	5128	3416	S	0.0	0.1	0:00.05	-bash
3461	cranbero	20	0	8024	3964	3232	R	0.7	0.1	0:00.17	htop
3089	root	20	0	12188	6812	5968	S	0.0	0.2	0:00.00	sshd: /usr/sbin/sshd -D [listene
1531	root	20	0	5828	1792	1676	S	0.0	0.0	0:00.00	/sbin/agetty -o -p -- \u --nocle
1329	root	20	0	243M	9472	8324	S	0.0	0.2	0:00.09	/usr/lib/upower/upowerd
1332	root	20	0	243M	9472	8324	S	0.0	0.2	0:00.00	/usr/lib/upower/upowerd
1331	root	20	0	243M	9472	8324	S	0.0	0.2	0:00.00	/usr/lib/upower/upowerd
792	root	20	0	105M	20632	12964	S	0.0	0.5	0:00.07	/usr/bin/python3 /usr/share/unat
828	root	20	0	105M	20632	12964	S	0.0	0.5	0:00.00	/usr/bin/python3 /usr/share/u
752	root	20	0	307M	11288	9580	S	0.0	0.3	0:00.07	/usr/sbin/ModemManager
768	root	20	0	307M	11288	9580	S	0.0	0.3	0:00.01	/usr/sbin/ModemManager
760	root	20	0	307M	11288	9580	S	0.0	0.3	0:00.00	/usr/sbin/ModemManager
714	daemon	20	0	3796	2120	1948	S	0.0	0.1	0:00.00	/usr/sbin/atd -f
703	root	20	0	384M	12304	10436	S	0.0	0.3	0:00.12	/usr/lib/udisks2/udisksd
818	root	20	0	384M	12304	10436	S	0.0	0.3	0:00.00	/usr/lib/udisks2/udisksd
769	root	20	0	384M	12304	10436	S	0.0	0.3	0:00.00	/usr/lib/udisks2/udisksd
749	root	20	0	384M	12304	10436	S	0.0	0.3	0:00.01	/usr/lib/udisks2/udisksd
728	root	20	0	384M	12304	10436	S	0.0	0.3	0:00.00	/usr/lib/udisks2/udisksd
700	root	20	0	17536	7916	7024	S	0.0	0.2	0:00.32	/lib/systemd/systemd-logind
699	root	20	0	1289M	30304	19580	S	0.0	0.8	0:03.15	/usr/lib/snapd/snapd
778	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.43	/usr/lib/snapd/snapd
777	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.23	/usr/lib/snapd/snapd
776	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.45	/usr/lib/snapd/snapd
775	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.40	/usr/lib/snapd/snapd
739	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.00	/usr/lib/snapd/snapd
737	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.53	/usr/lib/snapd/snapd
736	root	20	0	1289M	30304	19580	S	0.0	0.8	0:00.00	/usr/lib/snapd/snapd
732	root	20	0	1289M	30304	19580	S	0.0	0.8	0:01.00	/usr/lib/snapd/snapd
693	syslog	20	0	219M	5044	3980	S	0.0	0.1	0:00.06	/usr/sbin/rsyslogd -n -iNONE

F1Help F2Setup F3Search F4Filter F5Sorted F6Collap F7Nice - F8Nice + F9Kill F10Quit

- Добавленный вывод hostname, clock и uptime:

```
1 [ 0.0%] Hostname: winvairu-2
2 [ 0.0%] Time: 03:50:32
Mem[|||||] 164M/3.83G Uptime: 10:32:40
Swp[ ] 0K/2.24G

  PID USER      PRI  NI  VIRT   RES   SHR  S  CPU% MEM%   TIME+  Command
  ---  ---      ---  --  ---    ---    ---  -  ---  ---   ---+   ---
    1 root        20   0  101M  13040  8532  S   0.0  0.3   0:03.17 /sbin/init splash noprompt noshell
  3278 cranbero   20   0  19088  9848   8268  S   0.0  0.2   0:00.06 | /lib/systemd/systemd --user
  3284 cranbero   20   0   102M  4660    12  S   0.0  0.1   0:00.00 | | (sd-pam)
  3101 root        20   0   5972  3892   3112  S   0.0  0.1   0:00.01 | /bin/login -p --
  3290 cranbero   20   0   8264  5128   3416  S   0.0  0.1   0:00.05 | | -bash
  3463 cranbero   20   0   8024  4032   3300  R   0.7  0.1   0:01.08 | | htop
  3089 root        20   0  12188  6812   5968  S   0.0  0.2   0:00.00 | | sshd: /usr/sbin/sshd -D [listene
  1531 root        20   0   5828  1792   1676  S   0.0  0.0   0:00.00 | | /sbin/agetty -o -p -- \u --nocle
  1329 root        20   0   243M  9472   8324  S   0.0  0.2   0:00.09 | | /usr/lib/upower/upowerd
  1332 root        20   0   243M  9472   8324  S   0.0  0.2   0:00.00 | | | /usr/lib/upower/upowerd
  1331 root        20   0   243M  9472   8324  S   0.0  0.2   0:00.00 | | | /usr/lib/upower/upowerd
   792 root        20   0   105M  20632  12964  S   0.0  0.5   0:00.07 | | /usr/bin/python3 /usr/share/unat
   828 root        20   0   105M  20632  12964  S   0.0  0.5   0:00.00 | | | /usr/bin/python3 /usr/share/u
   752 root        20   0   307M  11288   9580  S   0.0  0.3   0:00.07 | | /usr/sbin/ModemManager
   768 root        20   0   307M  11288   9580  S   0.0  0.3   0:00.01 | | | /usr/sbin/ModemManager
   760 root        20   0   307M  11288   9580  S   0.0  0.3   0:00.00 | | | /usr/sbin/ModemManager
   714 daemon      20   0   3796   2120   1948  S   0.0  0.1   0:00.00 | | /usr/sbin/atd -f
   703 root        20   0   384M  12304  10436  S   0.0  0.3   0:00.12 | | /usr/lib/udisks2/udisksd
   818 root        20   0   384M  12304  10436  S   0.0  0.3   0:00.00 | | | /usr/lib/udisks2/udisksd
   769 root        20   0   384M  12304  10436  S   0.0  0.3   0:00.00 | | | /usr/lib/udisks2/udisksd
   749 root        20   0   384M  12304  10436  S   0.0  0.3   0:00.01 | | | /usr/lib/udisks2/udisksd
   728 root        20   0   384M  12304  10436  S   0.0  0.3   0:00.00 | | | /usr/lib/udisks2/udisksd
   700 root        20   0  17536   7916   7024  S   0.0  0.2   0:00.32 | | /lib/systemd/systemd-logind
   699 root        20   0  1289M  30304  19580  S   0.0  0.8   0:03.20 | | /usr/lib/snapd/snapd
   778 root        20   0  1289M  30304  19580  S   0.0  0.8   0:00.44 | | | /usr/lib/snapd/snapd
   777 root        20   0  1289M  30304  19580  S   0.0  0.8   0:00.24 | | | /usr/lib/snapd/snapd
   776 root        20   0  1289M  30304  19580  S   0.0  0.8   0:00.45 | | | /usr/lib/snapd/snapd
   775 root        20   0  1289M  30304  19580  S   0.0  0.8   0:00.41 | | | /usr/lib/snapd/snapd
   739 root        20   0  1289M  30304  19580  S   0.0  0.8   0:00.00 | | | /usr/lib/snapd/snapd
F1Help F2Setup F3Search F4Filter F5Sorted F6Collap F7Nice -F8Nice +F9Kill F10Quit
```

## Part 10. Использование утилиты fdisk

~\$fdisk -l

```
Disk /dev/loop0: 63.97 MiB, 67051520 bytes, 130960 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
Disk /dev/loop1: 38.85 MiB, 40714240 bytes, 79520 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
Disk /dev/loop2: 49.86 MiB, 52260864 bytes, 102072 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
Disk /dev/loop3: 63.29 MiB, 66359296 bytes, 129608 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
Disk /dev/loop4: 91.85 MiB, 96292864 bytes, 188072 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

```
Disk /dev/sda: 25 GiB, 26843545600 bytes, 52428800 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
-- INSERT --
```

1,1

Top

```
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: F84D18DE-6CB1-4027-80BF-B1DF4E8B9BE9
```

Device	Start	End	Sectors	Size	Type
/dev/sda1	2048	4095	2048	1M	BIOS boot
/dev/sda2	4096	4198399	4194304	2G	Linux filesystem
/dev/sda3	4198400	52426751	48228352	23G	Linux filesystem

```
Disk /dev/mapper/ubuntu--vg-ubuntu--lv: 11.51 GiB, 12343836672 bytes, 24109056 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
-- INSERT --
```

50,1

Bot

- Название жесткого диска: **dev/sda**;
- Размер и количество секторов: **26843545600 bytes, 52428800 sectors**;
- размер **swap**: не указан.

## Part 11. Использование утилиты df

1. Команда: **~\$df**:

```

cranbero@winvairu-2:~$ df
Filesystem            1K-blocks    Used Available Use% Mounted on
udev                  1960256         0   1960256   0% /dev
tmpfs                  401408      1116    400292   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv 11758760 5032100   6107552  46% /
tmpfs                  2007020         0   2007020   0% /dev/shm
tmpfs                   5120         0     5120   0% /run/lock
tmpfs                  2007020         0   2007020   0% /sys/fs/cgroup
/dev/loop0             65536      65536         0 100% /snap/core20/2318
/dev/sda2              1992552   111244   1760068   6% /boot
/dev/loop1             39808      39808         0 100% /snap/snapd/21759
/dev/loop3             64896      64896         0 100% /snap/core20/1828
/dev/loop2             51072      51072         0 100% /snap/snapd/18357
/dev/loop4             94080      94080         0 100% /snap/lxd/24061
tmpfs                   401404         0    401404   0% /run/user/1000
cranbero@winvairu-2:~$

```

- Информация корневого раздела (/):
  - размер раздела: 11758760;
  - размер занятого пространства: 5032100;
  - размер свободного пространства: 6107552;
  - процент использования: 46%.
- единица измерения в выводе: 1K-blocks.

## 2. Команда: ~\$df -Th:

```

cranbero@winvairu-2:~$ df -Th
Filesystem            Type      Size  Used Avail Use% Mounted on
udev                 devtmpfs  1.9G     0   1.9G   0% /dev
tmpfs                 tmpfs     392M   1.1M  391M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv ext4       12G   4.8G   5.9G  46% /
tmpfs                 tmpfs     2.0G     0   2.0G   0% /dev/shm
tmpfs                 tmpfs     5.0M     0   5.0M   0% /run/lock
tmpfs                 tmpfs     2.0G     0   2.0G   0% /sys/fs/cgroup
/dev/loop0            squashfs   64M    64M     0 100% /snap/core20/2318
/dev/sda2              ext4       2.0G  109M   1.7G   6% /boot
/dev/loop1            squashfs   39M    39M     0 100% /snap/snapd/21759
/dev/loop3            squashfs   64M    64M     0 100% /snap/core20/1828
/dev/loop2            squashfs   50M    50M     0 100% /snap/snapd/18357
/dev/loop4            squashfs   92M    92M     0 100% /snap/lxd/24061
tmpfs                 tmpfs     392M     0   392M   0% /run/user/1000
cranbero@winvairu-2:~$ _

```

- Информация корневого раздела (/):
  - размер раздела: 12G;
  - размер занятого пространства: 4.8G;
  - размер свободного пространства: 5.9G;
  - процент использования: 46%.
- Тип файловой системы для раздела: ext4.



# Part 12. Использование утилиты du

---

1. Запускаем команду ~\$**du**:

```
cranbero@winvairu-2:~$ du
8      ../local/share/nano
12     ../local/share
16     ../local
8      ../ssh
4      ../cache
8      ../config/htop
4      ../config/procps
16     ../config
100    .
cranbero@winvairu-2:~$
```

2. Выводим размер папок /home, /var, /var/log (в байтах, в человекочитаемом виде):

```
cranbero@winvairu-2:~$ sudo du -sb /home
77351    /home
cranbero@winvairu-2:~$ sudo du -sh /home
128K     /home
cranbero@winvairu-2:~$
```

```
cranbero@winvairu-2:~$ sudo du -sb /var
760261329    /var
cranbero@winvairu-2:~$ sudo du -sh /var
735M       /var
cranbero@winvairu-2:~$ _
```

```
cranbero@winvairu-2:~$ sudo du -sb /var/log
62276459     /var/log
cranbero@winvairu-2:~$ sudo du -sh /var/log
60M         /var/log
cranbero@winvairu-2:~$ _
```

3. Выведи размер всего содержимого в /var/log (не общее, а каждого вложенного элемента, используя \*)

```
16K    /var/log/dmesg.2.gz
4.0K   /var/log/ubuntu-advantage.log
48K    /var/log/apt/history.log
44K    /var/log/apt/term.log
24K    /var/log/apt/eipp.log.xz
120K   /var/log/apt
264K   /var/log/syslog.1
28K    /var/log/syslog
32K    /var/log/unattended-upgrades/unattended-upgrades-dpkg.log
4.0K   /var/log/unattended-upgrades/unattended-upgrades-shutdown.log
8.0K   /var/log/unattended-upgrades/unattended-upgrades.log
48K    /var/log/unattended-upgrades
8.0K   /var/log/faillog
516K   /var/log/dpkg.log
336K   /var/log/kern.log
16K    /var/log/dmesg.1.gz
24K    /var/log/installer/subiquity-server-info.log.2199
492K   /var/log/installer/installer-journal.txt
12K    /var/log/installer/block/discover.log
32K    /var/log/installer/block/probe-data.json
48K    /var/log/installer/block
4.0K   /var/log/installer/casper-md5check.json
4.0K   /var/log/installer/subiquity-client-info.log.2711
0      /var/log/installer/subiquity-client-info.log
108K   /var/log/installer/curtin-install.log
0      /var/log/installer/subiquity-client-debug.log
4.0K   /var/log/installer/media-info
4.0K   /var/log/installer/subiquity-client-info.log.2143
4.0K   /var/log/installer/subiquity-client-debug.log.2143
4.0K   /var/log/installer/device-map.json
0      /var/log/installer/subiquity-server-info.log
56K    /var/log/installer/cloud-init.log
0      /var/log/installer/subiquity-server-debug.log
136K   /var/log/installer/subiquity-server-debug.log.2766
8.0K   /var/log/installer/cloud-init-output.log
96K    /var/log/installer/subiquity-server-debug.log.2199
```

```
8.0K   /var/log/installer/cloud-init-output.log
96K    /var/log/installer/subiquity-server-debug.log.2199
4.0K   /var/log/installer/curtin-install/subiquity-partitioning.conf
4.0K   /var/log/installer/curtin-install/subiquity-initial.conf
4.0K   /var/log/installer/curtin-install/subiquity-curthooks.conf
4.0K   /var/log/installer/curtin-install/subiquity-extract.conf
4.0K   /var/log/installer/curtin-install/subiquity-curtin-apt.conf
24K    /var/log/installer/curtin-install
8.0K   /var/log/installer/subiquity-server-info.log.2766
4.0K   /var/log/installer/autoinstall-user-data
16K    /var/log/installer/subiquity-client-debug.log.2711
1.1M   /var/log/installer
4.0K   /var/log/ntpstats
40K    /var/log/wtmp
12K    /var/log/lastlog
4.0K   /var/log/ubuntu-advantage-timer.log
312K   /var/log/cloud-init.log
40K    /var/log/boot.log.2
12K    /var/log/boot.log.1
0      /var/log/boot.log
56K    /var/log/dmesg.0
4.0K   /var/log/private
72K    /var/log/auth.log
104K   /var/log/bootstrap.log
8.0K   /var/log/btmp
56K    /var/log/dmesg
16K    /var/log/cloud-init-output.log
0      /var/log/landscape/sysinfo.log
4.0K   /var/log/landscape
8.0M   /var/log/journal/49c7ad599b0f4a5ca883dce1da474ab5/user-1001.journal
8.1M   /var/log/journal/49c7ad599b0f4a5ca883dce1da474ab5/system@00061b4fb6d652b6-cb88b45607a5a7d7.j
ournal~
8.0M   /var/log/journal/49c7ad599b0f4a5ca883dce1da474ab5/user-1000.journal
17M    /var/log/journal/49c7ad599b0f4a5ca883dce1da474ab5/system.journal
8.0M   /var/log/journal/49c7ad599b0f4a5ca883dce1da474ab5/user-1000@00061b53f5465461-f5a95b6607bfbdc
1.journal~
```

```
8.0M    /var/log/journal/49c7ad599b0f4a5ca883dce1da474ab5/user-1000@00061b53f5465461-f5a95b6607bfbd0
1.journal~
8.1M    /var/log/journal/49c7ad599b0f4a5ca883dce1da474ab5/system@00061b53f2a483e5-aae5561318dda984.j
ournal~
57M     /var/log/journal/49c7ad599b0f4a5ca883dce1da474ab5
57M     /var/log/journal
44K     /var/log/alternatives.log
108K    /var/log/syslog.2.gz
4.0K    /var/log/dist-upgrade
16K     /var/log/dmesg.3.gz
60M     /var/log/
4.0K    disk.txt
4.0K    test_joe.txt
4.0K    test_joe.txt~
4.0K    test_nano.txt
4.0K    test_vim.txt
```

## Part 13. Установка и использование утилиты ncdu

---

1. Назмер папки /home:

```
ncdu 1.14.1 ~ Use the arrow keys to navigate, press ? for help
-- /home -----
108.0 KiB [#####] /cranbero
. 24.0 KiB [##    ] /newuser

Total disk usage: 136.0 KiB  Apparent size: 79.0 KiB  Items: 34
```

2. Назмер папки /var:

```
ncdu 1.14.1 ~ Use the arrow keys to navigate, press ? for help
--- /var -----
. 552.9 MiB [#####] /lib
. 117.8 MiB [##      ] /cache
. 59.3 MiB  [#       ] /log
692.0 KiB  [         ] /backups
. 56.0 KiB  [         ] /snap
. 24.0 KiB  [         ] /spool
. 24.0 KiB  [         ] /tmp
e 4.0 KiB   [         ] /opt
e 4.0 KiB   [         ] /mail
e 4.0 KiB   [         ] /local
e 4.0 KiB   [         ] /crash
@ 0.0 B     [         ] lock
@ 0.0 B     [         ] run

Total disk usage: 730.7 MiB Apparent size: 794.5 MiB Items: 3727
```

3. Назмер папки /var/log:

```
ncdu 1.14.1 ~ Use the arrow keys to navigate, press ? for help
--- /var -----
. 552.9 MiB [#####] /lib
. 117.8 MiB [##      ] /cache
. 59.3 MiB  [#       ] /log
692.0 KiB  [         ] /backups
. 56.0 KiB  [         ] /snap
. 24.0 KiB  [         ] /spool
. 24.0 KiB  [         ] /tmp
e 4.0 KiB   [         ] /opt
e 4.0 KiB   [         ] /mail
e 4.0 KiB   [         ] /local
e 4.0 KiB   [         ] /crash
@ 0.0 B     [         ] lock
@ 0.0 B     [         ] run

Total disk usage: 730.7 MiB Apparent size: 794.5 MiB Items: 3727
```

# Part 14. Работа с системными журналами

Смотрим логи:

1. /var/log/dmesg

~\$less /var/log/dmesg

```
[    0.000000] kernel: Linux version 5.4.0-186-generic (buildd@lcy02-amd64-100) (gcc version 9.4.0 (Ubuntu 9.4.0-1ubuntu1~20.04.2)) #206-Ubuntu SMP Fri Apr 26 12:31:10 UTC 2024 (Ubuntu 5.4.0-186.206-generic 5.4.271)
[    0.000000] kernel: Command line: BOOT_IMAGE=/vmlinuz-5.4.0-186-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro auto=true preseed/file=/cdrom/preseed.cfg priority=critical quiet splash noprompt no-shell automatic-ubiquity debian-installer/locale=en_US keyboard-configuration/layoutcode=us languagechooser/language-name=English localechooser/supported-locales=en_US.UTF-8 countrychooser/shortlist=US --
[    0.000000] kernel: KERNEL supported cpus:
[    0.000000] kernel:   Intel GenuineIntel
[    0.000000] kernel:   AMD AuthenticAMD
[    0.000000] kernel:   Hygon HygonGenuine
[    0.000000] kernel:   Centaur CentaurHauls
[    0.000000] kernel:   zhaoxin   Shanghai
[    0.000000] kernel: BIOS-provided physical RAM map:
[    0.000000] kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbff] usable
[    0.000000] kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
[    0.000000] kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
[    0.000000] kernel: BIOS-e820: [mem 0x0000000000100000-0x000000000dffffffffff] usable
[    0.000000] kernel: BIOS-e820: [mem 0x000000000dfff0000-0x000000000dffffffff] ACPI data
[    0.000000] kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
[    0.000000] kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
[    0.000000] kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[    0.000000] kernel: BIOS-e820: [mem 0x0000000100000000-0x000000011fffffffff] usable
[    0.000000] kernel: NX (Execute Disable) protection: active
[    0.000000] kernel: SMBIOS 2.5 present.
[    0.000000] kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
[    0.000000] kernel: Hypervisor detected: KVM
[    0.000000] kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
[    0.000000] kernel: kvm-clock: cpu 0, msr 3d401001, primary cpu clock
[    0.000000] kernel: kvm-clock: using sched offset of 6306773727 cycles
[    0.000002] kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 881590591483 ns
[    0.000004] kernel: tsc: Detected 3011.706 MHz processor
[    0.003053] kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[    0.003055] kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
/var/log/dmesg
```

2. /var/log/syslog

~\$less /var/log/syslog

```

Jun 22 00:00:15 any rsyslogd: [origin software="rsyslogd" swVersion="8.2001.0" x-pid="693" x-info="https://www.rsyslog.com"] rsyslogd was HUPed
Jun 22 00:17:01 any CRON[2851]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
Jun 22 00:35:01 any CRON[2878]: (root) CMD ( test -x /etc/cron.daily/popularity-contest && /etc/cron.daily/popularity-contest --cron)
Jun 22 00:40:54 any systemd[1]: session-12.scope: Succeeded.
Jun 22 00:41:02 any systemd[1]: getty@tty1.service: Succeeded.
Jun 22 00:41:02 any systemd[1]: session-8.scope: Succeeded.
Jun 22 00:41:02 any systemd[1]: getty@tty1.service: Scheduled restart job, restart counter is at 3.
Jun 22 00:41:02 any systemd[1]: Stopped Getty on tty1.
Jun 22 00:41:02 any systemd[1]: Started Getty on tty1.
Jun 22 00:41:05 any kernel: [26607.982747] usb 2-1: USB disconnect, device number 4
Jun 22 00:41:06 any kernel: [26608.616134] usb 2-1: new full-speed USB device number 5 using ohci-pci
Jun 22 00:41:06 any kernel: [26608.677686] e1000: enp0s3 NIC Link is Down
Jun 22 00:41:06 any systemd-networkd[665]: enp0s3: Lost carrier
Jun 22 00:41:06 any kernel: [26608.928320] usb 2-1: New USB device found, idVendor=80ee, idProduct=0021, bcdDevice= 1.00
Jun 22 00:41:06 any kernel: [26608.928322] usb 2-1: New USB device strings: Mfr=1, Product=3, SerialNumber=0
Jun 22 00:41:06 any kernel: [26608.928335] usb 2-1: Product: USB Tablet
Jun 22 00:41:06 any kernel: [26608.928337] usb 2-1: Manufacturer: VirtualBox
Jun 22 00:41:06 any kernel: [26608.942206] input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:06.0/usb2/2-1/2-1:1.0/0003:80EE:0021.0004/input/input10
Jun 22 00:41:06 any kernel: [26608.942858] hid-generic 0003:80EE:0021.0004: input,hidraw0: USB HID v1.10 Mouse [VirtualBox USB Tablet] on usb-0000:00:06.0-1/input0
Jun 22 00:41:12 any systemd[1724]: Stopped target Main User Target.
Jun 22 00:41:12 any systemd[1724]: Stopped target Basic System.
Jun 22 00:41:12 any systemd[1724]: Stopped target Paths.
Jun 22 00:41:12 any systemd[1724]: Stopped target Sockets.
Jun 22 00:41:12 any systemd[1724]: Stopped target Timers.
Jun 22 00:41:12 any systemd[1724]: dbus.socket: Succeeded.
Jun 22 00:41:12 any systemd[1]: Stopping User Manager for UID 1000...
Jun 22 00:41:12 any systemd[1724]: Closed D-Bus User Message Bus Socket.
Jun 22 00:41:12 any systemd[1724]: dirnmgr.socket: Succeeded.
Jun 22 00:41:12 any systemd[1724]: Closed GnuPG network certificate management daemon.
/var/log/syslog

```

### 3. /var/log/auth.log

~\$less /var/log/auth.log

```

Jun 19 12:57:17 winvairu useradd[671]: new group: name=cranbero, GID=1000
Jun 19 12:57:17 winvairu useradd[671]: new user: name=cranbero, UID=1000, GID=1000, home=/home/cranbero, shell=/bin/bash, from=none
Jun 19 12:57:17 winvairu useradd[671]: add 'cranbero' to group 'adm'
Jun 19 12:57:17 winvairu useradd[671]: add 'cranbero' to group 'cdrom'
Jun 19 12:57:17 winvairu useradd[671]: add 'cranbero' to group 'sudo'
Jun 19 12:57:17 winvairu useradd[671]: add 'cranbero' to group 'dip'
Jun 19 12:57:17 winvairu useradd[671]: add 'cranbero' to group 'plugdev'
Jun 19 12:57:17 winvairu useradd[671]: add 'cranbero' to group 'lxd'
Jun 19 12:57:17 winvairu useradd[671]: add 'cranbero' to shadow group 'adm'
Jun 19 12:57:17 winvairu useradd[671]: add 'cranbero' to shadow group 'cdrom'
Jun 19 12:57:17 winvairu useradd[671]: add 'cranbero' to shadow group 'sudo'
Jun 19 12:57:17 winvairu useradd[671]: add 'cranbero' to shadow group 'dip'
Jun 19 12:57:17 winvairu useradd[671]: add 'cranbero' to shadow group 'plugdev'
Jun 19 12:57:17 winvairu useradd[671]: add 'cranbero' to shadow group 'lxd'
Jun 19 12:57:17 winvairu systemd-logind[710]: New seat seat0.
Jun 19 12:57:17 winvairu systemd-logind[710]: Watching system buttons on /dev/input/event0 (Power Button)
Jun 19 12:57:17 winvairu systemd-logind[710]: Watching system buttons on /dev/input/event1 (Sleep Button)
Jun 19 12:57:17 winvairu systemd-logind[710]: Watching system buttons on /dev/input/event2 (AT Translated Set 2 keyboard)
Jun 19 12:57:21 winvairu useradd[1149]: new user: name=lxd, UID=998, GID=100, home=/var/snap/lxd/common/lxd, shell=/bin/false, from=none
Jun 19 13:00:51 winvairu login[779]: pam_unix(login:session): session opened for user cranbero by LD
GIN(uid=0)
Jun 19 13:00:51 winvairu systemd-logind[710]: New session 1 of user cranbero.
Jun 19 13:00:51 winvairu systemd: pam_unix(systemd-user:session): session opened for user cranbero by
y (uid=0)
Jun 19 13:15:36 winvairu sudo: cranbero : TTY=tty1 ; PWD=/home/cranbero ; USER=root ; COMMAND=/usr/b
in/apt update
Jun 19 13:15:36 winvairu sudo: pam_unix(sudo:session): session opened for user root by cranbero(uid=
0)
Jun 19 13:15:42 winvairu sudo: pam_unix(sudo:session): session closed for user root
Jun 19 13:15:42 winvairu sudo: cranbero : TTY=tty1 ; PWD=/home/cranbero ; USER=root ; COMMAND=/usr/b
in/apt upgrade
/var/log/auth.log

```

- Время последней успешной авторизации: **Jun 21 11:17:12**, имя пользователя: **newuser** и метод входа в систему: **local**

```
cranbero@winvairu-2:~$ grep -i "successful" /var/log/auth.log
Jun 19 17:07:01 winvairu polkitd(authority=local): Operator of unix-process:18907:1480053 successfully authenticated as unix-user:cranbero to gain TEMPORARY authorization for action org.freedesktop.hostname1.set-static-hostname for system-bus-name::1.43 [hostnamectl set-hostname winvairu-1] (owned by unix-user:cranbero)
Jun 21 11:17:12 any polkitd(authority=local): Operator of unix-process:3893:1745151 successfully authenticated as unix-user:newuser to gain TEMPORARY authorization for action org.freedesktop.hostname1.set-static-hostname for system-bus-name::1.54 [hostnamectl set-hostname winvairu-2] (owned by unix-user:newuser)
cranbero@winvairu-2:~$
```

- Перезапускаем службу sshd:

```
~$sudo systemctl restart sshd
```

- Скрин с сообщением о рестарте службы:

```
cranbero@winvairu-2:~$ sudo grep -r 'restart sshd' /var/log/auth.log
Jun 23 17:58:29 any sudo: cranbero : TTY=tty1 ; PWD=/home/cranbero ; USER=root ; COMMAND=/usr/bin/systemctl restart sshd
Jun 23 18:50:32 any sudo: cranbero : TTY=tty1 ; PWD=/home/cranbero ; USER=root ; COMMAND=/usr/bin/grep -r restart sshd /var/log/
Jun 23 18:51:33 any sudo: cranbero : TTY=tty1 ; PWD=/home/cranbero ; USER=root ; COMMAND=/usr/bin/grep -r restart sshd /var/log/
Jun 23 18:51:48 any sudo: cranbero : TTY=tty1 ; PWD=/home/cranbero ; USER=root ; COMMAND=/usr/bin/grep -r restart sshd /var/log/
Jun 23 18:52:43 any sudo: cranbero : TTY=tty1 ; PWD=/home/cranbero ; USER=root ; COMMAND=/usr/bin/grep -r restart sshd /var/log/auth.log
Jun 23 18:53:37 any sudo: cranbero : TTY=tty1 ; PWD=/home/cranbero ; USER=root ; COMMAND=/usr/bin/grep -r restart sshd /var/log/auth.log
cranbero@winvairu-2:~$
```

## Part 15. Использование планировщика заданий CRON

1. Создаем новый файл в директории /etc/cron.d/ с именем uptime\_checker.
2. Добавляем следующую строку в файл: **\*/2 \* \* \* \* root uptime >> /var/log/uptime.log 2>&1**

Эта строка означает следующее:

- **\*/2**: запускать каждые 2 минуты.
- **\* \* \* \* \***: указывает на то, что задача должна выполняться каждый час, каждый день, каждый месяц, каждый день недели.
- **root**: указывает, что задача должна выполняться от имени пользователя root.

- **uptime**: команда, которую нужно выполнить.
- **>> /var/log/uptime.log**: записывать вывод команды в файл **/var/log/uptime.log**.

3. Запускаем команду **sudo crontab /etc/cron.d/uptime\_checker** для применения изменений.

```
cranbero@winvairu-2:~$ sudo crontab -l
*/2 * * * * root uptime >> /var/log/uptime.log 2>&1
cranbero@winvairu-2:~$ sudo cat /var/log/uptime.log
/bin/sh: 1: root: not found
19:46:04 up 21:57,  1 user,  load average: 0.00, 0.00, 0.00
/bin/sh: 1: root: not found
19:48:01 up 21:59,  1 user,  load average: 0.00, 0.00, 0.00
/bin/sh: 1: root: not found
19:50:01 up 22:01,  1 user,  load average: 0.00, 0.00, 0.00
/bin/sh: 1: root: not found
19:52:01 up 22:03,  1 user,  load average: 0.00, 0.00, 0.00
/bin/sh: 1: root: not found
19:54:01 up 22:05,  1 user,  load average: 0.00, 0.00, 0.00
cranbero@winvairu-2:~$ _
```

4. Удаляем все задания из планировщика заданий. Скрин со списком текущих заданий для CRON.

```
cranbero@winvairu-2:~$ sudo crontab -r
cranbero@winvairu-2:~$ sudo crontab -l
no crontab for root
cranbero@winvairu-2:~$
```