

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ
Факультет физико-математических и естественных наук Кафедра
прикладной информатики и теории вероятностей

ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 1
дисциплина: Информационная безопасность

Студент: Петрова М.Е.

Группа: НФИбд-02-21

МОСКВА

2024 г.

Постановка задачи

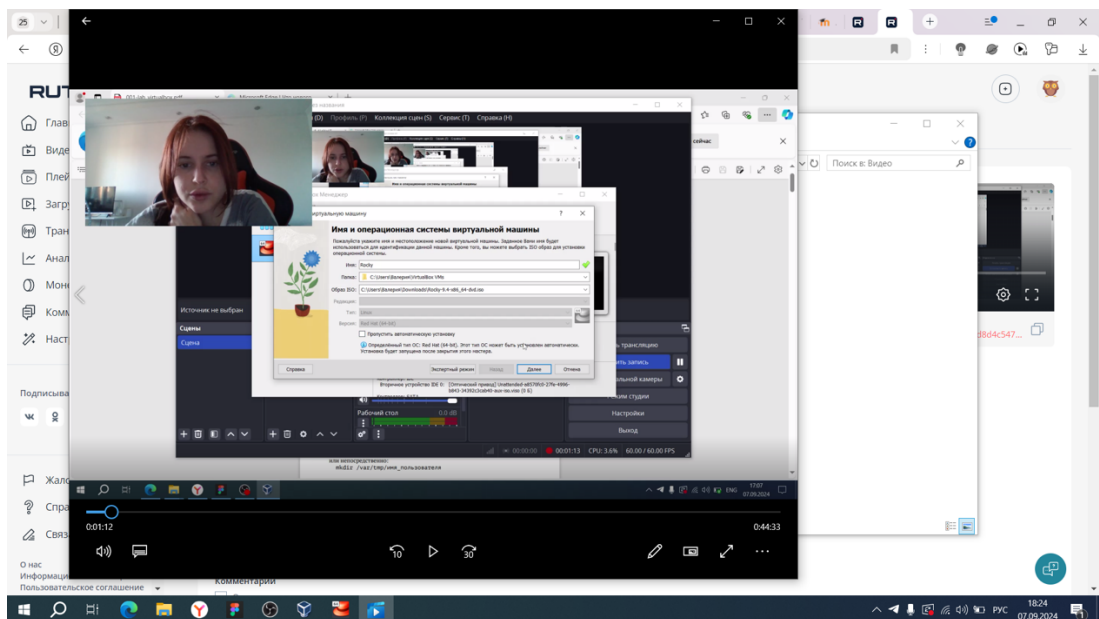
Целью данной работы является приобретение практических навыков установки операционной системы на виртуальную машину, настройки минимально необходимых для дальнейшей работы сервисов.

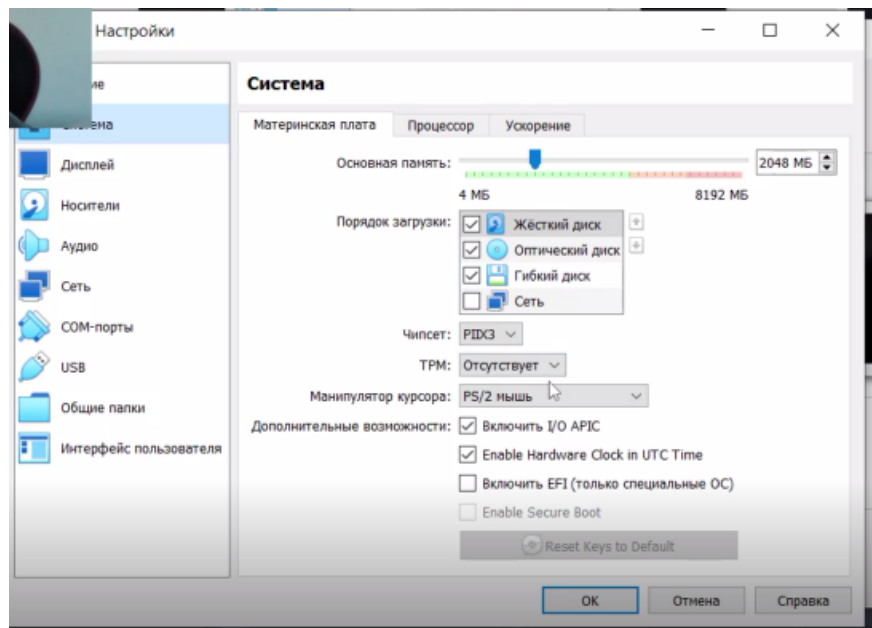
Теоретическое введение

Программа VirtualBox предоставляет широкий спектр возможностей для работы с виртуальными машинами. Это решение подходит для тестирования новых операционных систем, запуска старых приложений или изоляции потенциально опасного программного обеспечения. Благодаря интуитивно понятному интерфейсу и богатому функционалу, VirtualBox стал выбором многих пользователей по всему миру

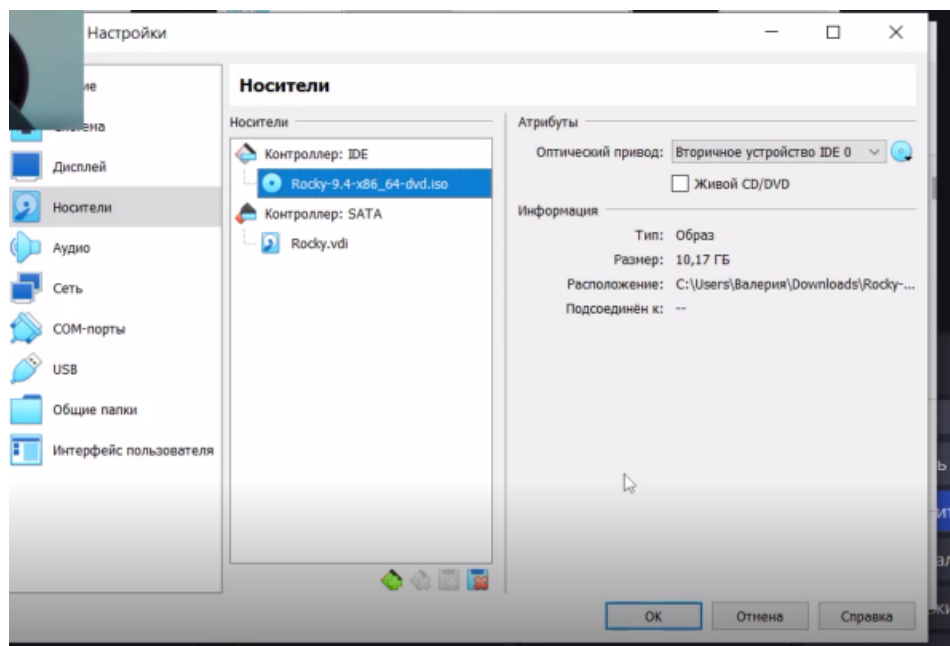
Выполнение работы

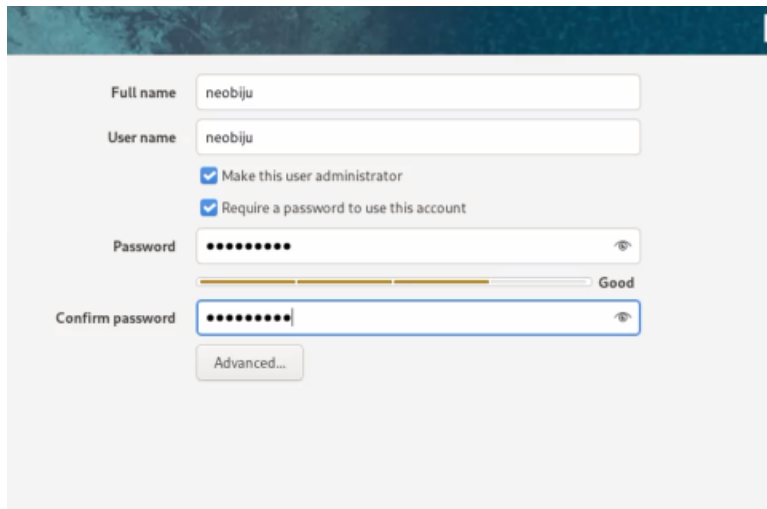
Запускаем виртуальную машину, нажимаем кнопку "создать" и выбираем скаченный образ ISO





Меняем контроллер на скаченный образ Rocky





Full name: neobiju

User name: neobiju

☒ Make this user administrator

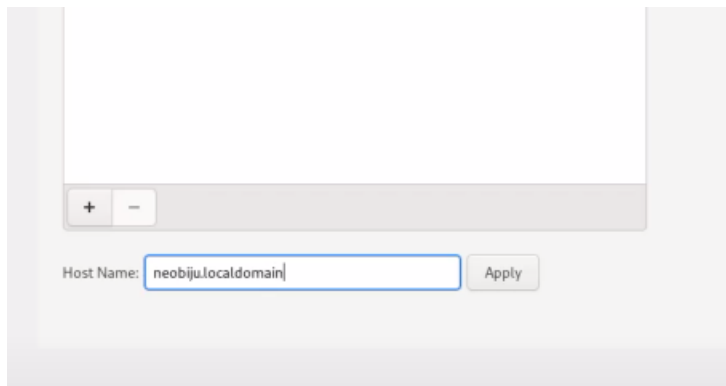
☒ Require a password to use this account

Password: [masked] Good

Confirm password: [masked]

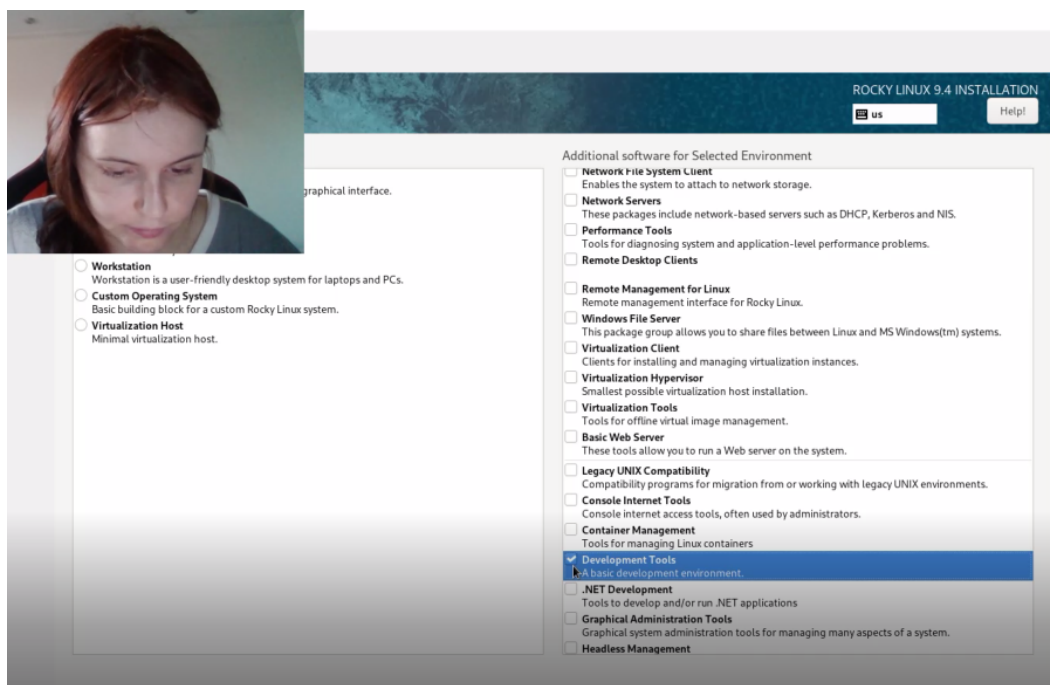
Advanced...

Заходим в Network&Host Name и прописываем host name:



Host Name: neobiju.localdomain Apply

В Software Selection выбираем Server with GUI. В дополнительном ПО отмечаем Development Tools:



ROCKY LINUX 9.4 INSTALLATION

us Help

graphical interface.

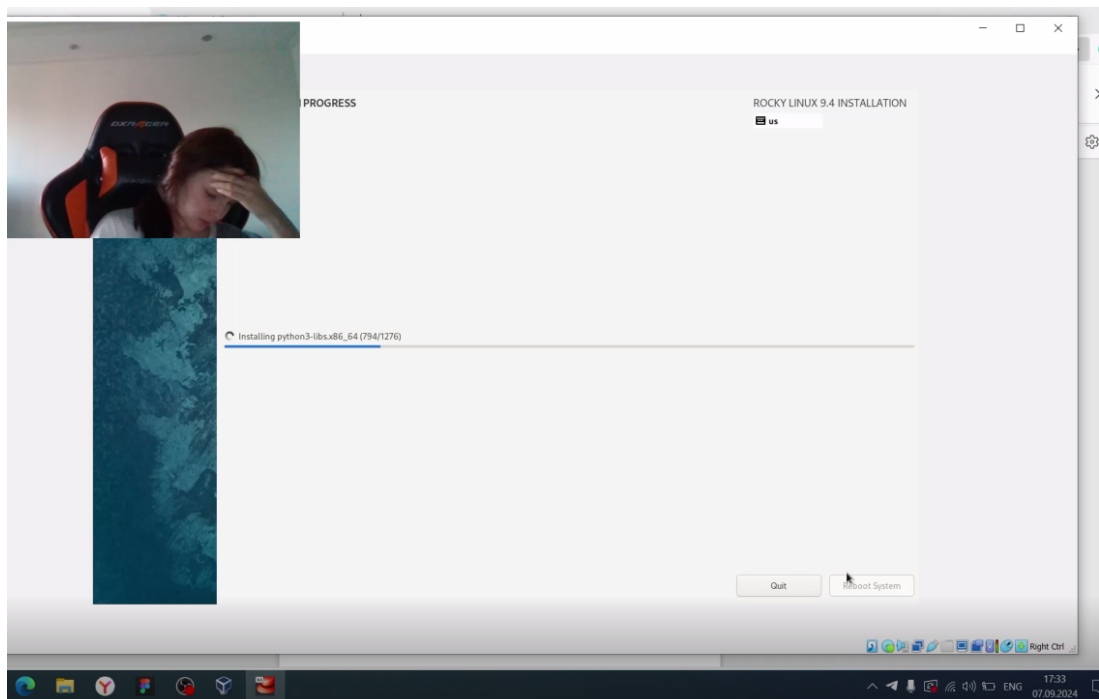
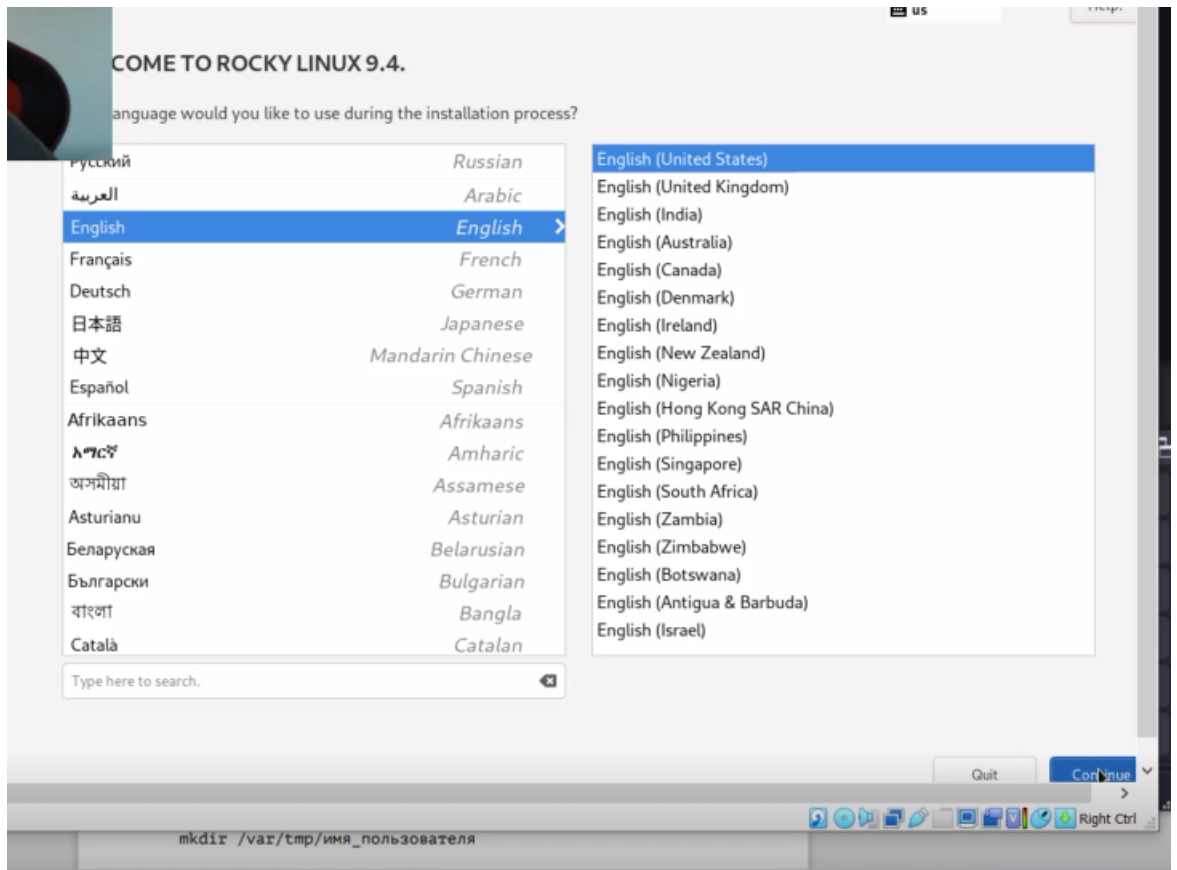
☐ Workstation
Workstation is a user-friendly desktop system for laptops and PCs.

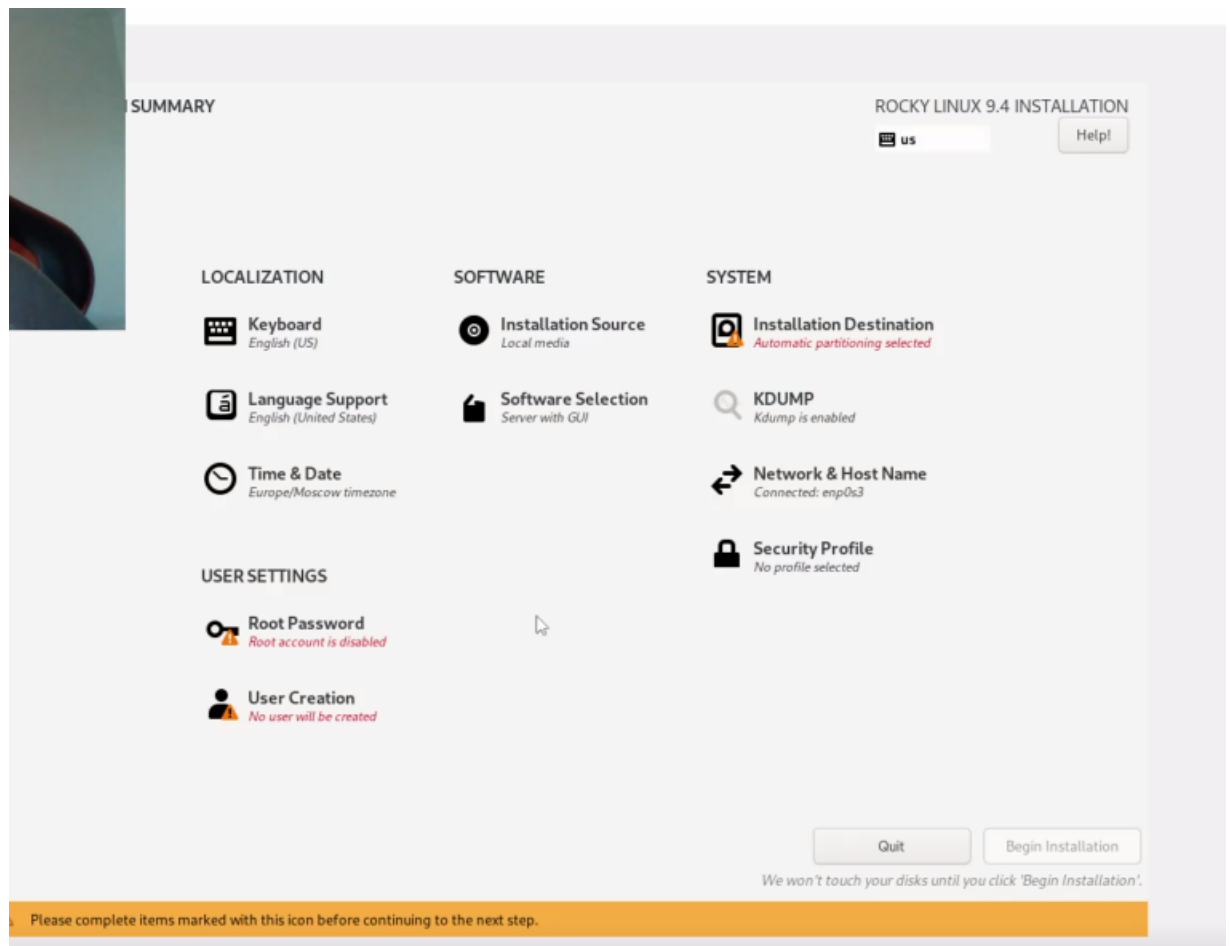
☐ Custom Operating System
Basic building block for a custom Rocky Linux system.

☐ Virtualization Host
Minimal virtualization host.

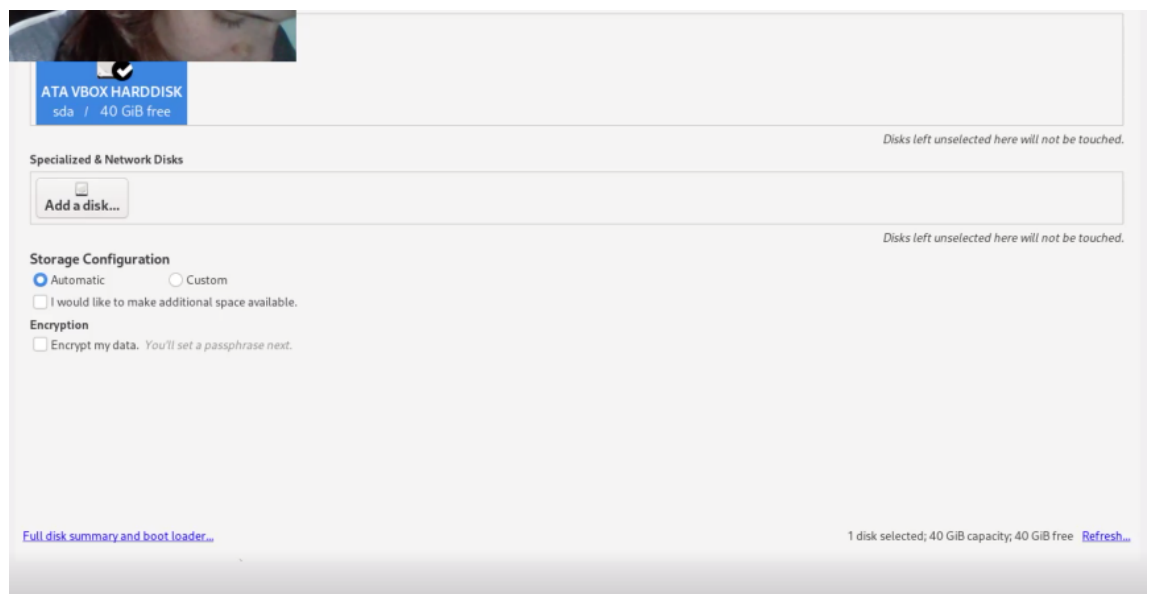
Additional software for Selected Environment

- ☐ Network File System Client
Enables the system to attach to network storage.
- ☐ Network Servers
These packages include network-based servers such as DHCP, Kerberos and NIS.
- ☐ Performance Tools
Tools for diagnosing system and application-level performance problems.
- ☐ Remote Desktop Clients
- ☐ Remote Management for Linux
Remote management interface for Rocky Linux.
- ☐ Windows File Server
This package group allows you to share files between Linux and MS Windows(tm) systems.
- ☐ Virtualization Client
Clients for installing and managing virtualization instances.
- ☐ Virtualization Hypervisor
Smallest possible virtualization host installation.
- ☐ Virtualization Tools
Tools for offline virtual image management.
- ☐ Basic Web Server
These tools allow you to run a Web server on the system.
- ☐ Legacy UNIX Compatibility
Compatibility programs for migration from or working with legacy UNIX environments.
- ☐ Console Internet Tools
Console internet access tools, often used by administrators.
- ☐ Container Management
Tools for managing Linux containers
- ☒ Development Tools
A basic development environment.
- ☐ .NET Development
Tools to develop and/or run .NET applications
- ☐ Graphical Administration Tools
Graphical system administration tools for managing many aspects of a system.
- ☐ Headless Management





В Installation Destination выбираем диск



The root account is used for administering the system. Enter a password for the root user.

Root Password: Good

Confirm:

☐ Lock root account

☐ Allow root SSH login with password

1. Версия ядра Linux (Linux version).
2. Частота процессора (Detected Mhz processor).
3. Модель процессора (CPU0).
4. Объем доступной оперативной памяти (Memory available).
5. Тип обнаруженного гипервизора (Hypervisor detected).
6. Тип файловой системы корневого раздела.
7. Последовательность монтирования файловых систем

```

[neobiju@neobiju ~]$ dmesg
bash: dmesg: command not found...
Similar command is: 'dmesg'
[neobiju@neobiju ~]$ dmesg
0.000000 Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iadi-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.4.1 20231218 (Red Hat 11.4.1-3),
GNU ld version 2.35.2-43.el9) #1 SMP PREEMPT_DYNAMIC Wed May 1 19:11:28 UTC 2024
0.000000 The list of certified hardware and cloud instances for Enterprise Linux 9 can be viewed at the Red Hat Ecosystem Catalog, https://catalog.redha
t.com.
0.000000 Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-427.13.1.el9_4.x86_64 root=/dev/mapper/rl-root ro resume=/dev/mapper/rl-swap rd.lvm.lv=rl/
root rd.lvm.lv=rl/swap rhgb quiet
0.000000 [Firmware Bug]: TSC doesn't count with P0 frequency!
0.000000 x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
0.000000 x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
0.000000 x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
0.000000 x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
0.000000 x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'standard' format.
0.000000 signal: max sigframe size: 1776
0.000000 BIOS-provided physical RAM map:
0.000000 BIOS-e820: [mem 0x00000000-0x00000000-0x00000000fbfff] usable
0.000000 BIOS-e820: [mem 0x00000000000fc00-0x00000000000ffff] reserved
0.000000 BIOS-e820: [mem 0x00000000000f000-0x00000000000ffff] reserved
0.000000 BIOS-e820: [mem 0x000000000010000-0x00000000007ffff] usable
0.000000 BIOS-e820: [mem 0x0000000007ffff000-0x0000000007fffffff] ACPI data
0.000000 BIOS-e820: [mem 0x00000000fec0000-0x00000000fec0fff] reserved
0.000000 BIOS-e820: [mem 0x00000000fee0000-0x00000000fee0fff] reserved
0.000000 BIOS-e820: [mem 0x00000000fffc000-0x00000000fffcfff] reserved
0.000000 NX (Execute Disable) protection: active
0.000000 SMBIOS 2.5 present.
0.000000 DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
0.000000 Hypervisor detected: KVM
0.000000 kvm-clock: Using msrs 4b564d01 and 4b564d00
0.000002 kvm-clock: using sched offset of 5052300954 cycles
0.000004 clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 881590591483 ns
0.000006 tsc: Detected 2096.064 MHz processor
0.001002 e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
0.001094 e820: remove [mem 0x000a0000-0x000ffff] usable
0.001098 last_pfn = 0x7fff0 max_arch_pfn = 0x400000000
0.001115 MTRRs disabled by BIOS
0.001119 x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
0.001187 found SMP MP-table at [mem 0x0009fff0-0x0009ffff]

```



```
Activities Terminal Sep 7 18:03 en neobiju@neobiju:~
neobiju@neobiju:~
6.739450] XFS (sdal): Mounting V5 Filesystem d9c6ac3c-9399-4778-8e6f-6c208c5a9d27
6.821316] XFS (sdal): Ending clean mount
8.596697] NET: Registered PF_QIPCRTR protocol family
9.469945] Warning: Unmaintained driver is detected: ip_set
9.608621] e1000: enp0s3 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
9.609800] IPv6: ADDRCONF(NETDEV_CHANGE): enp0s3: link becomes ready
13.576462] rfkill: input handler disabled
46.074325] rfkill: input handler enabled
49.918758] rfkill: input handler disabled
[neobiju@neobiju ~]$ dmesg | less
[neobiju@neobiju ~]$ dmesg | grep -i "Linux version"
[ 0.000000] Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.4.1 20231218 (Red Hat 11.4.1-3),
GNU ld version 2.35.2-43.el9) #1 SMP PREEMPT_DYNAMIC Wed May 1 19:11:28 UTC 2024
[neobiju@neobiju ~]$ dmesg | grep -i "Detected Mhz processor"
[neobiju@neobiju ~]$ dmesg | grep -i "Detected"
[ 0.000000] Hypervisor detected: KVM
[ 0.000006] tsc: Detected 2096.064 Mhz processor
[ 0.508512] hub 1-0:1.0: 12 ports detected
[ 0.517254] hub 2-0:1.0: 12 ports detected
[ 1.341502] systemd[1]: Detected virtualization oracle.
[ 1.341505] systemd[1]: Detected architecture x86-64.
[ 2.113599] Warning: Unmaintained driver is detected: e1000
[ 4.005154] systemd[1]: Detected virtualization oracle.
[ 4.005162] systemd[1]: Detected architecture x86-64.
[ 9.469945] Warning: Unmaintained driver is detected: ip_set
[neobiju@neobiju ~]$ dmesg | grep -i "CPU0"
[ 0.047404] CPU0: Hyper-Threading is disabled
[ 0.172895] smpboot: CPU0: AMD Ryzen 5 5500U with Radeon Graphics (family: 0x17, model: 0x68, stepping: 0x1)
[neobiju@neobiju ~]$ dmesg | grep -i "available"
[ 0.001843] On node 0, zone DMA: 1 pages in unavailable ranges
[ 0.001913] On node 0, zone DMA: 97 pages in unavailable ranges
[ 0.002868] On node 0, zone DMA32: 16 pages in unavailable ranges
[ 0.003330] [mem 0x80000000-0xfabfffff] available for PCI devices
[ 0.013661] Memory: 268860K/2096696K available (16384K kernel code, 5626K rwdata, 11748K rodata, 3892K init, 5956K bss, 145300K reserved, 0K cma-reserved)
[ 0.173230] Performance Events: PMU not available due to virtualization, using software events only.
[ 2.502883] vmwgfx 0000:00:02.0: [drm] Available shader model: Legacy.
[neobiju@neobiju ~]$ dmesg | grep -i "Hypervisor detected"
[ 0.000000] Hypervisor detected: KVM
[neobiju@neobiju ~]$
```

```
Activities Terminal Sep 7 18:04 en neobiju@neobiju:~
neobiju@neobiju:~
49.918758] rfkill: input handler disabled
[neobiju@neobiju ~]$ dmesg | less
[neobiju@neobiju ~]$ dmesg | grep -i "Linux version"
[ 0.000000] Linux version 5.14.0-427.13.1.el9_4.x86_64 (mockbuild@iad1-prod-build001.bld.equ.rockylinux.org) (gcc (GCC) 11.4.1 20231218 (Red Hat 11.4.1-3),
GNU ld version 2.35.2-43.el9) #1 SMP PREEMPT_DYNAMIC Wed May 1 19:11:28 UTC 2024
[neobiju@neobiju ~]$ dmesg | grep -i "Detected Mhz processor"
[neobiju@neobiju ~]$ dmesg | grep -i "Detected"
[ 0.000000] Hypervisor detected: KVM
[ 0.000006] tsc: Detected 2096.064 Mhz processor
[ 0.508512] hub 1-0:1.0: 12 ports detected
[ 0.517254] hub 2-0:1.0: 12 ports detected
[ 1.341502] systemd[1]: Detected virtualization oracle.
[ 1.341505] systemd[1]: Detected architecture x86-64.
[ 2.113599] Warning: Unmaintained driver is detected: e1000
[ 4.005154] systemd[1]: Detected virtualization oracle.
[ 4.005162] systemd[1]: Detected architecture x86-64.
[ 9.469945] Warning: Unmaintained driver is detected: ip_set
[neobiju@neobiju ~]$ dmesg | grep -i "CPU0"
[ 0.047404] CPU0: Hyper-Threading is disabled
[ 0.172895] smpboot: CPU0: AMD Ryzen 5 5500U with Radeon Graphics (family: 0x17, model: 0x68, stepping: 0x1)
[neobiju@neobiju ~]$ dmesg | grep -i "available"
[ 0.001843] On node 0, zone DMA: 1 pages in unavailable ranges
[ 0.001913] On node 0, zone DMA: 97 pages in unavailable ranges
[ 0.002868] On node 0, zone DMA32: 16 pages in unavailable ranges
[ 0.003330] [mem 0x80000000-0xfabfffff] available for PCI devices
[ 0.013661] Memory: 268860K/2096696K available (16384K kernel code, 5626K rwdata, 11748K rodata, 3892K init, 5956K bss, 145300K reserved, 0K cma-reserved)
[ 0.173230] Performance Events: PMU not available due to virtualization, using software events only.
[ 2.502883] vmwgfx 0000:00:02.0: [drm] Available shader model: Legacy.
[neobiju@neobiju ~]$ dmesg | grep -i "Hypervisor detected"
[ 0.000000] Hypervisor detected: KVM
[neobiju@neobiju ~]$ df -Th
Filesystem Type Size Used Avail Use% Mounted on
devtmpfs devtmpfs 4.0M 0 4.0M 0% /dev
tmpfs tmpfs 984M 0 984M 0% /dev/shm
tmpfs tmpfs 394M 6.1M 388M 2% /run
/dev/mapper/rl-root xfs 37G 5.9G 32G 16% /
/dev/sdal xfs 960M 272M 689M 29% /boot
tmpfs tmpfs 197M 120K 197M 1% /run/user/1000
[neobiju@neobiju ~]$
```

```
Activities Terminal Sep 7 18:04 en neobiju@neobiju:~
neobiju@neobiju:~
neobiju@neobiju:~
tmpfs tmpfs 984M 0 984M 0% /dev/shm
tmpfs tmpfs 394M 6.1M 388M 2% /run
/dev/mapper/rl-root xfs 37G 5.9G 32G 16% /
/dev/sda1 xfs 960M 272M 689M 29% /boot
tmpfs tmpfs 197M 120K 197M 1% /run/user/1000
[neobiju@neobiju ~]$ findmnt
TARGET SOURCE FSTYPE OPTIONS
/dev/mapper/rl-root xfs rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota
/proc proc rw,nosuid,nodev,noexec,relatime
/proc/sys/fs/binfmt_misc systemd-1 autofs rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=18806
/sys sysfs sysfs rw,nosuid,nodev,noexec,relatime,seclabel
/sys/kernel/security securityfs securityfs rw,nosuid,nodev,noexec,relatime
/sys/fs/cgroup cgroup2 cgroup2 rw,nosuid,nodev,noexec,relatime,seclabel,nsdelegate,memory_recursiveprot
/sys/fs/pstore pstore pstore rw,nosuid,nodev,noexec,relatime,seclabel
/sys/fs/bpf bpf bpf rw,nosuid,nodev,noexec,relatime,mode=700
/sys/fs/selinux selinuxfs selinuxfs rw,nosuid,noexec,relatime
/sys/kernel/debug debugfs debugfs rw,nosuid,nodev,noexec,relatime,seclabel
/sys/kernel/tracing tracefs tracefs rw,nosuid,nodev,noexec,relatime,seclabel
/sys/fs/fuse/connections fusectl fusectl rw,nosuid,nodev,noexec,relatime
/sys/kernel/config configfs configfs rw,nosuid,nodev,noexec,relatime
/dev devtmpfs devtmpfs rw,nosuid,seclabel,size=4096k,nr_inodes=243929,mode=755,inode64
/dev/shm tmpfs tmpfs rw,nosuid,nodev,relatime,seclabel,inode64
/dev/pts devpts devpts rw,nosuid,nodev,relatime,seclabel,gid=5,mode=620,ptmxmode=000
/dev/mqueue mqueue mqueue rw,nosuid,nodev,noexec,relatime,seclabel
/dev/hugepages hugetlbfs hugetlbfs rw,relatime,seclabel,pagesize=2M
/run tmpfs tmpfs rw,nosuid,nodev,seclabel,size=402992k,nr_inodes=819200,mode=755,inode64
/run/credentials/systemd-sysctl.service none ramfs ro,nosuid,nodev,noexec,relatime,seclabel,mode=700
/run/credentials/systemd-tmpfiles-setup-dev.service none ramfs ro,nosuid,nodev,noexec,relatime,seclabel,mode=700
/run/credentials/systemd-sysusers.service none ramfs ro,nosuid,nodev,noexec,relatime,seclabel,mode=700
/run/credentials/systemd-tmpfiles-setup.service none ramfs ro,nosuid,nodev,noexec,relatime,seclabel,mode=700
/run/user/1000 tmpfs tmpfs rw,nosuid,nodev,relatime,seclabel,size=201496k,nr_inodes=50374,mode=700,uid=1000,gid=1000,inode64
/run/user/1000/gvfs gvfsd-fuse fuse.gvfsd-fuse rw,nosuid,nodev,relatime,user_id=1000,group_id=1000
/boot /dev/sda1 xfs rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota
[neobiju@neobiju ~]$
```

Заключение

Приобрели практические навыки установки операционной системы на виртуальную машину, настроили минимально необходимые для дальнейшей работы сервисы.

Ответы на вопросы

1. Какую информацию содержит учётная запись пользователя?

Учётная запись пользователя в Linux содержит следующую информацию:

- Имя пользователя (username) — уникальное имя пользователя в системе.

- Идентификатор пользователя (UID) — уникальный числовой идентификатор для каждого пользователя.

- Идентификатор группы (GID) — идентификатор основной группы, к которой принадлежит пользователь.

- Домашний каталог (home directory) — директория, в которой пользователь хранит свои файлы и настройки.

- Интерпретатор команд (shell) — программа, запускаемая по умолчанию при входе пользователя в систему.

- Пароль пользователя — обычно хранится в хешированном виде в файле `/etc/shadow`.

Эти данные обычно содержатся в файле `/etc/passwd`, а зашифрованные пароли — в файле `/etc/shadow`.

2. Укажите команды терминала и приведите примеры:

— для получения справки по команде;

— для перемещения по файловой системе;

— для просмотра содержимого каталога;

— для определения объёма каталога;

— для создания / удаления каталогов / файлов;

— для задания определённых прав на файл / каталог;

— для просмотра истории команд.

Для получения справки по команде: `man <имя_команды>`

Пример: `man ls` — получить справку по команде `ls`.

Для перемещения по файловой системе: `cd <путь_к_каталогу>`

Пример: `cd /home/user` — перейти в каталог `/home/user`.

Для просмотра содержимого каталога: `ls [опции]`
`<путь_к_каталогу>`

Пример: `ls -la /home/user` — показать все файлы и каталоги, включая скрытые, с подробной информацией.

Для определения объёма каталога: `du -sh <путь_к_каталогу>`

Пример: `du -sh /home/user` — показать общий размер каталога `/home/user`.

Для создания / удаления каталогов / файлов:

`mkdir <имя_каталога>` - Создание каталога

`rmdir <имя_каталога>` - Удаление пустого каталога

`touch <имя_файла>` - Создание пустого файла

`rm <имя_файла>` - Удаление файла

`rm -r <имя_каталога>` - Рекурсивное удаление каталога и его содержимого

Примеры:

`mkdir new_folder`

```
touch new_file.txt
```

```
rm new_file.txt
```

```
rm -r new_folder
```

Для задания определённых прав на файл / каталог: `chmod <права> <имя_файла_или_каталога>`

Пример: `chmod 755 script.sh` — установить права `rw xr-xr-x` на файл `script.sh`.

Для просмотра истории команд: `history`

3. Что такое файловая система? Приведите примеры с краткой характеристикой.

Файловая система — это метод и структура, по которым данные хранятся, организуются и управляются на носителе информации (жесткий диск, SSD, USB-накопитель и т.д.).

Примеры файловых систем:

EXT4 (Fourth Extended Filesystem): Одна из самых популярных файловых систем в Linux. Поддерживает журналирование, большие объёмы данных, улучшенную производительность. Хорошо подходит для большинства стандартных Linux-установок.

NTFS (New Technology File System): Файловая система, используемая в операционных системах Windows. Поддерживает большие файлы, разрешения, шифрование и сжатие.

FAT32 (File Allocation Table 32): Универсальная файловая система, поддерживаемая практически всеми операционными системами.

Ограничение на размер файла — до 4 ГБ.

XFS: Журналируемая файловая система с высокой производительностью, разработанная для систем с большими объемами данных.

Хорошо подходит для серверных систем и больших файловых хранилищ.

ZFS: Передовая файловая система, поддерживающая большой объем данных, снапшоты, клонирование и защиту данных. Разработана для высоконадежных систем.

4. Как посмотреть, какие файловые системы подмонтированы в ОС?

Чтобы посмотреть, какие файловые системы подмонтированы в операционной системе Linux, можно воспользоваться несколькими способами. Во-первых, можно использовать команду `mount`, которая выводит список всех текущих монтированных файловых систем, их устройства, точки монтирования, типы файловых систем и параметры монтирования. Например, при вводе команды `mount` в терминале вы получите информацию о том, какие файловые системы были смонтированы и в каком порядке.

Во-вторых, можно просмотреть содержимое файла `/proc/mounts`, который также содержит сведения о всех монтированных файловых системах, включая псевдо-файловые системы вроде `proc` и `sysfs`. Это можно сделать, выполнив команду `cat /proc/mounts` в терминале. Наконец, команду `df -h` можно использовать для отображения информации о свободном и занятом пространстве на смонтированных файловых системах, что может быть полезным для мониторинга состояния системы.

5. Как удалить зависший процесс?

Для удаления зависшего процесса в Linux сначала нужно определить его идентификатор (PID). Это можно сделать с помощью команды `ps aux`, которая выводит список всех запущенных процессов в системе вместе с их PID, или с помощью утилит `top` или `htop`, которые предоставляют интерактивный список процессов.

После того как PID зависшего процесса известен, можно использовать команду `kill <PID>` для отправки сигнала завершения процессу. Если процесс не реагирует на обычный сигнал завершения, его можно принудительно завершить, используя команду `kill -9 <PID>`. Этот сигнал (-9) немедленно завершает процесс, игнорируя любые попытки его сохранения или корректного завершения.