

Отчёт по лабораторной работе №11

Основы информационной безопасности

Луангсуваннавонг Сайпхачан, НКАбд-01-24

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
3.1	Установка и настройка операционной системы	7
3.2	Выполнение дополнительной задачи	15
3.3	Ответы на контрольные вопросы	17
4	Выводы	20

Список иллюстраций

3.1	Установите DVD-диск с операционной системой	7
3.2	Имя пользователя и имя хоста	8
3.3	Настройка оборудования	8
3.4	Настройка оборудования	9
3.5	Подключение диска к носителю	9
3.6	Установка Rocky Linux	10
3.7	Выбор языка	10
3.8	Выбор раскладки клавиатуры	11
3.9	Выбор окружения	11
3.10	Проверка жесткого диска на предмет установки	11
3.11	отключение kdump	12
3.12	Настройка сети	12
3.13	Пароль для администратора	13
3.14	Создание пользователя	13
3.15	Проверка конфигурации	14
3.16	Завершение установки	14
3.17	Вход в аккунт	14
3.18	Установка гостевых дополнений ОС	15
3.19	Установка гостевых дополнений ОС	15
3.20	Версия ядра Linux	15
3.21	Частота процессора	16
3.22	Модель процессора	16
3.23	Объем доступной оперативной памяти	16
3.24	Тип обнаруженного гипервизора	16
3.25	тип файловой системы	17
3.26	Последовательность монтирования файловых систем.	17

Список таблиц

1 Цель работы

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

2 Задание

1. Установка и настройка операционной системы
2. найти информацию:
 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.

3 Выполнение лабораторной работы

3.1 Установка и настройка операционной системы

Я создаю новую виртуальную машину в Virtualbox, затем выбираю имя, расположение папки и ISO-образ, на который я устанавливаю Rocky Linux DVD.(рис. 3.1).

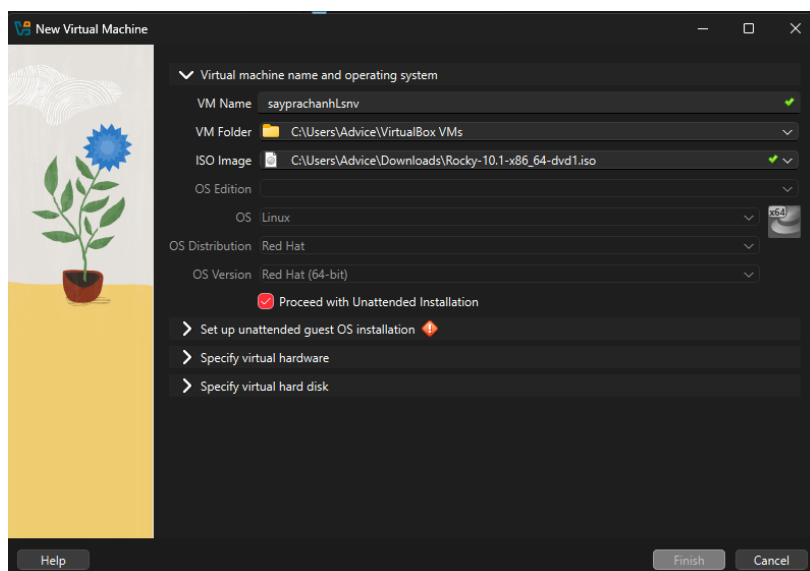


Рисунок 3.1: Установите DVD-диск с операционной системой

Я задаю имя пользователя и имя хоста(рис. 3.2).

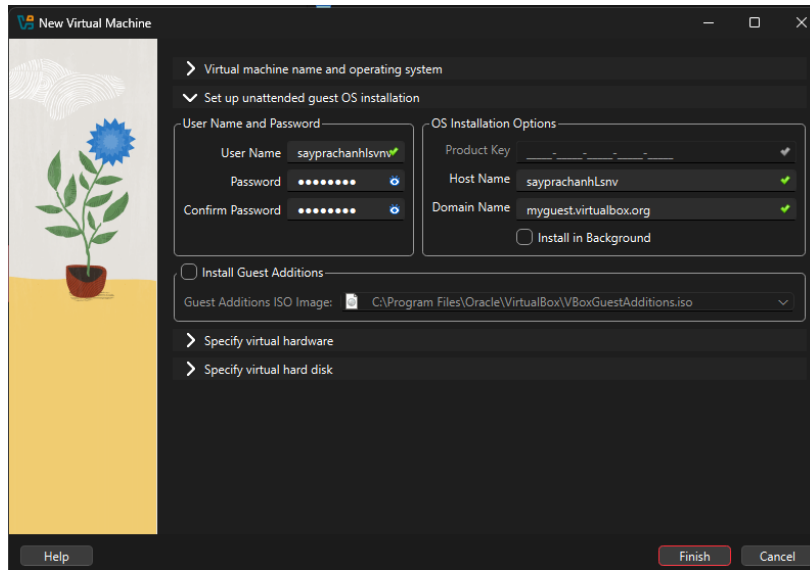


Рисунок 3.2: Имя пользователя и имя хоста

Я настраиваю аппаратную память и количество ядер процессора (поскольку предпочитаю использовать больше памяти, я устанавливаю значение выше необходимого), а также задаю расположение и размер файла жесткого диска (который я тоже делаю большим)(рис. 3.3 и рис. 3.4).

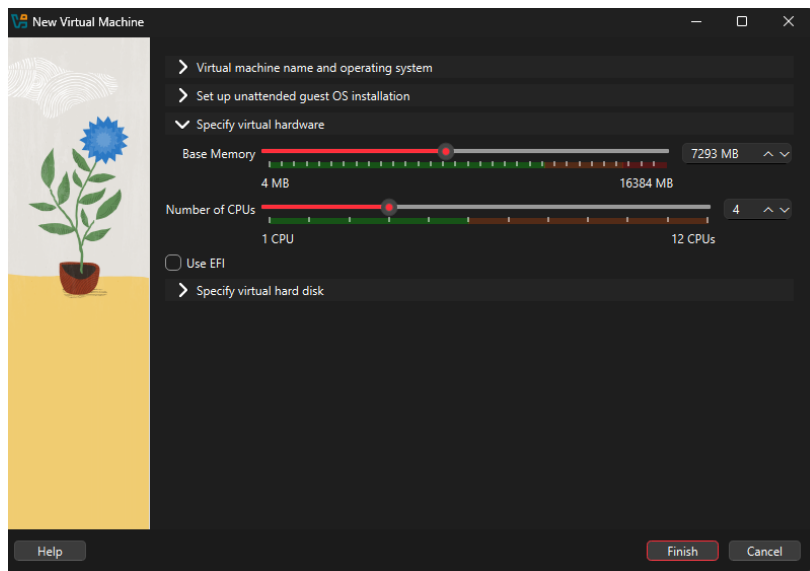


Рисунок 3.3: Настройка оборудования

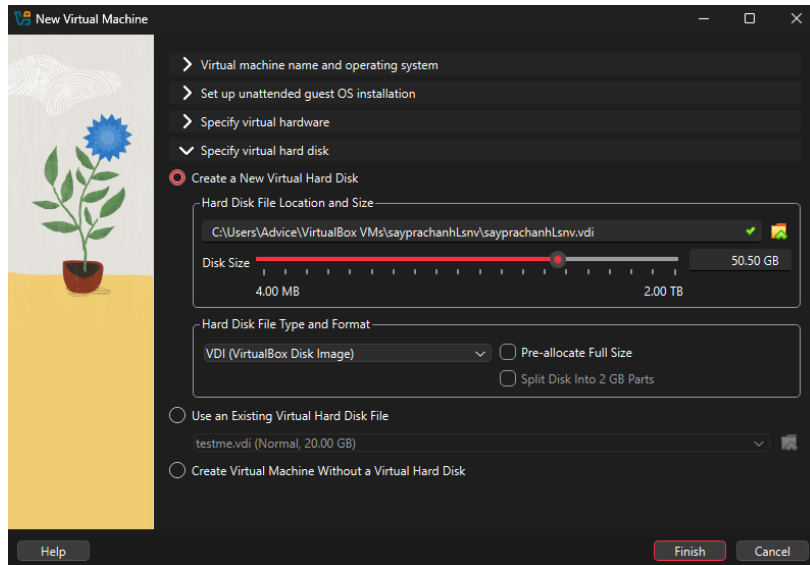


Рисунок 3.4: Настройка оборудования

Затем я подключаю образ диска к встроенному носителю, так как в первый раз он не запустился(рис. 3.5).

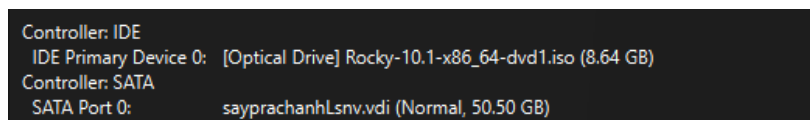


Рисунок 3.5: Подключение диска к носителю

устанавливаю Rocky Linux 10.1(рис. 3.6).

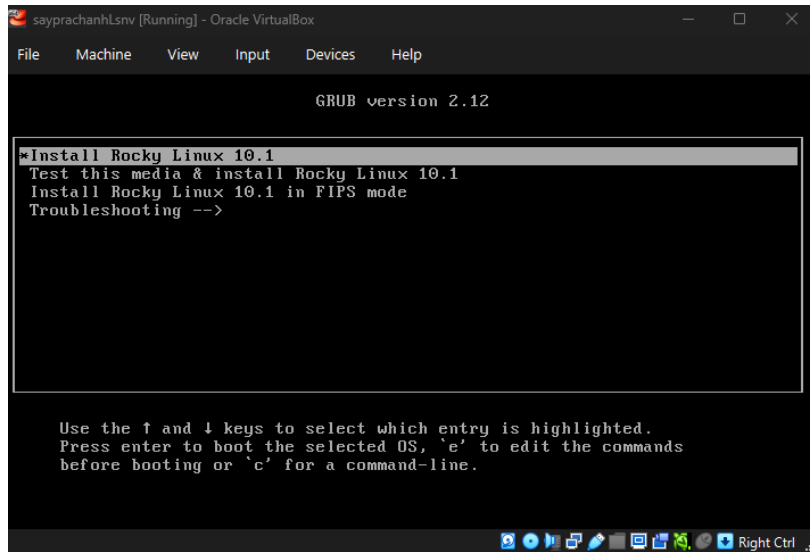


Рисунок 3.6: Установка Rocky Linux

Я выбираю язык установки(рис. 3.7).

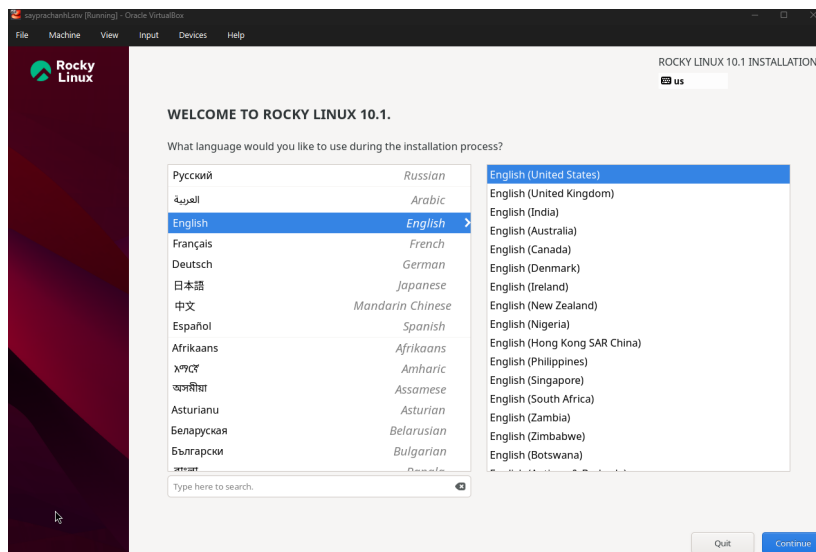


Рисунок 3.7: Выбор языка

выбираю раскладку клавиатуры(рис. 3.8).

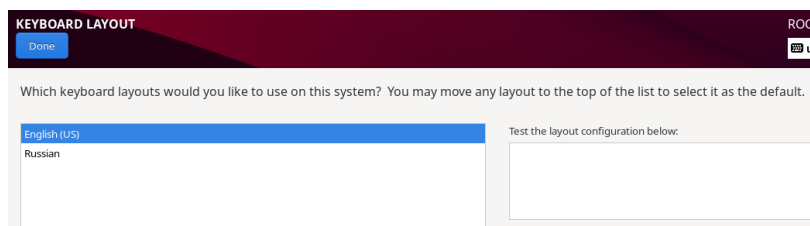


Рисунок 3.8: Выбор раскладки клавиатуры

В соответствии с требованием лабораторной работы выбираю окружение сервер с GUI и средства разработки в дополнительном программном обеспечении(рис. 3.9).

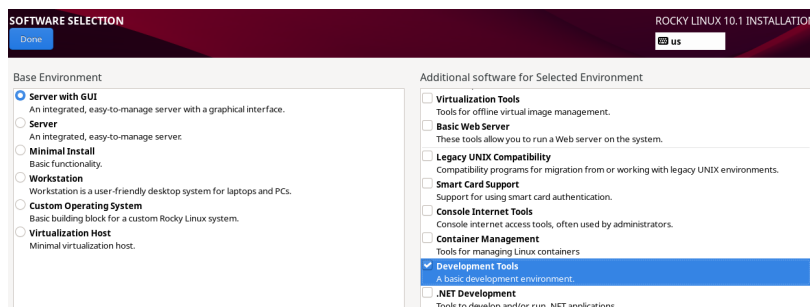


Рисунок 3.9: Выбор окружения

Я проверяю и снова выбираю жесткий диск для расположения установки(рис. 3.10).

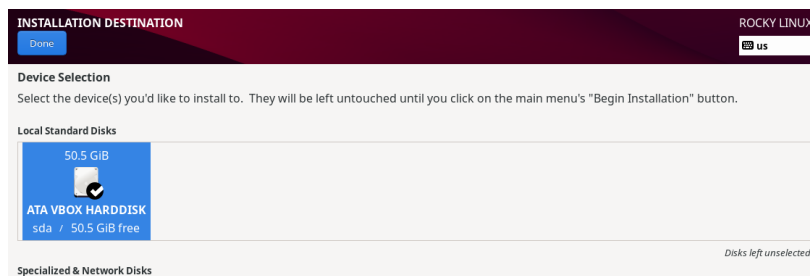


Рисунок 3.10: Проверка жесткого диска на предмет установки

Я отключаю kdump(рис. 3.11).

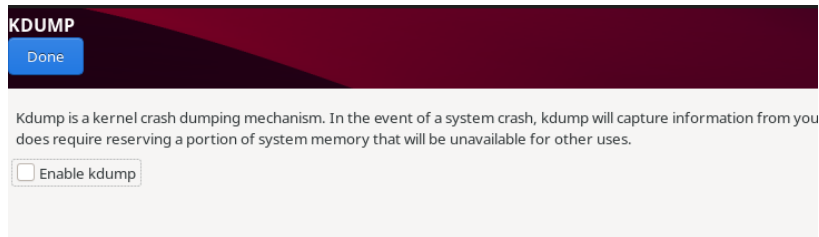


Рисунок 3.11: отключение kdump

Я проверяю сеть, указываю имя хоста(рис. 3.12).

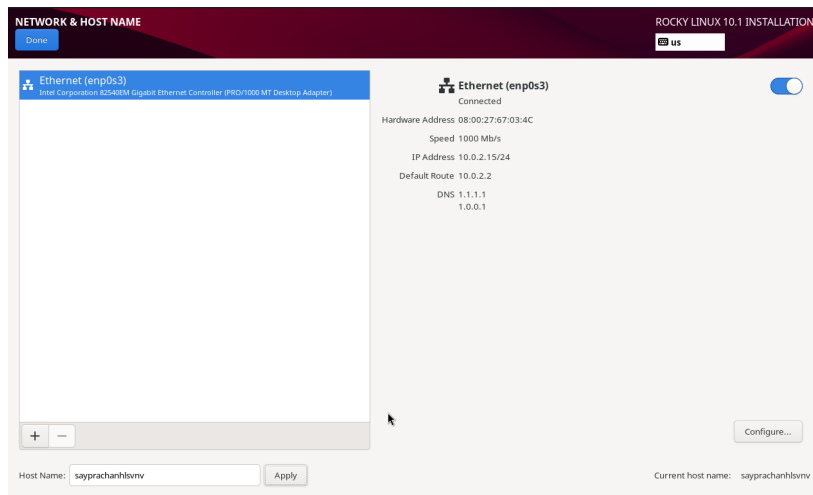


Рисунок 3.12: Настройка сети

Я создаю пароль для администратора(рис. 3.13).

ROOT ACCOUNT
Done

The root account is used for administering the system.

The root user (also known as super user) has complete access to the entire system. For this reason, logging into this system as the root user is best done only to perform system maintenance or administration.

☐ **Disable root account**
Disabling the root account will lock the account and disable remote access with root account. This will prevent unintended administrative access to the system.

☒ **Enable root account**
Enabling the root account will allow you to set a root password and optionally enable remote access to root account on this system.

Root Password: sayprachanh Strong

Confirm: sayprachanh

☐ Allow root SSH login with password

Рисунок 3.13: Пароль для администратора

Я создаю пользователя и его пароль, а также предоставляю ему административные привилегии(рис. 3.14).

CREATE USER
Done

Full name sayprachanhslvrv

User name sayprachanhslvrv

☒ Add administrative privileges to this user account (wheel group membership)

☒ Require a password to use this account

Password ●●●●●●●● Strong

Confirm password ●●●●●●●●

Advanced...

Рисунок 3.14: Создание пользователя

Я все проверяю перед началом установки(рис. 3.15).

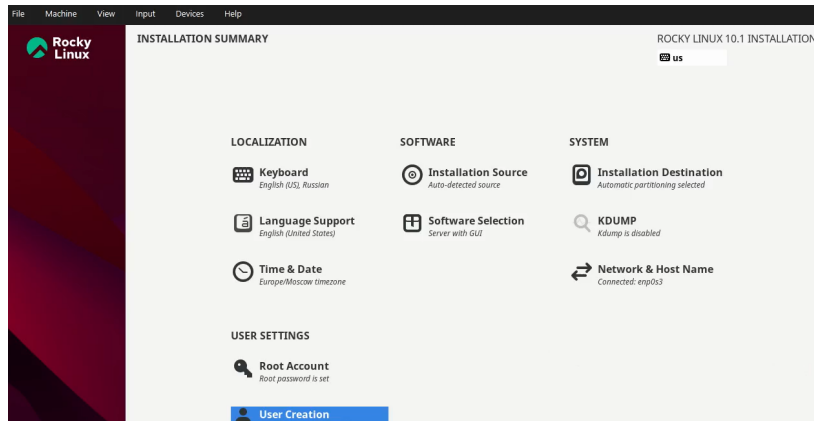


Рисунок 3.15: Проверка конфигурации

После того, как все настроено, я запускаю установку и жду ее завершения(рис. 3.16).

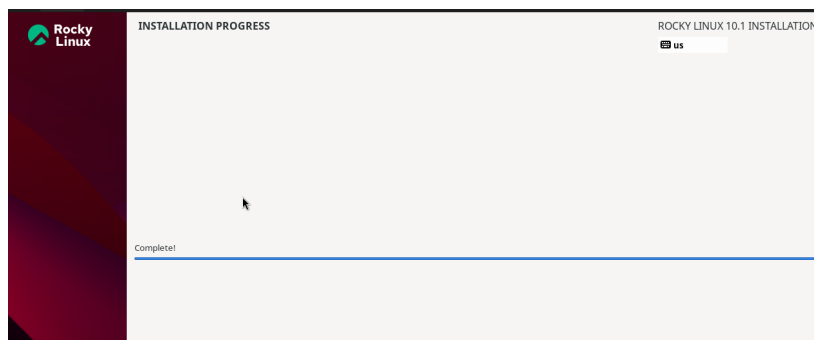


Рисунок 3.16: Завершение установки

После завершения установки я перезагружаю ОС и захожу в аккаунт, который создал ранее(рис. 3.17).

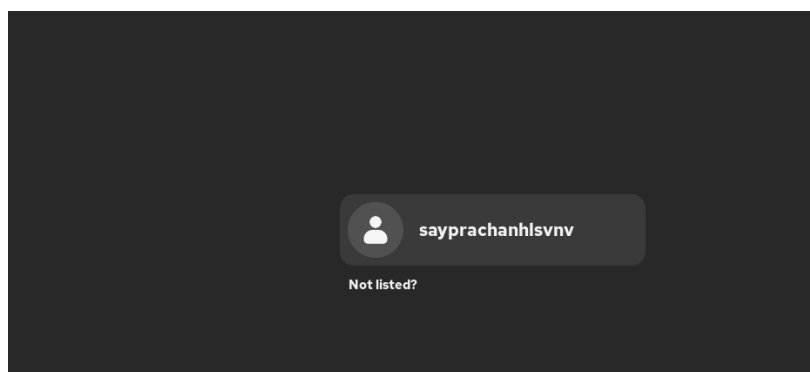


Рисунок 3.17: Вход в аккаунт

Я вставляю образ диска дополнений гостевой ОС, и он отображается в том месте, куда мы установили диск (сам образ диска исчезает из носителей после завершения установки).(рис. 3.18 и рис. 3.19).

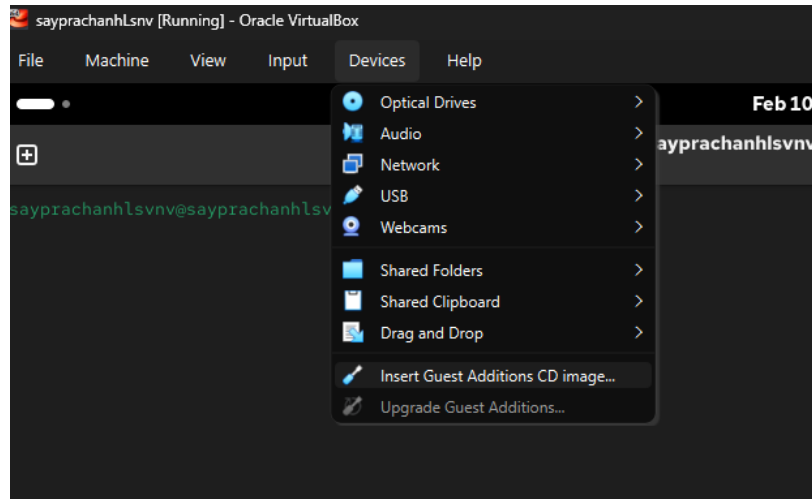


Рисунок 3.18: Установка гостевых дополнений ОС

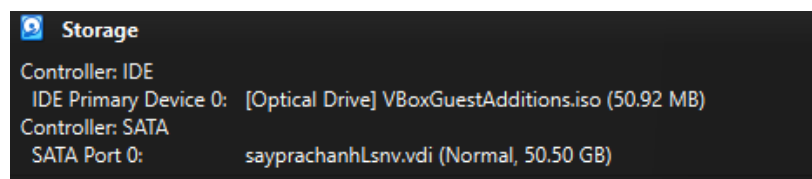


Рисунок 3.19: Установка гостевых дополнений ОС

3.2 Выполнение дополнительной задачи

Я открываю терминал, ввожу команды `dmesg` и `grep`, чтобы найти информацию (мы можем отобразить всю информацию, используя `grep | less`).

Версия ядра Linux - 6.12.0-124.8.1.el10_1.x86_64(рис. 3.20).

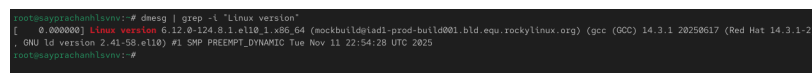


Рисунок 3.20: Версия ядра Linux

Частота процессора - 2592.006 MHz (рис. 3.21).

```

root@sayprachanhlsnv:~# dmesg | grep -i "Detected"
[ 0.000000] Hypervisor detected: KVM
[ 0.000011] tsc: Detected 2592.006 MHz processor
[ 1.008833] hub 1-0:1.0: 12 ports detected
[ 1.022594] hub 2-0:1.0: 12 ports detected
[ 1.423115] systemd[1]: Detected virtualization oracle.
[ 1.423291] systemd[1]: Detected architecture x86-64.
[ 2.886449] Warning: Unmaintained driver is detected: cnic
[ 2.896816] Warning: Unmaintained driver is detected: cnic_init
[ 2.911570] Warning: Unmaintained driver is detected: bnx2i
[ 2.926659] Warning: Unmaintained driver is detected: bnx2i_mod_init
[ 4.089534] Warning: Unmaintained driver is detected: e1000
[ 4.132508] Warning: Unmaintained driver is detected: e1000_init_module
[ 11.361915] systemd[1]: Detected virtualization oracle.
[ 11.362063] systemd[1]: Detected architecture x86-64.
root@sayprachanhlsnv:~#

```

Рисунок 3.21: Частота процессора

Модель процессора (CPU0) - Intel i7-10750H(рис. 3.22).

```

root@sayprachanhlsnv:~# dmesg | grep -i "CPU0"
[ 0.270165] smpboot: CPU0: Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz (family: 0x6, model: 0xa5, stepping: 0x2)
root@sayprachanhlsnv:~#

```

Рисунок 3.22: Модель процессора

Объем доступной оперативной памяти - 7157444K из 7467576K(рис. 3.23).

```

root@sayprachanhlsnv:~# dmesg | grep -i "memory"
[ 0.000000] DMI: Memory slots populated: 0/0
[ 0.017207] ACPI: Reserving FACP table memory at [mem 0xfffff000-0xfffff01e3]
[ 0.017209] ACPI: Reserving GSDT table memory at [mem 0xfffff0310-0xfffff0352]
[ 0.017310] ACPI: Reserving FACS table memory at [mem 0xfffff0200-0xfffff023f]
[ 0.017311] ACPI: Reserving FACS table memory at [mem 0xfffff0200-0xfffff023f]
[ 0.017312] ACPI: Reserving APIC table memory at [mem 0xfffff0240-0xfffff02ab]
[ 0.017314] ACPI: Reserving SSDT table memory at [mem 0xfffff02b0-0xfffff030e]
[ 0.019898] Early memory node ranges
[ 0.031527] PM: hibernation: Registered nosave memory: [mem 0x00000000-0x000000fff]
[ 0.031530] PM: hibernation: Registered nosave memory: [mem 0x00000000-0x000000fff]
[ 0.031531] PM: hibernation: Registered nosave memory: [mem 0x00000000-0x000000fff]
[ 0.031531] PM: hibernation: Registered nosave memory: [mem 0x00000000-0x000000fff]
[ 0.031532] PM: hibernation: Registered nosave memory: [mem 0xffff0000-0xfffffff]
[ 0.031533] PM: hibernation: Registered nosave memory: [mem 0x00000000-0xfefbffff]
[ 0.031534] PM: hibernation: Registered nosave memory: [mem 0xfec00000-0xfec00fff]
[ 0.031535] PM: hibernation: Registered nosave memory: [mem 0xfec00000-0xfec00fff]
[ 0.031535] PM: hibernation: Registered nosave memory: [mem 0xfec00000-0xfec00fff]
[ 0.031536] PM: hibernation: Registered nosave memory: [mem 0xfec00000-0xfec00fff]
[ 0.031536] PM: hibernation: Registered nosave memory: [mem 0xfec00000-0xfec00fff]
[ 0.031536] PM: hibernation: Registered nosave memory: [mem 0xfec00000-0xfec00fff]
[ 0.166165] Freeing SMP alternatives memory: 40K
[ 0.303564] Memory: 7157444K/7467576K available (18432K kernel code, 5804K rodata, 14268K rodata, 4344K init, 6690K bss, 303276K reserved, 0K cma-reserved)
[ 0.305553] x86/mm: Memory block size: 128MB
[ 0.896884] Freeing initrd memory: 48380K
[ 0.941228] Non-volatile memory driver v1.3
[ 1.383944] Freeing unused decrypted memory: 2028K
[ 1.385382] Freeing unused kernel image (initmem) memory: 4344K
[ 1.386883] Freeing unused kernel image (rodata/data gap) memory: 69K
[ 4.343796] vmwgfx 0000:00:02:0: [drm] Legacy memory limits: VRAM = 16384 KiB, FIFO = 2048 KiB, surface = 587904 KiB
[ 4.343809] vmwgfx 0000:00:02:0: [drm] Maximum display memory size is 16384 KiB

```

Рисунок 3.23: Объем доступной оперативной памяти

Тип обнаруженного гипервизора - KVM(рис. 3.24).

```

root@sayprachanhlsnv:~# dmesg | grep -i "hypervisor"
[ 0.000000] Hypervisor detected: KVM
[ 0.166165] SRBDS: Unknown: Dependent on hypervisor status
[ 0.166165] GDS: Unknown: Dependent on hypervisor status
[ 4.342882] vmwgfx 0000:00:02:0: [drm] *ERROR* vmwgfx seems to be running on an unsupported hypervisor.
root@sayprachanhlsnv:~#

```

Рисунок 3.24: Тип обнаруженного гипервизора

sudo fdisk -l показывает тип файловой системы, типа Linux, Linux LVM(рис. 3.25).

```
root@sayprachanhlsnv:~# sudo fdisk -l
Disk /dev/sda: 50.5 GiB, 54225272832 bytes, 105908736 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 0AB70AB8-8E67-49DC-8B2B-02D54294971C

Device            Start      End      Sectors  Size Type
/dev/sda1          2048       4095       2048      1M BIOS boot
/dev/sda2          4096    2101247    2097152      1G Linux extended boot
/dev/sda3    2101248 105908223 103806976 49.5G Linux LVM

Disk /dev/mapper/rl-root: 44.45 GiB, 47722790912 bytes, 93208576 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/mapper/rl-swap: 5.05 GiB, 5423235072 bytes, 10592256 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
root@sayprachanhlsnv:~#
```

Рисунок 3.25: тип файловой системы

Последовательность монтирования файловых систем.(рис. 3.26).

```
root@sayprachanhlsnv:~# dmesg | grep -i "mount"
[ 0.166165] Mount-cache hash table entries: 16384 (order: 5, 131072 bytes, linear)
[ 0.166165] Mountpoint-cache hash table entries: 16384 (order: 5, 131072 bytes, linear)
[ 9.643721] XFS (sda2): Mounting VFS filesystem #f024913-7549-41e0-b7e2-azada33316e2
[ 9.685521] XFS (sda2): Ending clean mount
[ 12.754796] system[1]: Set up automount proc-sys-fs-binfmt_misc.automount - Arbitrary Executable File Formats File System Automount Point.
[ 12.773473] system[1]: Mounting dev-hugepages.mount - Huge Pages File System...
[ 12.777839] system[1]: Mounting dev-queue.mount - POSIX Message Queue File System...
[ 12.779817] system[1]: Mounting sys-kernel-debug.mount - Kernel Debug File System...
[ 12.781829] system[1]: Mounting sys-kernel-tracing.mount - Kernel Trace File System...
[ 12.781295] system[1]: fips-crypto-policy-overlay.service - Blind-mount FIPS crypto-policy in FIPS mode was skipped because of an unset condition check (Condition=KernelCommandLineFips=1).
[ 12.883818] system[1]: Starting systemd-remount-fs.service - Remount Root and Kernel File Systems...
[ 12.916293] system[1]: Mounted dev-hugepages.mount - Huge Pages File System.
[ 12.916744] system[1]: Mounted dev-queue.mount - POSIX Message Queue File System.
[ 12.917080] system[1]: Mounted sys-kernel-debug.mount - Kernel Debug File System.
[ 12.917098] system[1]: Mounted sys-kernel-tracing.mount - Kernel Trace File System.
[ 12.943643] system[1]: Mounting sys-fs-fuse-connections.mount - FUSE Control File System...
[ 12.966168] system[1]: Mounted sys-fs-fuse-connections.mount - FUSE Control File System.
[ 12.969247] system[1]: Finished systemd-remount-fs.service - Remount Root and Kernel File Systems.
[ 14.837881] XFS (sda2): Mounting VFS filesystem f024913-7549-41e0-b7e2-azada33316e2
[ 14.943293] XFS (sda2): Ending clean mount
root@sayprachanhlsnv:~#
```

Рисунок 3.26: Последовательность монтирования файловых систем.

3.3 Ответы на контрольные вопросы

1. Что содержит учётная запись? Учётная запись содержит данные для идентификации и авторизации:

Системное имя — уникальный логин.

UID и GID — числовые идентификаторы пользователя и его основной группы.

Полное имя — может быть ФИО.

Домашний каталог — личная папка.

Начальная оболочка — командный интерпретатор при входе (например, bash).

Пароль — хранится отдельно в /etc/shadow.

2. Основные команды терминала

Справка: команда `-help` или `man` команда

Перемещение: `cd` путь (например, `cd /home`, `cd ..`)

Просмотр каталога: `ls` (просто список), `ls -la` (подробно)

Размер каталога: `du -sh` путь (пример: `du -sh ~`)

Создание/удаление:

Каталоги: `mkdir` имя, `rmdir` имя (пустой) или `rm -r` имя

Файлы: `touch` имя, `rm` имя

Права доступа: `chmod` права файл (пример: `chmod 755 script.sh`)

История команд: `history` (показать), `!<номер>` (выполнить)

3. Что такое файловая система? Порядок организации и хранения данных на носителе.

Примеры:

FAT32 — простая, для флешек. Имеет три области: служебные структуры, таблица FAT и зона файлов.

ext3/ext4 — журналируемые системы для Linux (ext4 — современная, надёжная).

4. Как посмотреть подмонтированные ФС?

`df -hT` — краткая информация с типами ФС.

`mount` — подробный список.

5. Как удалить зависший процесс?

Найти ID: `ps aux | grep (название процесса)`

Завершить:

`kill -9 PID (принудительно)`

`killall (название процесса) (все процессы с таким именем)`

4 Выводы

Я приобрёл практические навыки установки операционной системы на виртуальную машину и настройки минимально необходимых для дальнейшей работы сервисов.