Учебный курс

Системное администрирование РЕД ОС

Автор: Груздев П.Ю.

г.Екатеринбург
2025

Оглавление

Глава 1. Процесс загрузки операционной системы в РЕД ОС....3
1.1. Управление загрузкой....3
1.2. Управление инициализацией systemd....3
Глава 2. Работа с дисками в РЕД ОС....5
2.1. Управление разделами дисков....5
2.2. Управление файловыми системами....6
2.3. Монтирование файловых систем....6
Глава 3. Использование RAID и LVM в РЕД ОС....8
3.1. LVM....8
3.2. Программный RAID....8
Глава 4. Управление пользователями....9
4.1. Управление пользователями....9
4.2. Управление средой пользователя....10
4.3. Мониторинг пользовательской активности....10
Глава 5. Настройка сетевых параметров....12
5.1. Простая настройка сети....12
5.2. Настройка SSH....12
Глава 6. Сбор информации, мониторинг и журналирование в РЕД ОС....14
6.1. Управление журналированием....14
Глава 7. Управление программным обеспечением....15
7.1. Управление пакетами rpm....15
7.2. Установка ПО из исходных кодов....15
7.3. Библиотеки....16
Глава 8. Работа с ядром в РЕД ОС....17
8.1. Установка ядра....17
8.2. Управление параметрами ядра....17
8.3. Модули ядра....17
Глава 9. Поиск и устранение неисправностей в РЕД ОС....18
9.1. Восстановление работоспособности системы....18
Глава 10. Автоматизация установки РЕД ОС....24
10.1. Автоматизация развертывания при помощи PXE....24

Глава 1. Процесс загрузки операционной системы в РЕД ОС.

1.1. Управление загрузкой.

1. Изучите содержимое файла конфигурации GRUB2. Какие пункты меню загрузки там определены? Как описывается раздел, с которого производится загрузка ядра? Как устанавливается раздел для корневого каталога?

   Какие пункты меню загрузки там определены?

   Пунктов меню может и не быть вместо этого используется Boot Loader Specification (BLS), тогда в конфигурации будут строки:

```
insmod blscfg
blscfg
```

В случае использования классической конфигурации, пункты меню описываются в разделах:

```
$ info grub2 menuentry
$ info grub2 submenu
```

Как описывается раздел, с которого производится загрузка ядра?

```
set root='hd0,gpt2'
```

Как опция загрузки ядра `root=UUID=...`

2. Выполните команду `grub2-mkconfig` и сравните вывод с файлом `/boot/grub2/grub.cfg`.

   Вывод `grub2-mkconfig` и файл `/boot/grub2/grub.cfg` совпадают

3. Через встроенную оболочку GRUB задайте параметр загрузки ядра `init=/bin/bash`. Запустите систему. Что произошло? Получите список всех процессов. Загрузите систему в обычном режиме.

Такой способ позволяет получить доступ к системе минуя нормальную инициализацию. Сразу после загрузки ядра запускается оболочка, которая имеет полный доступ к ОС.

1.2. Управление инициализацией systemd.

1. Определите состояние службы `sshd`.

```
# systemctl status sshd.service
```

2. Определите в какую цель по умолчанию загружается система. Как изменить эту цель?

```
# systemctl get-default
# systemctl set-default
```

3. Установит цель загрузки по умолчанию в `multi-user.target`. Перезагрузите систему.

```
# systemctl set-default multi-user.target
```

4. Прервите загрузку в меню выбора ОС. И, через встроенную оболочку GRUB, загрузите систему в цель `basic.target`. Можете ли вы взаимодействовать с компьютером?

   В конце строчки `linux ($root)/vmlinuz …..rhgb quiet` дописать `systemd.unit=basic.target`

Консоль не доступна. Systemd не инициализирует интерфейс взаимодействия с пользователем.

5. Какая команда показывает только текущее состояние сервиса?

```
# systemctl is-active sshd.service
```

6. Проверьте нормально ли работает система в целом. Если состояние системы не соответствует нормальному (`running`), то как определить в чем причина?

```
# systemctl is-system-running
# systemctl --failed
```

7. Остановите и запретите запуск службы `cups`.

```
# systemctl disable cups.service
# systemctl mask cups.service
```

Глава 2. Работа с дисками в РЕД ОС.

2.1. Управление разделами дисков.

Предполагается что вы выполняете задание на виртуальной машине, в которую вы предварительно добавили два новых диска. Размер добавляемых дисков не менее 8Гб.

1. Проверьте текущее разбиение дисков на разделы.

```
# fdisk -l
```

2. Выполните команду `sfdisk -s` . Узнайте, что она выдает.

   Кол-во блоков на дисках

3. На каком разделе вашего диска имеется область подкачки `swap`?

```
# fdisk -l
```

4. В интерактивном режиме команды `fdisk` получите информацию о таблице разделов на одном из ваших новых дисков.

```
# fdisk /dev/sdb
> p
```

5. С помощью команды `fdisk` создайте на одном из дисков таблицу разделов типа DOS и:

   - раздел размером 2Гб с типом «Linux filesystem»;
   - раздел размером 2Гб с типом «Linux swap».

```
> n
> t
> 83 - Linux filesystem
> n
> t
> 2
> 82 - Linux swap
> w
```

6. На втором диске создайте таблицу разделов GPT. Затем два раздела по 2Гб типа «Linux filesystem» и «Linux swap».

```
# fdisk /dev/sdc
> g
> n
> t
> 20
> n
> t
> 2
> 19
> w
```

7. Определите код типа раздела для физического тома системы Linux LVM (Logical Volume Manager). Для таблицы разделов типа DOS и типа GPT.

```
# fdisk /dev/sdb
> t
> L
```

Внимание! *При ошибочных действиях все данные на диске могут быть утрачены! При создании раздела на диске, где размещена корневая файловая система, возможно потребуется перезагрузка после создания раздела.*

2.2. Управление файловыми системами.

1. Создайте на вновь созданном разделе диска файловую систему XFS.

```
# mkfs -t xfs /dev/sdb1
```

2. Создайте на другом разделе файловую систему EXT2. Отличается ли информация, выдаваемая командой создания файловой системы, от той, которую выдавала предыдущая команда?

```
# mkfs -t ext2 /dev/sdc1
```

3. Создайте на том же разделе, где ранее создавали EXT2 файловую систему EXT4 с предварительной проверкой поверхности диска на плохие блоки. Файловая система должна иметь размер блока 2048 байт.

```
# mkfs -t ext4 /dev/sdc1 -c
```

4. Определите, где находится первая копия суперблока в только что созданной файловой системе.

```
# dumpe2fs /dev/sdc1
```

5. Проверьте целостность только что файловой системы.

```
# e2fsck /dev/sdc1
```

6. Выполните команду проверки этой же файловой системы так, чтобы была выполнена ее полная проверка.

```
# e2fsck -f /dev/sdc1
```

2.3. Монтирование файловых систем.

1. Для файловой системы EXT4, созданной в предыдущих параграфах, создайте каталог - точку монтирования `/storage1` и смонтируйте эту файловую систему.

```
# mkdir /storage1
# mount /dev/sdc1 /storage1
```

2. Какой каталог находится в `/storage1`?

3. Для файловой системы XFS создайте каталог - точку монтирования `/storage2` и смонтируйте эту файловую систему

```
# mkdir /storage2
# mount /dev/sdb1 /storage2
```

4. Имеется ли в ФС `/storage2` какие либо файлы или каталоги?

```
. ..
```

5. Перейдите в каталог - точку монтирования. Попытайтесь размонтировать файловую систему. Что при этом происходит?

```
# cd /storage1
# umount
```

Провал, тк ФС используется

6. Какая команда позволяет узнать, какой процесс использует файл устройства?

```
fuser
```

7. Что надо сделать для размонтирования устройства?

Перейти в каталог вне смонтированной ФС

8. Настройте автоматическое монтирование каталога `/storage1` в `/etc/fstab`.

```
# blkid /dev/sdc1
/dev/sdc1: UUID="457968bb-fef4-4030-95b3-84a18a3b2e6c" BLOCK_SIZE="4096"
TYPE="ext4" PARTUUID="b51c04b0-63d9-2c49-8a0d-60eb3db66cc5"
# vi /etc/fstab
UUID=457968bb-fef4-4030-95b3-84a18a3b2e6c /storage1   ext4  defaults    0     0
```

9. Для каталога `/storage2` опишите автоматическое монтирование посредством юнита `systemd`.

```
# blkid /dev/sdb2
/dev/sdb2: UUID="afd4f037-c9d3-47c0-8bbc-c8b468d74777" BLOCK_SIZE="512"
TYPE="xfs" PARTUUID="50f6f004-5436-a449-9057-c7a97795f7ef"
# cat /etc/systemd/system/storage2.mount:
[Unit]
Description=filestorage

[Mount]
What=/dev/disk/by-uuid/afd4f037-c9d3-47c0-8bbc-c8b468d74777
Where=/storage2
Type=xfs
Options=default

[Install]
WantedBy=graphical.target
```

10. Перезагрузите систему и убедитесь, что:

- ОС загружается.
- Монтируются каталоги `/storage1` и `/storage2`

Глава 3. Использование RAID и LVM в РЕД ОС

3.1. LVM

1. Добавьте по одному LVM разделу размером 3Гб, на каждый из дисков.

```
# fdisk
```

2. Создайте логический том с зеркальным отображением. Размер тома 1 Гб. Файловая система ext4.

```
# pvcreate /dev/sdb3
# pvcreate /dev/sdc3
# vgcreate mvg /dev/sdb3 /dev/sdc3
# lvcreate -m 1 -L 1G /dev/mvg -n mlv
# mkfs -t ext4 /dev/mvg/mlv
```

3. Увеличьте размер зеркального тома и файловой системы на нем на 1 Гб.

```
# lvextend -L +1G /dev/mvg/mlv -r
```

4. Создайте логический том размером 1 Гб с чередованием.

```
# lvcreate -i 2 -L 1G /dev/mvg -n slv
```

5. Получите информацию о состоянии группы и использовании дисков в ней.

```
# vgdisplay -v
```

6. Опишите подключение зеркального тома к каталогу `/mirror1` в `/etc/fstab`.

```
/dev/mvg/mlv      /mirror1    ext4  defaults    0     0
```

7. Подключите еще один диск размером 8Гб к виртуальной машине. Добавьте этот диск к группе целиком.

```
# pvcreate /dev/sdd
# vgextend mvg /dev/sdd
```

8. Перенесите на новый диск данные с одного из разделов и удалите освобожденный раздел из группы.

```
# pvmove /dev/sdb3 /dev/sdd
# vgreduce mvg /dev/sdb3
# pvremove /dev/sdb3
```

3.2. Программный RAID

1. Создайте RAID 5 из трех разделов, размером по 3 Гб каждый. Файловая система ext4.

```
# mdadm -C -l 5 -n 3 /dev/md/myraid /dev/sde1 /dev/sde2 /dev/sde3
# mkfs -t ext4 /dev/md/myraid
```

2. Получите информацию о состоянии созданного RAID массива.

```
# cat /proc/mdstat
```

И/или

```
# mdadm --detail /dev/md/myraid
```

3. Каков размер файловой системы, созданной в RAID массиве?

Немного меньше 6 Гб

4. Опишите подключение RAID 5 к каталогу `/raid5` в `/etc/fstab`.

```
/dev/md/localhost.localdomain:myraid      /raid5      ext4  defaults    0     0
```

Глава 4. Управление пользователями.

4.1. Управление пользователями.

1. Просмотрите файл `/etc/shadow` (с правами root). У всех ли пользователей содержимое второго поля выглядит приблизительно одинаково или же у некоторых пользователей имеются существенные отличия от записей для других пользователей?

```
#cat /etc/shadow
```

Есть отличия для пользователей, у которых нет пароля, во втором поле установлено * или !!. У пользователей с паролями там хэш пароля.

2. Какие символы могут содержаться шифрованной строке пароля во втором поле файла `/etc/shadow` ?

Цифры, спецсимволы, буквы в обоих регистрах

3. Используя текстовые утилиты выведите таблицу, содержащую имена пользователей, их UID и GID, а также шифрованный пароль (необходимо иметь права root). Таблица должна содержать записи только для пользователей имеющих шифрованные пароли длиной более 10 символов.

```
# join -t: --nocheck-order /etc/passwd /etc/shadow | awk -F: \
'length($8)>10{printf "%s:%d:%d:%s\n",$1,$3,$4,$8}'
```

4. Зарегистрируйте пользователя test1, для которого запрещен вход в сеанс, имеющего домашний каталог `/var/spool/mail`, и являющегося членом групп users и mail. Пользователь должен иметь UID=1100.

```
# useradd -s /sbin/nologin -d /var/spool/mail -G users,mail -u 1100 test1
```

5. Создайте учетную запись для пользователя test2 с настройками по умолчанию, но без создания приватной группы. Проверьте создался ли домашний каталог пользователя, наполнен ли он файлами, и кому он принадлежит.

```
# useradd -n test2
# ls -l /home
# ls /home -a /test2
```

6. Измените имя пользователя test2 на test3.

```
# usermod -l test3 test2
```

7. Удалите пользователя test3 передав после этого права владения его файлами суперпользователю и группе sys.

```
# userdel test3
# chown -R sys:sys /home/test2
```

8. Помимо файла `/etc/default/useradd` имеется еще один конфигурационный файл, влияющий на поведение команды `useradd` (см. `man useradd`) Найдите его и изучите его содержание. Какая настройка позволяет изменять минимальный UID для новых пользователей?

Файл `/etc/login.defs` и параметр в нем UID_MIN

```
# grep ^UID_MIN /etc/login.defs
UID_MIN                  1000
```

9. Зарегистрируйте пользователя test4 с настройками по умолчанию и установите для него пароль. Изучите содержимое соответствующей пользователю записи в файле `/etc/shadow`.

```
# useradd test4
# passwd test4
# cat /etc/shadow
```

10. Установите дату устаревания пароля (Password expires) для пользователя test4 на 31 декабря текущего года. Проверьте, что изменилось в `/etc/shadow`.

```
# chage -E 2025-12-31 test4
```

11. Удалите пароль пользователя и проверьте изменения в `/etc/shadow`.

```
# passwd -d test4
# cat /etc/shadow
```

12. Заблокируйте учетную запись test4.

```
# passwd -l test4
```

13. Создайте группу пользователей xusers с GID 1010.

```
# groupadd -g 1010 xusers
```

14. Зарегистрируйте себя (пользуясь правами root) в качестве участника группы xusers.

```
# gpasswd -a sa xusers
```

15. От имени своей учетной записи добавьте пользователя test4 в группу xusers.

```
$ gpasswd -a test4 xusers Команда проваливается
```

16. Найдите утилиту, позволяющую изменять имена и GID групп. Измените имя группы на yusers.

```
# groupmod -n yusers xusers
```

4.2. Управление средой пользователя.

1. Измените значение `umask` на 027 для всех пользователей системы, оболочкой по умолчанию для которых является Bash.

```
# vi /etc/profile
```

2. Установите в собственном профиле оболочки псевдоним `l` для команды `ls -Ll`.

```
#vi .bash_profile
alias l='ls -Ll'
```

3. Каким образом сделать так, чтобы этот же псевдоним устанавливался и для всех вновь регистрируемых пользователей в системе, для которых оболочкой по умолчанию будет Bash?

```
Добавить alias l='ls -Ll'  в /etc/profile
```

4. В каком файле удобнее всего добавить к переменной окружения PATH путь к каталогу bin, находящемуся в домашнем каталоге обычного пользователя? Проверьте может такая настройка уже есть.

```
# cat ~/.bash_profile там есть строчка PATH=$PATH:$HOME/bin
```

5. Измените вид вторичного приглашения командной строки на -> так, чтобы при каждом входе в сеанс Bash значение этой переменной устанавливалось автоматически.

```
#vim ~/.bashrc
PS2="->"
```

4.3. Мониторинг пользовательской активности.

1. Определите, когда была последний раз загружена система.

```
# last reboot
```

2. С помощью опции `-a` команды `who` получите подробную информацию о пользователях и статусе системы.

```
# who -aq
```

3. С помощью команды `who` получите список пользователей, входивших в сеанс ранее.

4. Сравните предыдущий список со списком, выводимым командой `last`.

```
# last
```

5. Получите отчет по входам в сеанс суперпользователя с помощью `lastlog`.

```
# lastlog | grep root
```

6. Кто входил в сеанс за последние пять дней?

```
# lastlog -t 5
```

7. Откройте еще один сеанс и с помощью `loginctl` получите описание и состояние сеанса. Завершите этот сеанс.

```
# loginctl show-session 3
# loginctl terminate-session 3
```

Глава 5. Настройка сетевых параметров

5.1. Простая настройка сети



1. Создайте клон виртуальной машины РЕД ОС с именем H1.
2. В настройках H1:
    1. Первый интерфейс подключите к предварительно созданной сети NatNetwork20 (адрес сети установить 20.20.20.0/24). (Адрес сети и имя сети NAT уточните у преподавателя!)
3. Настройте имена машин:
    1. Для ВМ H1 — h1.
    2. Для изначальной ВМ - server.
    3. Не забудьте настроить локальное разрешение имен в файле `/etc/hosts`.

```
sudo hostnamectl hostname h1
sudo nano /etc/hosts
...
127.0.1.1   h1
ip_адрес_сервера server
...
```

4. На H1 настройка производится с помощью `nmcli`:
    1. Удалите все подключения.

```
nmcli connection delete Имя\ вашего\ подключения\ 1
```

    2. Создайте подключение с именем External. К этому подключению добавьте первый интерфейс. Адрес настройте согласно схеме.

```
nmcli connection add con-name External type ethernet ifname enp0s3 ipv4.method
manual ipv4.addresses 20.20.20.10/24 ipv4.gateway 20.20.20.1 ipv4.dns
172.27.255.254
```

    3. Аналогичными образом настройте ВМ sever. Назначьте ему IP адрес согласно схеме и измените имя. Вместо nmcli попробуйте использовать nmtui.
    4. Проверьте какой адрес назначен на интерфейс и связь с H1.

```
ip ad
ping 20.20.20.1
```

5.2. Настройка SSH

1. Подключитесь с H1 на server по SSH, используя аутентификацию по паролю.

```
ssh sa@server
```

2. Создайте файл 1.txt с текущей датой в домашнем каталоге пользователя sa на ВМ server. Закройте подключение по SSH. Используя утилиту scp скопируйте этот файл в домашний каталог на ВМ H1.

```
date >/home/sa/1.txt
```

```
exit
scp sa@server:/home/sa/1.txt  ~
```

3. На ВМ H1 настройте ssh подключение по ключам RSA к хосту server под учетной записью sa.

На H1:

```
ssh-keygen -t rsa
ssh-copy-id sa@server
```

4. С ВМ H1 попробуйте подключиться на ВМ server под пользователем sa без ввода пароля. Должно получиться.

```
ssh sa@server
```

5. В файле /etc/ssh/sshd_config смените стандартный 22 порт SSH на 10022 на ВМ server.
6. Перезапустите службу sshd

```
systemctl restart sshd.service
```

7. Попробуйте подключиться к ВМ server не указывая порт. (Попытка должна провалиться)

```
ssh sa@server
```

8. Попробуйте подключиться к ВМ server указывая вручную порт 10022. (Подключение должно пройти успешно)

```
ssh -p 10022 sa@server
```

Глава 6. Сбор информации, мониторинг и журналирование в РЕД ОС

6.1. Управление журналированием

1. Создайте в конфигурации демона `rsyslogd` строку, которая заставит его записывать сообщения от источника auth с уровнем важности не ниже info в файл `/var/log/mylog` . Не забудьте перезапустить службу, чтобы изменения вступили в силу.

```
auth.info                       /var/log/mylog
```

2. Проверьте, записываются ли в этот файл сообщения при входе в сеанс и выходе из него пользователей.

```
$ logout
```

3. Создайте аналогичный журнал `/var/log/mylogpriv` для записи сообщений от источника `authpriv` . Проверьте его работоспособность. Записываются ли в него те же сообщения, что и в предыдущий журнал?

```
authpriv.info                   /var/log/mylog
```

4. Посмотрите с помощью `journalctl` журнал загрузки системы.

```
# journalctl -b
```

5. Настройте `systemd` вести постоянные журналы.

```
# vim /etc/systemd/journald.conf
Storage = persistent
```

6. Создайте настройки ротации для журналов `/var/log/mylog` и `/var/log/mylogpriv`.
   Файлы должны ротироваться ежедневно.
   Ротация первой копии должна осуществляться два раза.
   Ротируемые копии должны сжиматься утилитой gzip.

```
# vim /etc/logrotate.conf
/var/log/mylog {
      daily
      rotate 2
      create
      compress
}
```

Аналогично для mylogpriv

7. Для файла `/var/log/mylog` установите в качестве дополнительного условия ротации достижение им размера 10 Кб.

Добавить строчку внутрь скобок

```
size  10K
```

Глава 7. Управление программным обеспечением.

7.1. Управление пакетами rpm.

1. Получите список установленных пакетов.

```
# rpm -qa
```

2. Как в RPM увеличить информативность получаемых данных, например, при проверке целостности установленных пакетов.

   Опция -v - выводить более детальные сообщения

3. Определите, каким образом можно получить список всех возможных ключей запроса к базе данных RPM?

```
$ rpm --help
$ man rpm
```

   Ответ:

```
rpm --querytags
```

4. Выведите информацию о полном имени, группе и размере пакета bash.

```
$ rpm -qi bash
```

5. Получите список из десяти пакетов, файлы из которых занимают на диске максимальное место (на основе данных из самих пакетов).

6. Получите список включенных и доступных репозиториев.

```
# dnf repolist
```

7. Установите пакет bash-completion.

```
# dnf install bash-completion
```

8. Найдите и установите пакет, который предоставляет утилиту `wireshark`.

```
# dnf provides wireshark
```

9. Обновите ОС.

```
# dnf upgrade
```

10. Получите список доступных групп пакетов.

```
# dnf group list
```

11. Узнайте список пакетов входящих в группу «Графические средства администрирования».

```
# dnf group info "Графические средства администрирования"
```

7.2. Установка ПО из исходных кодов.

1. Следуя примеру, приведенному в учебнике, установите из исходных кодов пакет net-tools. Перед установкой, убедитесь что данный пакет у вас не используется. Сдлеать это можно при помощи команды

```
sudo ifconfig
```

2. Если команда была выполнена успешна - удалитепакет с ней из системы при помощи команды

```
sudo dnf remove net-tools
```

3. Скачать пакет с исходным кодом можно командой

```
sudo wget https://sourceforge.net/projects/net-tools/files/net-tools-2.10.tar.xz
```

4. Следуя инструкциям из файла INSTALLING попробуйте собрать пакет самостоятельно.

5. Исходя из рекомендаций в файле INSTALLING перейдем в каталог скопируем наш архив в каталог /usr/src

```
sudo -i
cp /home/sa/net-tools-2.10.tar.xz /usr/src
```

Распаковываем архив

```
cd /usr/src
sudo tar xf net-tools-2.10.tar.xz
```

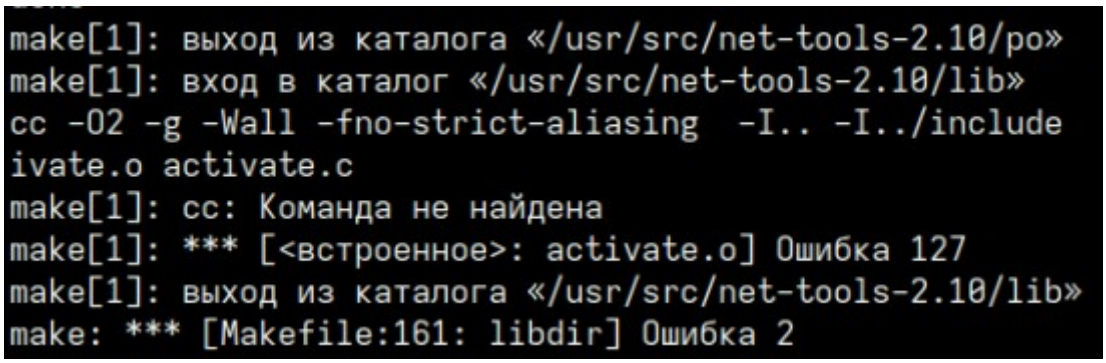
Переходим в распакованный каталог

```
cd net-tools-2.10
```

Выполняем сборку программы, исходя из инструкции (в процессе работы программы нажимайте на Enter чтобы оставить ответы на задаваемые вопросы предложенными значениями по умолчанию)

```
make config ; make ; make -n install ; make install
```

В результате получаем ошибку



Данная ошибка говорит нам о том, что отсутствует компилятор gcc. Узнать это можно, поискав информацию о команде "cc" в Интернете.

Устанавливаем необходимый нам пакет при помощи команды

```
dnf install gcc
```

Повторно выполняем сборку программы

```
make config ; make ; make -n install ; make install
```

Проверяем, что всё работает

```
exit
ifconfig
```

7.3. Библиотеки.

1. Определите от каких библиотек зависит исполняемый файл утилиты ifconfig (`/bin/ifconfig`), собранный в предыдущем параграфе.

```
$ ldd /bin/ifconfig
```

2. Определите имена файлов библиотек, SO-name которых получены в предыдущем задании.

```
$ ls -l  so_имена_библиотек
```

3. Установлены ли в системе какие-либо библиотеки без участия системы управления пакетами (см. `/usr/local`)?

```
$ ls -l  /usr/local | grep .so
```

Глава 8. Работа с ядром в РЕД ОС.

8.1. Установка ядра

1. Установите утилиту kernel-manager

```
# dnf install kernel-manager
```

2. Запустите утилиту из "Главное меню" - "Стандартные" - "Менеджер ядер"
3. Установите последнюю доступную версию ядра

8.2. Управление параметрами ядра

1. Просмотрите значение всех параметров ядра

```
#sysctl -a
```

2. Просмотрите значение параметра net.ipv4.ip_forward

```
#sysctl net.ipv4.ip_forward
```

3. Установите "1" в качестве значения данного параметра на постоянно основе

```
#sysctl -w net.ipv4.ip_forward=1
```

4. Перезагрузитесь и проверьте, что значение переменной net.ipv4.ip_forward осталось неизменным.

8.3. Модули ядра.

1. Получите список модулей, загруженных в ядро в вашей системе. Имеется ли в списке модуль e1000?

```
# lsmod
```

2. Узнайте, кто является автором модуля e1000.

```
# modinfo e1000
```

3. Определите зависимости модуля e1000 от других модулей.

```
# less /lib/modules/4.18.0-331.el8.x86_64/modules.dep | grep e1000
```

4. Если модуль e1000 загружен, то попробуйте его выгрузить. Что при этом происходит?

```
# modprobe -r e1000
```

5. Вновь загрузите модуль e1000, какова реакция системы?

```
# modprobe e1000
```

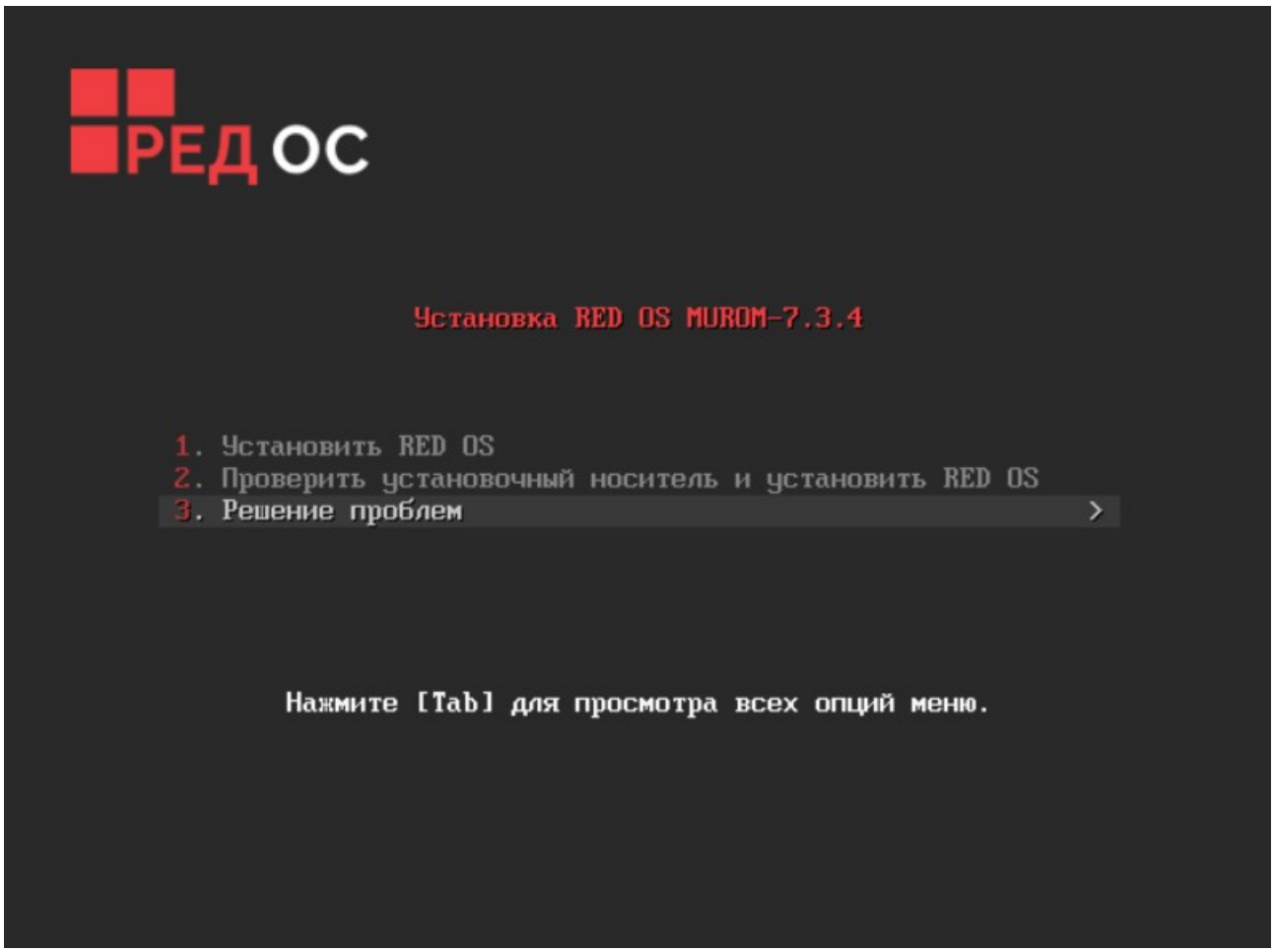
6. Для какого оборудования предназначен модуль igb?

```
# modinfo igb
```

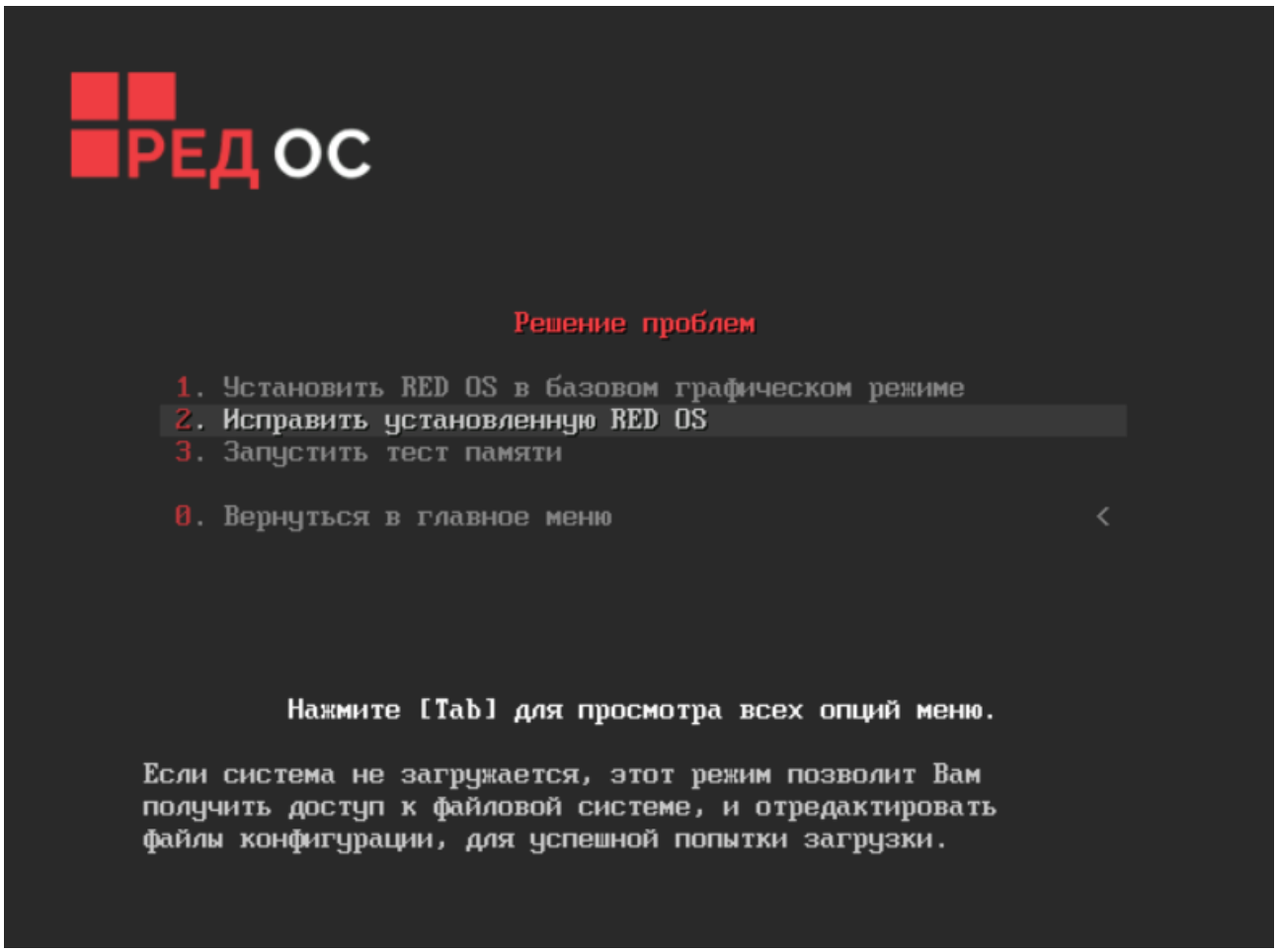
Глава 9. Поиск и устранение неисправностей в РЕД ОС

9.1. Восстановление работоспособности системы

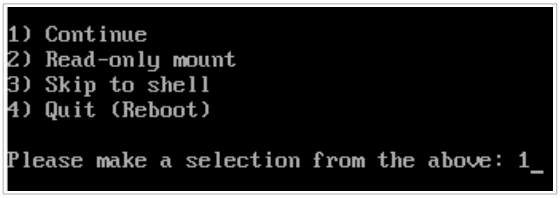
1. Включите сломанную машину. Машина не включается. Загрузка останавливается на моменте работы загрузчика GRUB. Меню GRUB отображено не было, сразу появился вывод командной строки GRUB. Вывод - скорее всего ошибка именно в самом загрузчике. Переходим к устранению.
2. Подключаем установочный диск к машине и включаем её. Переходим в "Решение проблем"



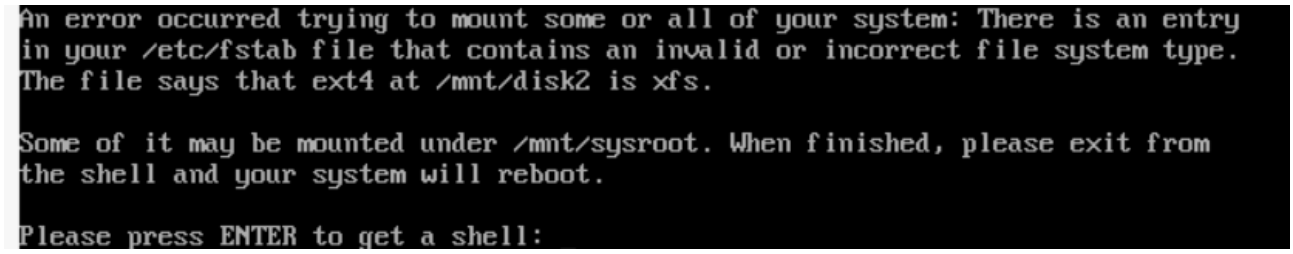
Далее - "Исправить установленную RED OS"



3. В появившемся списке выберите пункт «Continue», введя цифру 1 и нажав Enter:



После выполнения данного шага вы увидите следующее сообщение



4. Тут можно увидеть две вещи:

1) Произошла ошибка при монтировании - в файле /etc/fstab допущена ошибка - вместо файловой системы ext4 выставлена xfs, для устройства, которое монтируется в каталог /mnt/disk2

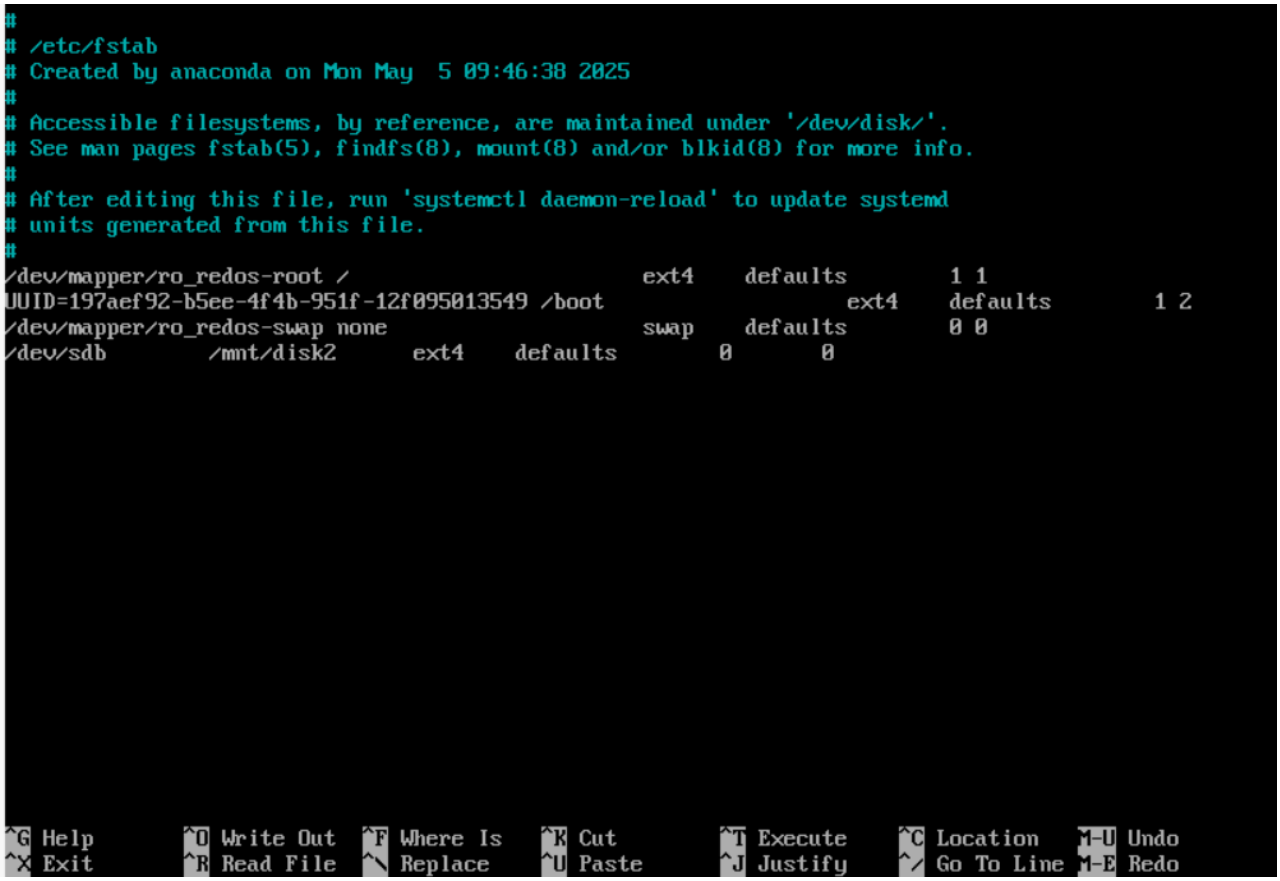
2) Чтобы получить доступ к оболочке, необходимо изменить корневой каталог при помощи команды chroot /mnt/sysroot

Выполняем команду:

```
chroot /mnt/sysroot
```

Устраняем ошибку в /etc/fstab. Находим там строчку с точкой монтирования /mnt/disk2 и меняем xfs на ext4.

```
nano /etc/fstab
```



Сохраняем изменения и перезагружаем машину. Перезагрузку можно выполнить командой

```
/sbin/reboot -f
```

5. Возвращаемся в режим восстановления, для этого повторяем шаги 2 и 3. Следующим шагом является изменение корневого каталога на /mnt/sysroot с помощью команды chroot (это сделает вашу систему корневой средой):

```
chroot /mnt/sysroot
```

Для определения диска, на котором установлена система, можно использовать следующую команду:

```
lsblk
```

Далее выполните установку загрузчика командой (в конце указывается нужный диск, в нашем случае это /dev/sda. Понять это можно по выводу команды lsblk):

```
grub2-install /dev/sda
```

6. Обновляем конфигурацию grub при помощи команды

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Выходим из chroot

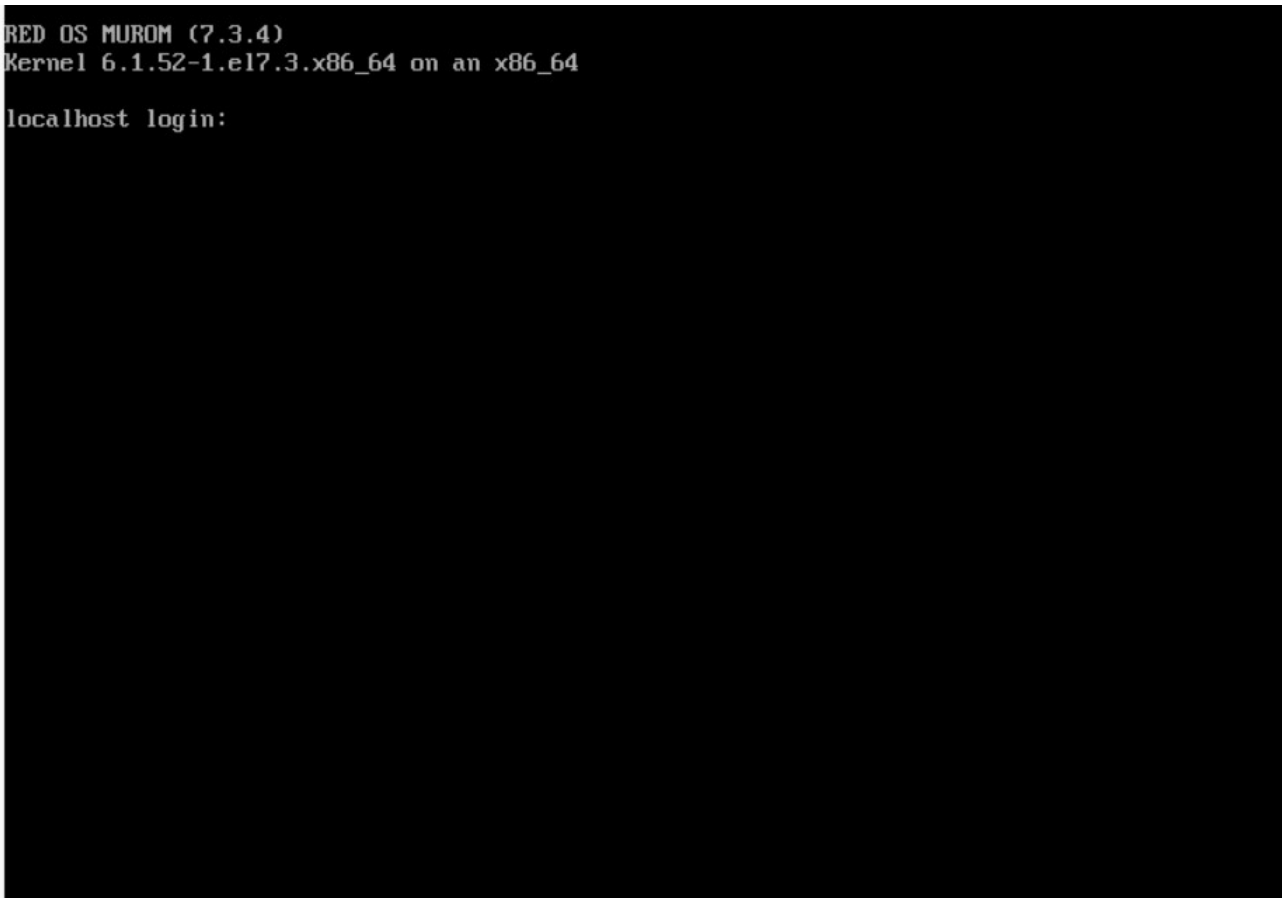
```
exit
```

Перезагружаем систему

```
reboot
```

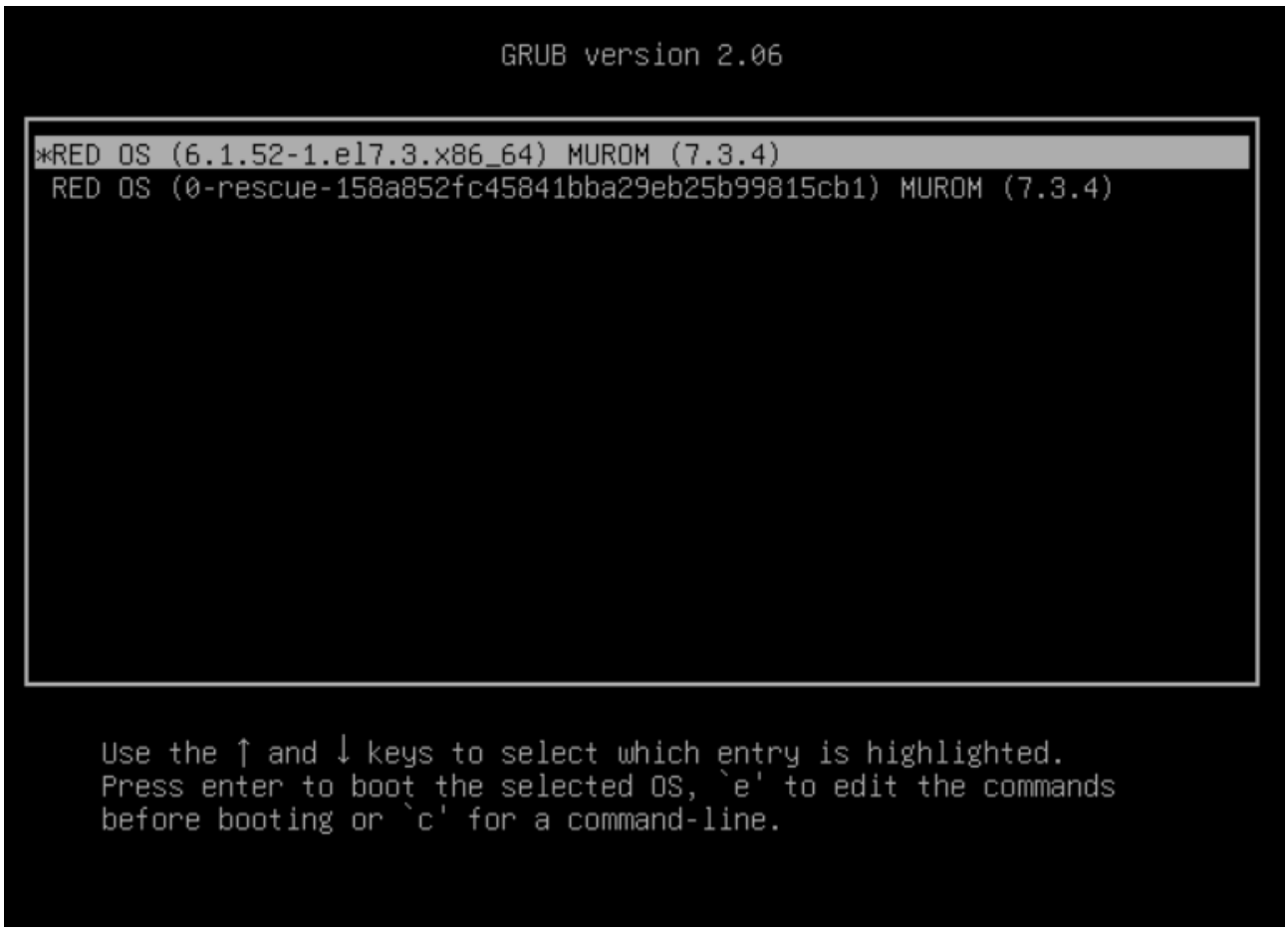
Во время перезагрузки выполните изъятие iso-образа диска из машины.

7. В результате мы восстановили работоспособность системы. Попробуем в неё войти.



Пароль для пользователей root и sa нам не известен, поэтому зададим им новый пароль.

8. Перезагружаем систему и во время выбора меню загрузки нажимаем на "e"



9. Находим строку, которая начинается с "linux", меняем в ней параметр "ro" на "rw" и дописываем в конце строки "init=/bin/bash"



10. Нажимаем Ctrl+x для загрузки системы с данными параметрами.

11. Меняем пароли пользователям root и sa при помощи команды passwd. После этого вводим команду

```
touch /.autorelabel
```



12. Перезагружаем систему при помощи команды

```
/sbin/reboot -f
```

13. Входим в систему за пользователя sa или root.

14. Проверим работоспособность сети, при помощи команды ping до H1.

15. Настраиваем сеть на использование dhcp любым удобным для вас способом.

16. Пробуем подключиться по ssh к машине с именем server.

17. Если подключение прошло успешно и последующие перезагрузки не создают ошибок, то работоспособность системы полностью восстановлена.

Глава 10. Автоматизация установки РЕД ОС

10.1. Автоматизация развертывания при помощи PXE

1. Устанавливаем необходимые пакеты

```
sudo -i
dnf install dhcp-server tftp-server syslinux httpd dnf-plugins-core
```

2. Создайте следующие каталоги:

```
mkdir /var/lib/tftpboot/pxelinux.cfg
mkdir /var/lib/tftpboot/uefi
mkdir -p /var/lib/tftpboot/images/REDOS
```

3. скопируйте файлы для запуска установки РЕД ОС в режиме legacy через PXE:

```
cp
/usr/share/syslinux/{chain.c32,mboot.c32,memdisk,menu.c32,pxelinux.0,ldlinux.c32
,libutil.c32} /var/lib/tftpboot/

chmod 777 /var/lib/tftpboot/pxelinux.0
```

4. Скопируйте файлы для UEFI режима установки РЕД ОС в каталог /var/lib/tftpboot/uefi.

```
dnf download shim-x64 grub2-efi-x64 --downloaddir=/root/
cd /root/
rpm2cpio shim-x64-*.rpm | cpio -dimv
rpm2cpio grub2-efi-x64-*.rpm | cpio -dimv
cp ./boot/efi/EFI/BOOT/BOOTX64.EFI /var/lib/tftpboot/uefi
cp ./boot/efi/EFI/redos/grubx64.efi /var/lib/tftpboot/uefi

chmod 777 /var/lib/tftpboot/uefi/*.*
```

5. Подключите загрузочный USB-носитель с РЕД ОС 7.3 и скопируйте его содержимое в каталог /var/lib/tftpboot/images/REDOS

```
cp -vR "/run/media/sa/redos-DVD-x86_64-MUROM-7.3.4/."
/var/lib/tftpboot/images/REDOS
```

6. Настройте dhcp-сервер для выдачи адресов в вашей подсети

```
nano /etc/dhcp/dhcpd.conf

non-authoritative;
allow bootp;
option space pxelinux;
option pxelinux.magic code 208 = string;
option pxelinux.configfile code 209 = text;
option pxelinux.pathprefix code 210 = text;
option pxelinux.reboottime code 211 = unsigned integer 32;
option architecture-type code 93 = unsigned integer 16;
subnet 20.20.20.0 netmask 255.255.255.0 {
option routers 20.20.20.20;
range 20.20.20.70 20.20.20.80;
class "pxeclients" {
match if substring (option vendor-class-identifier, 0, 9) = "PXEClient";
next-server 20.20.20.20;
if option architecture-type = 00:07 {
filename "uefi/grubx64.efi";
}
else {
filename "pxelinux.0";
}}}
```

7. Запустите службу dhcpd:

```
systemctl enable dhcpd --now
```

8. Создайте загрузочное меню для установки в режиме legacy с использованием PXE

```
nano /var/lib/tftpboot/pxelinux.cfg/default
```

```
default menu.c32
PROMPT 0
TIMEOUT 150
MENU TITLE PXE Menu

LABEL REDOS 7.3
MENU LABEL REDOS 7.3
KERNEL images/REDOS/images/pxeboot/vmlinuz
APPEND initrd=images/REDOS/images/pxeboot/initrd.img ramdisk_size=128000 ip=dhcp
inst.repo=http://20.20.20.20/images/REDOS/

LABEL KICKSTART
MENU LABEL KICKSTART
KERNEL images/REDOS/images/pxeboot/vmlinuz
APPEND initrd=images/REDOS/images/pxeboot/initrd.img ramdisk_size=128000 ip=dhcp
inst.repo=http://20.20.20.20/images/REDOS/
inst.ks=http://20.20.20.20/images/REDOS/ks.cfg
```

Примечание: Текст выделенный жирным должен быть расположен в одну строку!

9. Создайте загрузочное меню для установки в режиме UEFI с использованием PXE:

```
nano /var/lib/tftpboot/uefi/grub.cfg
```

```
function load_video {
insmod efi_gop
insmod efi_uga
insmod video_bochs
insmod video_cirrus
insmod all_video
}
load_video
set gfxpayload=keep
insmod gzio
menuentry 'REDOS 7.3' {
linux images/REDOS/images/pxeboot/vmlinuz ip=dhcp kernel vmlinuz
inst.repo=http://20.20.20.20/images/REDOS/
initrd images/REDOS/images/pxeboot/initrd.img
}
menuentry 'KICKSTART' {
linux images/REDOS/images/pxeboot/vmlinuz ip=dhcp kernel vmlinuz
inst.repo=http://20.20.20.20/images/REDOS/
inst.ks=http://20.20.20.20/images/REDOS/ks.cfg
initrd images/REDOS/images/pxeboot/initrd.img
}
```

Примечание: Текст выделенный жирным должен быть расположен в одну строку!

10. Скопируйте файл anaconda-ks.cfg из каталога /root.

```
cp anaconda-ks.cfg /var/lib/tftpboot/images/REDOS/ks.cfg
chmod 777 /var/lib/tftpboot/images/REDOS/ks.cfg
```

11. Закомментируйте в файле /var/lib/tftpboot/images/REDOS/ks.cfg следующие строчки:

```
#@^graphical-server-environment
#cdrom
```

12. Настройте веб-сервер httpd

```
nano /etc/httpd/conf.d/pxeboot.conf

Alias /images /var/lib/tftpboot/images
<Directory /var/lib/tftpboot/images>
Options Indexes FollowSymLinks
Require ip 127.0.0.1 20.20.20.0/24
</Directory>
```

13. Настройте SELinux

```
setenforce 0
```

14. Запустите службу httpd:

```
systemctl enable httpd --now
```

15. Настройте и запустите службу tftp.

```
nano /usr/lib/systemd/system/tftp.service
```

добавьте строку в секцию [Install]:

```
WantedBy=multi-user.target
```

16. Откройте файл:

```
nano /usr/lib/systemd/system/tftp.socket
```

измените строку ListenDatagram=69 на ListenDatagram=0.0.0.0:69, чтобы запустить tftp на 69 порту по IPv4-протоколу. По умолчанию порт публикуется на IPv6.

```
[Unit]
Description=Tftp Server Activation Socket

[Socket]
ListenDatagram=0.0.0.0:69

[Install]
WantedBy=sockets.target
```

17. Проинициализируйте модули systemd:

```
systemctl daemon-reload
```

18. Добавьте службу tftp в автозапуск:

```
systemctl enable tftp --now
```

19. Создайте ВМ со следующими параметрами:

HDD - 50 GB

RAM - 4096MB

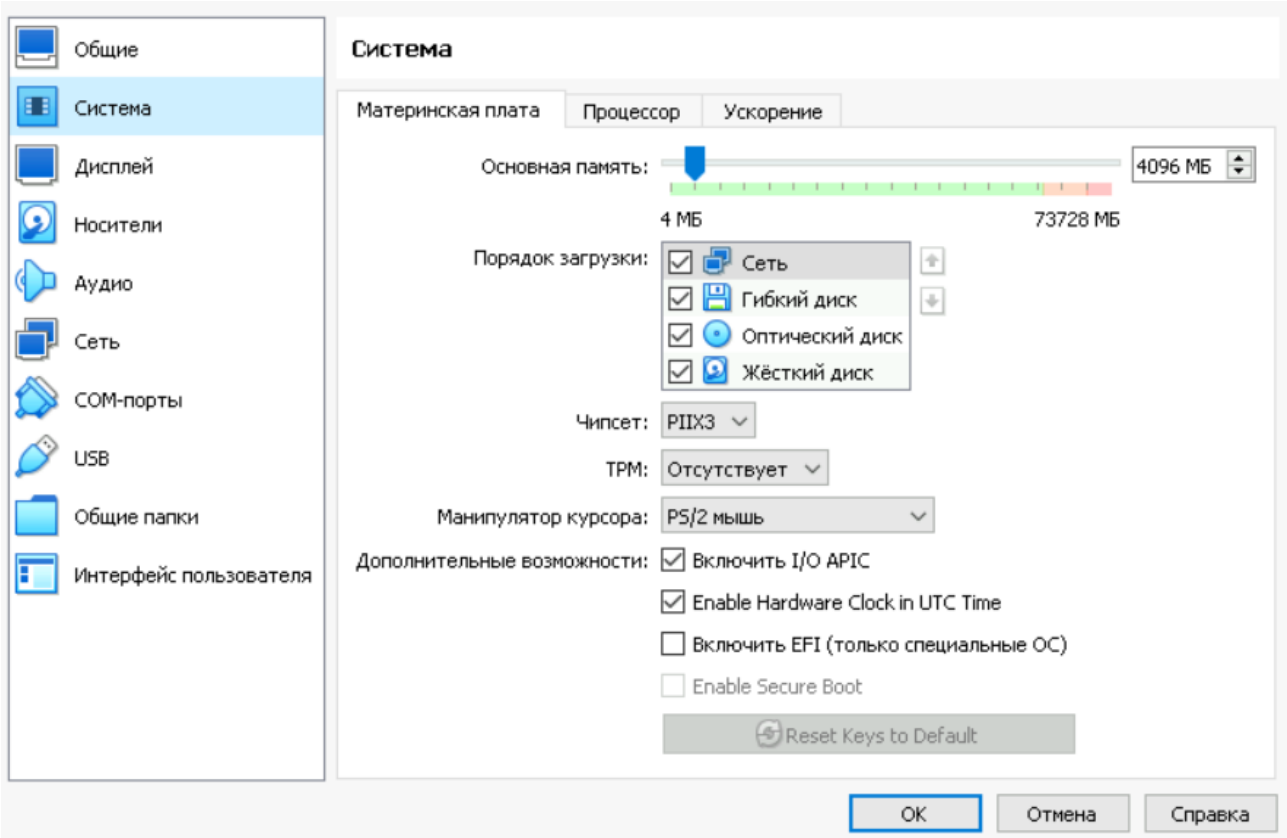
CPU - 1

Сетевой адаптер:

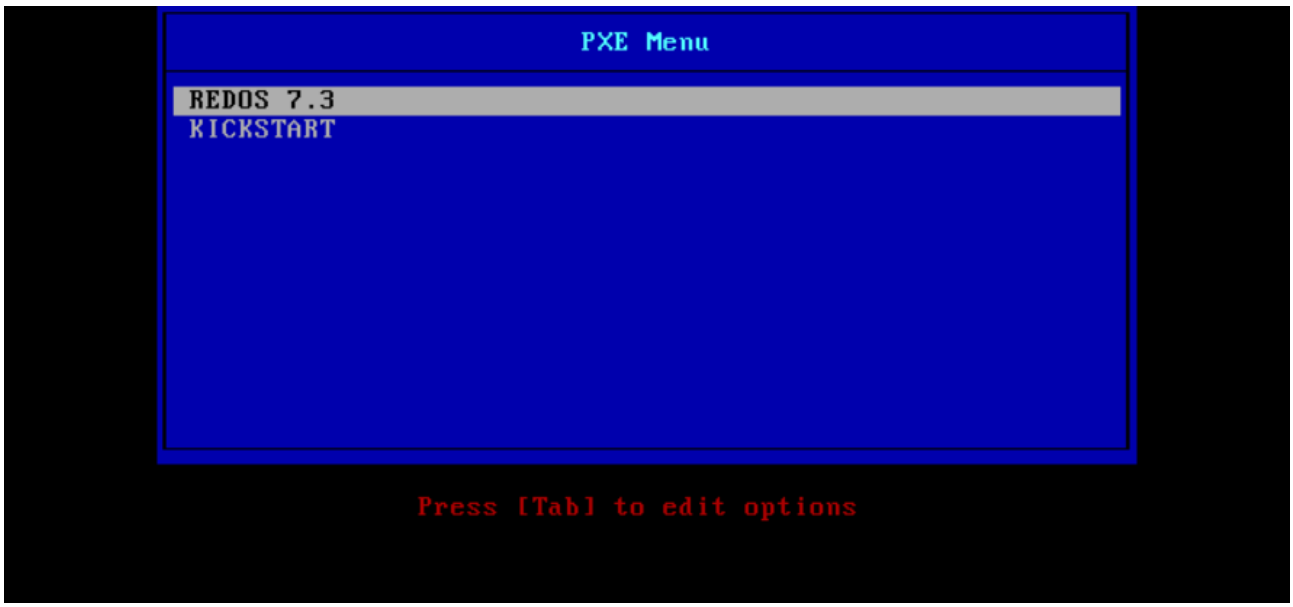
Тип подключения: Сеть NAT

Имя: как на других ваших машинах

Настройте порядок загрузки, как на картинке ниже



20. Запустите ВМ. Появится меню PXE с двумя пунктами. Первый пункт - для ручной установки, второй для автоматизированной установки с использованием kickstart



21. Запустите kikcstart установку