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....4
2.1. Управление разделами дисков....4
2.2. Управление файловыми системами....4
2.3. Монтирование файловых систем....4
Глава 3. Использование RAID и LVM в РЕД ОС....6
3.1. LVM....6
3.2. Программный RAID....6
Глава 4. Управление пользователями....7
4.1. Управление пользователями....7
4.2. Управление средой пользователя....7
4.3. Мониторинг пользовательской активности....8
Глава 5. Настройка сетевых параметров....9
5.1. Простая настройка сети....9
5.2. Настройка SSH....9
Глава 6. Сбор информации, мониторинг и журналирование в РЕД ОС....10
6.1. Управление журналированием....10
Глава 7. Управление программным обеспечением....11
7.1. Управление пакетами rpm....11
7.2. Установка ПО из исходных кодов....11
7.3. Библиотеки....11
Глава 8. Работа с ядром в РЕД ОС....12
8.1. Установка ядра....12
8.2. Управление параметрами ядра....12
8.3. Модули ядра....12
Глава 9. Поиск и устранение неисправностей в РЕД ОС....13
9.1. Восстановление работоспособности системы....13
Глава 10. Автоматизация установки РЕД ОС....14
10.1. Автоматизация развертывания при помощи PXE....14

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:

   _____

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

   _____

   Как описывается раздел, с которого производится загрузка ядра?

   Как опция загрузки ядра?

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

1.2. Управление инициализацией systemd.

1. Определите состояние службы `sshd`.
2. Определите в какую цель по умолчанию загружается система. Как изменить эту цель?
3. Установит цель загрузки по умолчанию в `multi-user.target`. Перезагрузите систему.
4. Прервите загрузку в меню выбора ОС. И, через встроенную оболочку GRUB, загрузите систему в цель `basic.target`. Можете ли вы взаимодействовать с компьютером?
5. Какая команда показывает только текущее состояние сервиса?
6. Проверьте нормально ли работает система в целом. Если состояние системы не соответствует нормальному (`running`), то как определить в чем причина?
7. Остановите и запретите запуск службы `cups`.

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.
2. Выполните команду `sfdisk -s` . Узнайте, что она выдает.
3. На каком разделе вашего диска имеется область подкачки `swap`?
4. В интерактивном режиме команды `fdisk` получите информацию о таблице разделов на одном из ваших новых дисков.
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».
6. На втором диске создайте таблицу разделов GPT. Затем два раздела по 2Гб типа «Linux filesystem» и «Linux swap».
7. Определите код типа раздела для физического тома системы Linux LVM (Logical Volume Manager). Для таблицы разделов типа DOS и типа GPT.

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.
2. Создайте на другом разделе файловую систему EXT2. Отличается ли информация, выдаваемая командой создания файловой системы, от той, которую выдавала предыдущая команда?
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.
4. Определите, где находится первая копия суперблока в только что созданной файловой системе.
5. Проверьте целостность только что файловой системы.
6. Выполните команду проверки этой же файловой системы так, чтобы была выполнена ее полная проверка.

2.3. Монтирование файловых систем.

1. Для файловой системы EXT4, созданной в предыдущих параграфах, создайте каталог - точку монтирования `/storage1` и смонтируйте эту файловую систему.
2. Какой каталог находится в `/storage1`?
3. Для файловой системы XFS создайте каталог - точку монтирования `/storage2` и

смонтируйте эту файловую систему

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?
6. Какая команда позволяет узнать, какой процесс использует файл устройства?
7. Что надо сделать для размонтирования устройства?
8. Настройте автоматическое монтирование каталога `/storage1` в `/etc/fstab`.
9. Для каталога `/storage2` опишите автоматическое монтирование посредством юнита `systemd`.
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.
2. Создайте логический том с зеркальным отображением. Размер тома 1 Гб. Файловая система ext4.
3. Увеличьте размер зеркального тома и файловой системы на нем на 1 Гб.
4. Создайте логический том размером 1 Гб с чередованием.
5. Получите информацию о состоянии группы и использовании дисков в ней.
6. Опишите подключение зеркального тома к каталогу `/mirror1` в `/etc/fstab`.
7. Подключите еще один диск размером 8Гб к виртуальной машине. Добавьте этот диск к группе целиком.
8. Перенесите на новый диск данные с одного из разделов и удалите освобожденный раздел из группы.

3.2. Программный RAID

1. Создайте RAID 5 из трех разделов, размером по 3 Гб каждый. Файловая система ext4.
2. Получите информацию о состоянии созданного RAID массива.
3. Каков размер файловой системы, созданной в RAID массиве?
4. Опишите подключение RAID 5 к каталогу `/raid5` в `/etc/fstab`.

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?
2. Какие символы могут содержаться шифрованной строке пароля во втором поле файла `/etc/shadow` ?
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.
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.
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.
6. Измените имя пользователя test2 на test3.
7. Удалите пользователя test3 передав после этого права владения его файлами суперпользователю и группе sys.
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?
9. Зарегистрируйте пользователя test4 с настройками по умолчанию и установите для него пароль. Изучите содержимое соответствующей пользователю записи в файле `/etc/shadow`.
10. Установите дату устаревания пароля (Password expires) для пользователя test4 на 31 декабря текущего года. Проверьте, что изменилось в `/etc/shadow`.
11. Удалите пароль пользователя и проверьте изменения в `/etc/shadow`.
12. Заблокируйте учетную запись test4.
13. Создайте группу пользователей xusers с GID 1010.
14. Зарегистрируйте себя (пользуясь правами root) в качестве участника группы xusers.
15. От имени своей учетной записи добавьте пользователя test4 в группу xusers.
16. Найдите утилиту, позволяющую изменять имена и GID групп. Измените имя группы на yusers.

4.2. Управление средой пользователя.

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

2. Установите в собственном профиле оболочки псевдоним `l` для команды `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?
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.
5. Измените вид вторичного приглашения командной строки на -> так, чтобы при каждом входе в сеанс Bash значение этой переменной устанавливалось автоматически.

4.3. Мониторинг пользовательской активности.

1. Определите, когда была последний раз загружена система.
2. С помощью опции `-a` команды `who` получите подробную информацию о пользователях и статусе системы.
3. С помощью команды `who` получите список пользователей, входивших в сеанс ранее.
4. Сравните предыдущий список со списком, выводимым командой `last`.
5. Получите отчет по входам в сеанс суперпользователя с помощью `lastlog` .
6. Кто входил в сеанс за последние пять дней?
7. Откройте еще один сеанс и с помощью `loginctl` получите описание и состояние сеанса. Завершите этот сеанс.

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`.
4. На H1 настройка производится с помощью `nmcli`:
    1. Удалите все подключения.
    2. Создайте подключение с именем External. К этому подключению добавьте первый интерфейс. Адрес настройте согласно схеме.
    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.

5.2. Настройка SSH

1. Подключитесь с H1 на server по SSH, используя аутентификацию по паролю.
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.
3. На ВМ H1 настройте ssh подключение по ключам RSA к хосту server под учетной записью sa.
4. С ВМ H1 попробуйте подключиться на ВМ server под пользователем sa без ввода пароля. Должно получиться.
5. В файле /etc/ssh/sshd_config смените стандартный 22 порт SSH на 10022 на ВМ server.
6. Перезапустите службу sshd
7. Попробуйте подключиться к ВМ server не указывая порт. (Попытка должна провалиться)
8. Попробуйте подключиться к ВМ server указывая вручную порт 10022. (Подключение должно пройти успешно)

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.
2. Проверьте, записываются ли в этот файл сообщения при входе в сеанс и выходе из него пользователей.
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?
4. Посмотрите с помощью `journalctl` журнал загрузки системы.
5. Настройте `systemd` вести постоянные журналы.
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.
7. Для файла `/var/log/mylog` установите в качестве дополнительного условия ротации достижение им размера 10 Кб.

Глава 7. Управление программным обеспечением.

7.1. Управление пакетами rpm.

1. Получите список установленных пакетов.
2. Как в RPM увеличить информативность получаемых данных, например, при проверке целостности установленных пакетов.
3. Определите, каким образом можно получить список всех возможных ключей запроса к базе данных RPM?
4. Выведите информацию о полном имени, группе и размере пакета 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.
7. Установите пакет bash-completion.
8. Найдите и установите пакет, который предоставляет утилиту `wireshark`.
9. Обновите ОС.
10. Получите список доступных групп пакетов.
11. Узнайте список пакетов входящих в группу «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
2. Если команда была выполнена успешна - удалитепакет с ней из системы при помощи команды
3. Скачать пакет с исходным кодом можно командой
4. Следуя инструкциям из файла INSTALLING попробуйте собрать пакет самостоятельно.

7.3. Библиотеки.

1. Определите от каких библиотек зависит исполняемый файл утилиты ifconfig (`/bin/ifconfig`), собранный в предыдущем задании.
2. Определите имена файлов библиотек, SO-name которых получены в предыдущем задании.
3. Установлены ли в системе какие-либо библиотеки без участия системы управления пакетами (см. `/usr/local`)?

Глава 8. Работа с ядром в РЕД ОС.

8.1. Установка ядра

1. Установите утилиту 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
2. Просмотрите значение параметра net.ipv4.ip_forward
3. Установите "1" в качестве значения данного параметра на постоянно основе
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?
2. Узнайте, кто является автором модуля e1000.
3. Определите зависимости модуля e1000 от других модулей.
4. Если модуль e1000 загружен, то попробуйте его выгрузить. Что при этом происходит?
5. Вновь загрузите модуль e1000, какова реакция системы?
6. Для какого оборудования предназначен модуль igb?

Глава 9. Поиск и устранение неисправностей в РЕД ОС

9.1. Восстановление работоспособности системы

1. Восстановите работоспособность сломанной машины. Для получения сломанной машины обратитесь к преподавателю.

Глава 10. Автоматизация установки РЕД ОС

10.1. Автоматизация развертывания при помощи PXE

1. Устанавливаем необходимые пакеты
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:
4. Скопируйте файлы для UEFI режима установки РЕД ОС в каталог /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
6. Настройте dhcp-сервер для выдачи адресов в вашей подсети
7. Запустите службу dhcpd:
8. Создайте загрузочное меню для установки в режиме legacy с использованием PXE
9. Создайте загрузочное меню для установки в режиме UEFI с использованием PXE:
10. Скопируйте файл anaconda-ks.cfg из каталога /root.
11. Закомментируйте в файле /var/lib/tftpboot/images/REDOS/ks.cfg следующие строчки:

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

12. Настройте веб-сервер httpd
13. Настройте SELinux
14. Запустите службу httpd:
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` и 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.
17. Проинициализируйте модули systemd:
18. Добавьте службу tftp в автозапуск:
19. Создайте ВМ со следующими параметрами:

HDD - 50 GB

RAM - 4096MB

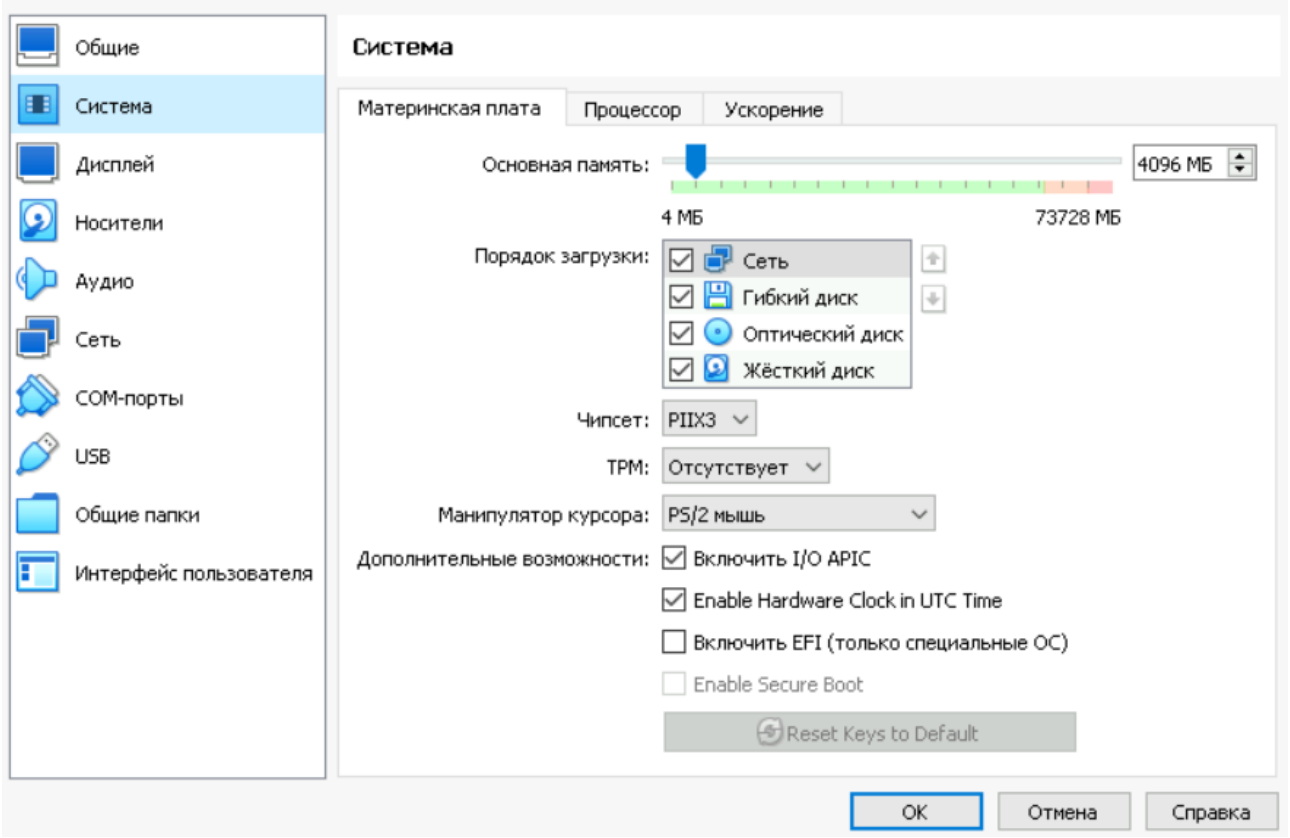
CPU - 1

Сетевой адаптер:

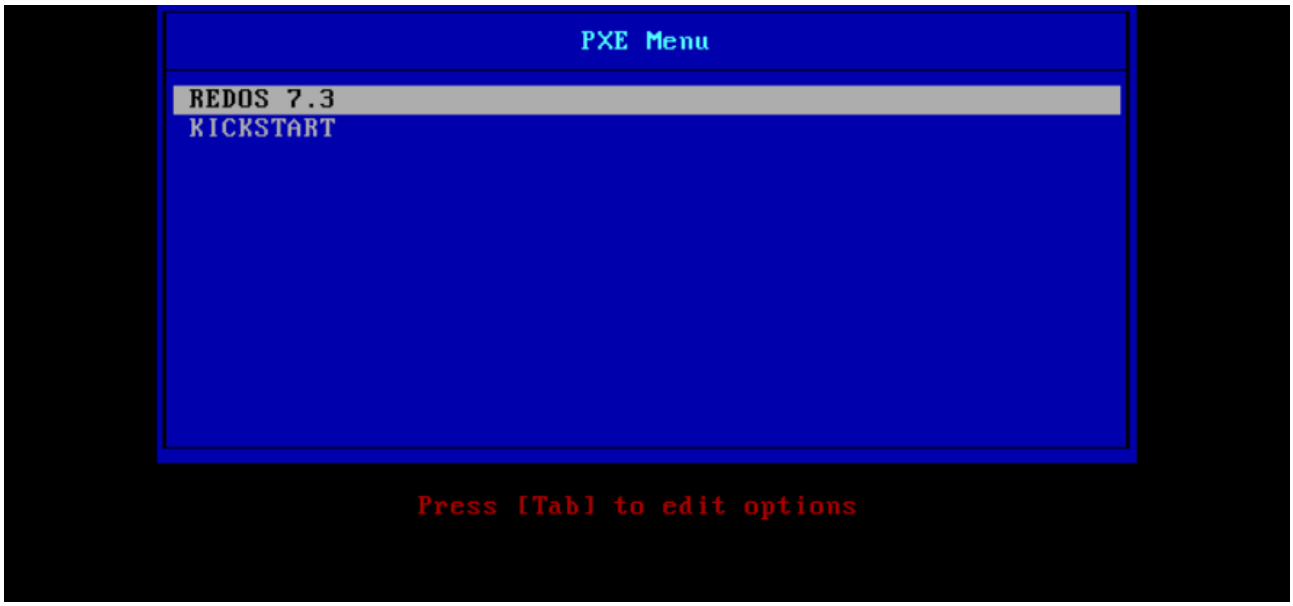
Тип подключения: Сеть NAT

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