

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Локтионова Оксана Геннадьевна

Должность: проректор по учебной работе

Дата подписания: 18.08.2024 05:29:13

Уникальный программный ключ:

0b817ca911e6668abb13a5d426e09a5f61-13a5d426e09a5f61-13a5d426e09a5f61-13a5d426e09a5f61

## МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования  
«Юго-Западный государственный университет»  
(ЮЗГУ)

Кафедра космического приборостроения и систем связи

УТВЕРЖДАЮ  
Проректор по учебной работе  
О.Г. Локтионова  
«19» \_\_\_\_\_ 2020 г.

## СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ LINUX

Методические указания  
по выполнению лабораторных работ  
для студентов, обучающихся по направлению подготовки  
11.03.02 «Инфокоммуникационные технологии и системы связи»

Курск 2020

УДК 004.451

Составитель: И.Г. Бабанин

Рецензент

Кандидат технических наук, доцент кафедры *Е.О. Брежнева*

**Системное администрирование Linux** : методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т; сост.: И.Г. Бабанин.– Курск, 2020. – 14 с.

Методические указания по выполнению лабораторных работ содержат цель, задания по выполнению лабораторных работ, требования к оформлению отчёта.

Методические указания полностью соответствуют учебному плану по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи», а также рабочей программе дисциплины.

Предназначены для студентов, обучающихся по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи».

Текст печатается в авторской редакции

Подписано в печать *19.10.20*. Формат 60x84 1/16.  
Усл. печ. л. 0,81. Уч.-изд. л. 0,74. Тираж 100 экз. Заказ *319*. Бесплатно.  
Юго-Западный государственный университет.  
305040, г. Курск, ул. 50 лет Октября, 94.

# **1 Лабораторная работа №1 «Обеспечение целостности и доступности данных. RAID, LVM»**

## **1.1 Цель работы**

Получение теоретических и практических навыков построения и управления RAID массивами и логическими томами.

## **1.2 Задание по выполнению лабораторной работой**

- 1) Добавить пять виртуальных жестких дисков.
- 2) Запустить Linux.
- 3) Установить mdadm.
- 4) Ознакомится с утилитой mdadm, ее возможностями и параметрами.
- 5) В отдельном терминале следить за состоянием файла /proc/mdstat
- 6) Собрать RAID 1 с помощью mdadm.
- 7) Создать на созданном RAID файловую систему ext4.
- 8) Смонтировать созданную файловую систему.
- 9) Записать туда файл raid.txt с произвольным содержимым.
- 10) Разрушить один из дисков RAID и проследить за происходящим в файле /proc/mdstat
- 11) Проверить целостность файла raid.txt
- 12) Остановить RAID 1.
- 13) Очистить информацию дисков о принадлежности к программному RAID.
- 14) Собрать RAID 0 с помощью mdadm.
- 15) Создать на созданном RAID файловую систему ext3.
- 16) Смонтировать созданную файловую систему.
- 17) Записать туда файл raid.txt с произвольным содержимым.
- 18) Разрушить один из дисков RAID и проследить за происходящим в файле /proc/mdstat
- 19) Проверить целостность файла raid.txt
- 20) Остановить RAID 0.
- 21) Очистить информацию дисков о принадлежности к программному RAID.
- 22) Собрать RAID 5 с диском горячей замены с помощью mdadm.
- 23) Создать на созданном RAID файловую систему ext4.

- 24) Смонтировать созданную файловую систему.
- 25) Записать туда файл raid.txt с произвольным содержимым.
- 26) Разрушить три диска RAID и проследить за происходящим в файле /proc/mdstat
- 27) Проверить целостность файла raid.txt
- 28) Остановить RAID 5.
- 29) Очистить информацию дисков о принадлежности к программному RAID.
- 30) Собрать RAID 10 с диском горячей замены с помощью mdadm.
- 31) Создать на созданном RAID файловую систему ext2.
- 32) Смонтировать созданную файловую систему.
- 33) Записать туда файл raid.txt с произвольным содержимым.
- 34) Разрушить два диска RAID и проследить за происходящим в файле /proc/mdstat
- 35) Проверить целостность файла raid.txt
- 36) Остановить RAID 10.
- 37) Очистить информацию дисков о принадлежности к программному RAID.
- 38) Инициализировать физические диски, поверх которых будет создан LVM.
- 39) Создать группу томов на основе четырех виртуальных жестких дисков.
- 40) Создать логический том.
- 41) На созданном логическом томе создать файловую систему.
- 42) Смонтировать систему и создать файл файл LVM.txt .
- 43) Добавить в группу томов еще один виртуальный жесткий диск.
- 44) Определить количество добавленных экстендов.
- 45) Расширить созданный логический том на размер добавленных экстендов.
- 46) Увеличить размер файловой системы.
- 47) Сделать снапшот логического тома.
- 48) Удалить группу томов и снапшот.

## 2 Лабораторная работа №2 «Файловые подсистемы»

### 2.1 Цель работы

Получение теоретических и практических навыков работы с таблицами разделов (MBR и GPT), создания разделов и файловых систем.

### 2.2 Задание по выполнению лабораторной работой

- 1) Добавьте в виртуальную машину с операционной системой Linux виртуальный жесткий диск (делается это в настройках виртуальной машины).
- 2) Запустите виртуальную машину с операционной системой Linux.
- 3) Ознакомьтесь с командой `fdisk` и ее возможностями из справочной документации.
- 4) Создайте таблицу разделов (3 первичных и 1 логический) с помощью команды `fdisk` на **добавленном** виртуальном диске (обычно это диск `/dev/sdb`).
- 5) Запишите изменения на диск
- 6) Проверьте факт создания разделов используя команду `fdisk`. (Так же, создание разделов можно проверить используя команду `ls /dev/sd*`)
- 7) Отформатируйте созданные разделы в файловую систему `ext4`.
- 8) Ознакомьтесь с командами `mount` и `umount` и их возможностями из справочной документации.
- 9) Смонтируйте созданные разделы и создайте там произвольные файлы.
- 10) Сделайте резервную копию MBR с помощью утилиты `DD`.
- 11) Сотрите таблицу разделов MBR с помощью утилиты `DD`.
- 12) Восстановите MBR с помощью утилиты `DD`.
- 13) Смонтируйте разделы и проверьте целостность данных.
- 14) Отмонтируйте разделы.
- 15) Установите `gdisk` `<sudo apt-get install gdisk>`
- 16) Создайте таблицу разделов GPT (5 первичных разделов) с помощью `gdisk`.
- 17) Отформатируйте созданные разделы в файловую систему `ext3`.

- 18) Смонтируйте созданные разделы и создайте там произвольные файлы.
- 19) Сделайте резервную копию GPT с помощью утилиты DD, предварительно определив необходимое количество байт для резервной копии.
- 20) Сотрите GPT с помощью утилиты DD.
- 21) Восстановите GPT с помощью утилиты DD.
- 22) Смонтируйте разделы и проверьте целостность данных.
- 23) Отмонтируйте разделы.
- 24) Определите достоинства и недостатки таблиц разделов MBR и GPT.

### **3 Лабораторная работа №3 «Основы работы в командной строке»**

#### **3.1 Цель работы**

Первичное знакомство с командным интерпретатором. Изучение базовых команд операционной системы Linux.

#### **3.2 Задание по выполнению лабораторной работой**

- 1) Откройте терминал.
- 2) Ознакомьтесь с возможностями команды pwd с помощью команды man:
- 3) Определите текущий каталог, в котором вы находитесь командой pwd:
- 4) Ознакомьтесь с возможностями команды cd с помощью команды man:
- 5) Перейдите в корневой каталог командой cd
- 6) Ознакомьтесь с возможностями команды ls с помощью команды man:
- 7) Просмотрите содержимое корневого каталога командой ls:
- 8) Сделайте копию экрана для использования в отчете по лабораторной работе .
- 9) Вернитесь в домашний каталог, используя команду cd без параметров:
- 10) Ознакомьтесь с возможностями команды mkdir с помощью команды man:

- 11) Создайте каталог «test», используя команду mkdir:
- 12) Перейдите в каталог «test», используя команду cd:
- 13) Просмотрите содержимое каталога, используя команду ls:
- 14) Создайте каталог «test2», используя команду mkdir:
- 15) Ознакомьтесь с возможностями команды touch с помощью команды man:
- 16) Создайте файл «text» в каталоге «test2» используя команду touch:
- 17) Ознакомьтесь с возможностями команды mv с помощью команды man:
- 18) Переименуйте файл «text» в «textSIT» используя команду mv
- 19) Ознакомьтесь с возможностями команды cp с помощью команды man:
- 20) Скопируйте файл «textSIT» в каталог «test2» под именем «copy.txt», используя команду cp:
- 21) Ознакомьтесь с возможностями команды ln с помощью команды man:
- 22) Создайте жесткую ссылку «link» на файл «copy.txt» используя команду ln:
- 23) Создайте символическую ссылку «simlink» на файл «copy.txt» используя команду ln:
- 24) Просмотрите результаты в текущем каталоге при помощи команды ls с аргументами la:
- 25) Сделайте копию экрана для использования в отчете по лабораторной работе.
- 26) Удалите созданные вами файлы и ссылки в лабораторной работе используя команду rm
- 27) Сделайте копию экрана для использования в отчете по лабораторной работе.

## **4 Лабораторная работа №4 «Разграничение прав доступа»**

### **4.1 Цель работы**

Изучение механизмов управления доступа к ресурсам, прав доступа. Постигание понятия пользователя и группы. Приобретение практических навыков управления пользователями при помощи консольных утилит. Приобретение навыков работы с

правами пользователей и правами на файлы, каталоги при помощи консольных утилит.

## 4.2 Задание по выполнению лабораторной работой

- 1) Откройте два терминала (в серверных Linux для переключения между терминалами (tty) обычно используется сочетание клавиш Alt+F[1-5]). В одном из них получите права суперпользователя используя команду `sudo su`:
- 2) Изучите как создать пользователя с домашним каталогом с помощью команды `useradd` из справочной документации `man`
- 3) Используя `useradd` создайте пользователя «sit2» с домашним каталогом «sit2».
- 4) Установите пароль для нового пользователя «sit2» с помощью команды `passwd sit2`
- 5) Выйдите из суперпользователя командой `exit`
- 6) Войдите под первым терминалом в пользователя «sit», во втором в пользователя «sit2».
- 7) Посмотрите какой идентификатор получил пользователь «sit» и пользователь «sit2» используя команду `id`
- 8) Посмотрите права доступа на домашний каталог пользователей «sit» и «sit2», используя команду `ls`
- 9) Создайте файл под пользователем «sit2» с маской 0077 используя `umask`
- 10) Попробуйте прочитать его содержимое под пользователем «sit» используя команду `cat`
- 11) Измените права доступа на файл так, чтобы пользователь «sit» мог записывать в файл, но не читать его.
- 12) Запишите текстовую информацию в файл из под пользователя «sit» используя консольный текстовый редактор `vi` или `nano`
- 13) Проверьте права на файл, и прочитайте его содержимое из под пользователя «sit2»
- 14) Создайте каталог из под пользователя «sit2»
- 15) Установите права записи для группы пользователей на данный каталог
- 16) Добавьте пользователя «sit» в группу «sit2» с помощью команды `usermod`
- 17) Проверьте в какие группы входит пользователь «sit»



- 18) Создайте несколько файлов в каталоге, который был создан пользователем «sit2» из под пользователя «sit».
- 19) Ознакомьтесь как удалить пользователя вместе с содержимым его домашнего каталога из справочной документации
- 20) Удалите пользователя «sit2» вместе с его домашним каталогом.

## **5 Лабораторная работа №5 «Шифрование данных»**

### **5.1 Цель работы**

Получение теоретических и практических навыков работы с программными средствами шифрования данных.

### **5.2 Задание по выполнению лабораторной работой**

- 1) Установить PGP, GPG `<sudo apt-get install pgpgpg>`
- 2) Произвести операции шифрования и дешифрования над произвольными файлами. Для шифрования используйте команду `<gpg -c>`. Для дешифрования `<gpg -decrypt-file>` (В этом случае в директории зашифрованного файла будет создан расшифрованный. Если нужно лишь вывести на экран расшифрованное содержимое используйте `<gpg -decrypt>`)
- 3) Установить TrueCrypt. Нам потребуется версия 7.1a.
- 4) Создать криптоконтейнер, примонтировать его как виртуальный диск.
- 5) Поместить в криптоконтейнер какую-то информацию.
- 6) Отмонтировать диск и переместить криптоконтейнер.
- 7) Повторно примонтировать криптоконтейнер как виртуальный диск. Убедиться, что криптоконтейнер может передаваться и использоваться независимо.
- 8) Установить LUKS/dm-crypt `<sudo apt-get update>`, `<sudo apt-get install cryptsetup>`.
- 9) Создаем файл, где будем хранить зашифрованные данные. Самый простой способ `<fallocate -l 512M /root/test1>`, где /root - директория хранения файла, test1 - имя файла. Так же для создания этого файла можно использовать команду dd. `<dd if=/dev/zero of=/root/test2 bs=1M count=512>`. Третий способ - использовать

команду `dd` и заполнить файл случайными данными. `<dd if=/dev/urandom of=/root/test3 bs=1M count=512>`.

10) Создать криптоконтейнер. `<cryptsetup -y luksFormat /root/test1>` (нужно будет согласиться переписать данные и задать пароль).

11) Открыть контейнер. `<cryptsetup luksOpen /root/test1 volume1>`. (`volume1` - имя контейнера, его мы задаем этой командой). При этом будет создан файл `/dev/mapper/volume1`.

12) Создать в нем файловую систему `<mkfs.ext4 -j /dev/mapper/volume1>`.

13) Создать папку для монтирования `<mkdir /mnt/files>`.  
Монтировать `<mount /dev/mapper/volume1 /mnt/files>`

14) Теперь перенесем какие-нибудь файлы в криптоконтейнер. Например, скопируем папку `/etc` `<cp -r /etc/* /mnt/files>`.

15) Размонтировать `<umount /mnt/files>`.

16) Теперь закрываем `volume1`. `<cryptsetup luksClose volume1>`. После этого наши данные зашифрованы.

17) Чтобы открыть их выполним `<cryptsetup luksOpen /root/test1 volume1>` и `<mount /dev/mapper/volume1 /mnt/files>`

## **6 Лабораторная работа №6 «Настройка ЛВС»**

### **6.1 Цель работы**

Получение теоретических и практических навыков построения ЛВС

### **6.2 Задание по выполнению лабораторной работой**

1) Установите на 4 виртуальные машины операционную систему Ubuntu Server. Условно назовем эти машины: Hacker, Server, WWW, DataBase.

2) Настройте сеть. В настройках сети (По умолчанию Файл->настройки-> сеть, на вкладке Виртуальные сети хоста) создаем 2 адаптера ( По умолчанию 1 уже создан).

3) Для каждого из них прописать разные IP-адреса `192.168.*.*`, где `*` - любое число от 0 до 255 (Если хотите сделать все как на схеме, на первом оставьте значения по умолчанию - `192.168.56.1`, а на втором `192.168.57.1`). На уже имеющемся адаптере можете

посмотреть настройки DHCP и, по аналогии, настроить DHCP для второго адаптера. DHCP-сервер будет выдавать всем подключенным в сеть машинам IP-адреса автоматически через определенные промежутки времени. В данной лабораторной работе настройка DHCP в VirtualBox никак не отразится на ее выполнении, а наоборот, только упростит построение сети между виртуальными машинами.

4) Теперь в настройках каждой из виртуальных машин выберите вкладку сеть.

5) В машине Hacker создайте 2 адаптера. В первом, чтобы вы могли использовать интернет, выберите тип подключения NAT. Во втором - виртуальный адаптер хоста (если Вы делаете все по схеме выберите тот, где ip-адрес 192.168.56.\*).

6) На машине Server создайте 3 адаптера. Первый - чтобы использовать интернет. Второй - тот же виртуальный адаптер хоста, что и в машине Hacker. Третий - виртуальный адаптер хоста, но выбираете уже второй ( если вы делаете все по схеме выбираете тот, где ip-адрес 192.168.57.\*).

7) На машинах WWW и DataBase создайте 2 адаптера. Первый - выход в интернет. Второй - виртуальный адаптер хоста (второй, тот где 196.168.57.\*).

8) Особенностью подключения типа виртуальный адаптер хоста, является то, что компьютер, на котором запущен VirtualBox так же доступен, что может помочь во второй части лабораторной работы.

9) Настройка статического IP-адреса (если используется на DHCP). Настройка сети осуществляется с помощью создания виртуального адаптера хоста. При первичном запуске всех виртуальных машин необходимо внести изменения в файл /etc/network/interfaces.

10) В нем необходимо прописать новое соединение в форме:

```
auto eth1
iface eth1 inet static
address 192.168.58.103
netmask 255.255.255.0
gateway 192.168.58.102
```

Поле `address` — ip адрес, выделяющийся машине, `netmask` — маска сети, используемая для разграничения адреса сети и непосредственно машины в ней, а `gateway` — шлюз, на который пойдут отправляемые пакеты. В данной лабораторной работе, например, в поле `gateway` пишется ip-адрес виртуального адаптера хоста на сервере, соответствующего локальной сети. Поэтому `gateway` не нужно прописывать для сервера, если этот сервер сам не подключается к какому-либо другому серверу. Запись осуществляется с правами суперпользователя. После записи необходима перезагрузка системы.

11) Чтобы изменения вступили в силу необходимо перезапустить систему.

12) Просмотреть сетевые интерфейсы вы можете, используя команду `ifconfig`

13) После настройки, используйте команду `ping` и проверьте локальное соединение.

14) Машина `Hacker` – «злоумышленник», который попытается просканировать нашу сеть. Для того, чтобы он смог это сделать, необходимо установить универсальное средство сканирования – `Nmap`:

```
sudo apt-get install nmap
```

15) `Server` – сервер, атаку на который совершает `Hacker`. Во второй части работы будем устанавливать на него CMS `WordPress`.

16) `WWW` – web-сервер, с помощью которого осуществляется доступ к базе данных `DataBase`. Соответственно, как и для `Server`, устанавливаем web-сервер. Также необходимо установить `PHP`.

```
sudo apt-get install php5 libapache2-mod-php5 php5-mysql
```

Далее, необходимо создать файл `/var/www/index.php`, в который прописывается следующий скрипт:

```
<?php
$link = mysql_connect('192.168.57.101', 'sit', 'sit');
if (!$link) {
die('Error: ' . mysql_error());
}
```

```
echo 'Ok';  
mysql_close($link);  
?>
```

Этот скрипт определяет подключение WWW к DataBase, и если ввести в адресное поле браузера ip-адрес WWW /index.php, то при успешном подключении к базе данных будет выведено «ОК».

17) Настройка базы данных. На DataBase необходимо установить Mysql – универсальную систему управления базами данных.

```
sudo apt-get install mysql-server
```

18) Запускаем MySQL:

```
sudo mysql -p
```

Затем, в MySQL необходимо добавить набор привилегий для пользователя

(по умолчанию sit)

```
GRANT ALL PRIVILEGES ON *.* TO sit@localhost IDENTIFIED BY 'sit' WITH GRANT OPTION  
GRANT ALL PRIVILEGES ON *.* TO sit@"%" IDENTIFIED BY 'sit' WITH GRANT OPTION
```

19) Далее необходимо в файле /etc/mysql/my.cnf найти и закомментировать (поставить в начале строки символ #) строчку bind-address = 127.0.0.1.

## 7 Список использованных источников

1) Пантюхин, И.С. Лабораторный практикум по основам информационной безопасности [Электронный ресурс]. – СПб. : ИТМО, 2019–. – Режим доступа: [https:// пантюхин.рф/оиб/](https://пантюхин.рф/оиб/), свободный. – Загл. с экрана.