Факультет компьютерных технологий и прикладной математики

Кафедра вычислительных технологий

02.03.02

Информационная безопасность

Лабораторная работа № 5

Тема: Обеспечение целостности и доступности данных. Raid, LVM. Восстановление данных.

## Цель работы

Получение теоретических и практических навыков построения и управления RAID массивами и логическими томами, а также навыков программного восстановления данных.

## Указания к работе

Вначале студенты изучают теоретическую часть. Далее каждый студент должен выполнить задания, а также ответить на вопросы к лабораторной работе. За проделанную работу студент может получить оценку от «неудовлетворительно» до «отлично». Для получения оценки «удовлетворительно» студент должен выполнить ВСЕ задания к лабораторной работе. Оценка «хорошо» ставится, если студент ответил на ВСЕ вопросы к лабораторной работе. Оценку «отлично» студент получает, если подготовлен отчёт по лабораторной работе.

ОЦЕНКУ ЗА ПРОДЕЛАННУЮ РАБОТУ МОЖНО ПОВЫСИТЬ ДО СДАЧИ СЛЕДУЮЩЕЙ ЛАБОРАТОРНОЙ РАБОТЫ.

## Теоретическая часть

Консольные команды

- mdadm <параметры> – Консольная программа управления программными RAID массивами в Linux.
- lvm <параметры> – Консольная программа управления логическими томами LVM.
- parted <параметры> – Консольная программа для управления дисками

• watch <параметры> – Консольная программа, которая позволяет следить за изменениями в выводе команды.

## RAID

RAID (Redundant Array of Independent Disks – избыточный массив независимых жестких дисков) – массив, состоящий из нескольких дисков, управляемых программным или аппаратным контроллером, связанных между собой и воспринимаемых как единое целое. В зависимости от того, какой тип массива используется, может обеспечивать различные степени быстродействия и отказоустойчивости. Служит для повышения надежности хранения данных и/или для повышения скорости чтения/записи информации.

Калифорнийский университет в Беркли предложил следующие уровни спецификации RAID, которые являются стандартом во всем мире:

• RAID 0 представлен как дисковый массив повышенной производительности, без отказоустойчивости. (Требуется минимум 2 диска)

• RAID 1 определен как зеркальный дисковый массив. (Требуется минимум 2 диска)

• RAID 2 массивы, в которых применяется код Хемминга. (Требуется минимум 7 дисков, для рационального использования)

• RAID 3 и 4 используют массив дисков с чередованием и выделенным диском четности. (Требуется минимум 4 диска)

• RAID 5 используют массив дисков с чередованием и «невыделенным диском четности». (Требуется минимум 3 диска)

• RAID 6 используют массив дисков с чередованием и двумя независимыми «четностями» блоков. (Требуется минимум 4 диска)

• RAID 10 – RAID 0, построенный из RAID 1 массивов. (Требуется минимум 4 диска, четное количество)

• RAID 50 – RAID 0, построенный из RAID 5 массивов. (Требуется минимум 6 дисков, четное количество)

• RAID 60 – RAID 0, построенный из RAID 6 массивов. (Требуется минимум 8 дисков, четное количество)

Пример создания RAID 10

Проверим наличие виртуальных дисков.

```
sit@sit:~$ sudo parted -l
Model: ATA VBOX HARDDISK (scsi)
Disk /dev/sda: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size    Type      File system  Flags
 1      1049kB  256MB   255MB   primary   ext2         boot
 2      257MB   21.5GB  21.2GB  extended
 5      257MB   21.5GB  21.2GB  logical               lvm



Error: /dev/sdb: unrecognised disk label
Model: ATA VBOX HARDDISK (scsi)
Disk /dev/sdb: 8590MB
Sector size (logical/physical): 512B/512B
Partition Table: unknown
Disk Flags:

Error: /dev/sdc: unrecognised disk label
Model: ATA VBOX HARDDISK (scsi)
Disk /dev/sdc: 8590MB
Sector size (logical/physical): 512B/512B
Partition Table: unknown
Disk Flags:

Error: /dev/sdd: unrecognised disk label
```

```
Model: ATA VBOX HARDDISK (scsi)
Disk /dev/sdd: 8590MB
Sector size (logical/physical): 512B/512B
Partition Table: unknown
Disk Flags:

Error: /dev/sde: unrecognised disk label
Model: ATA VBOX HARDDISK (scsi)
Disk /dev/sde: 8590MB
Sector size (logical/physical): 512B/512B
Partition Table: unknown
Disk Flags:

Error: /dev/sdf: unrecognised disk label
Model: ATA VBOX HARDDISK (scsi)
Disk /dev/sdf: 8590MB
Sector size (logical/physical): 512B/512B
Partition Table: unknown
Disk Flags:

Model: Linux device-mapper (linear) (dm)
Disk /dev/mapper/sit--vg-swap_1: 533MB
Sector size (logical/physical): 512B/512B
Partition Table: loop
Disk Flags:

Number  Start  End    Size   File system     Flags
 1      0.00B  533MB  533MB  linux-swap(v1)
```

```
Model: Linux device-mapper (linear) (dm)
Disk /dev/mapper/sit--vg-root: 20.7GB
Sector size (logical/physical): 512B/512B
Partition Table: loop
Disk Flags:

Number  Start  End     Size    File system  Flags
 1      0.00B  20.7GB  20.7GB  ext4



sit@sit:~$
```

Как видно из листинга, у нас присутствуют диски sda (на котором установлена операционная система Linux), sdb, sdc, sdd, sde, sdf. Теперь можно построить массив RAID 10 из дисков sdb, sdc, sdd и sde, а диск sdf пометим как диск горячей замены (применяется для горячей замены в случае отказа одного из дисков RAID массива).

Необходимо открыть два терминала. В одном создается RAID массив, в другом осуществляется процесс наблюдения за созданием RAID массива.

Запустим процесс отслеживания состояния RAID массивов в терминале №1:

```
sit@sit:~$ sudo watch -n1 cat /proc/mdstat
```

Создадим RAID 10 в отдельном терминале №2:

```
sit@sit:~$ sudo mdadm -C /dev/md0 -l 10 -n 4 -x 1 /dev/sd[b-f]
[sudo] password for sit:
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/md0 started.
sit@sit:~$
```

В терминале №1 наблюдаем процесс создания RAID 10:

```
Every 1.0s: cat /proc/mdstat                    Wed Sep 23 18:02:03
2015
```

```
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
md0 : active raid10 sdf[4](S) sde[3] sdd[2] sdc[1] sdb[0]
      16760832 blocks super 1.2 512K chunks 2 near-copies [4/4] [UUUU]
      [============>.....]  resync = 61.3% (10286144/16760832) finish=0.5min
speed=201781K/sec

unused devices: <none>
```

Создадим раздел в 1GB с файловой системой ext4 на созданном RAID 10:

```
sit@sit:~$ sudo parted /dev/md0
[sudo] password for sit:
GNU Parted 3.2
Using /dev/md0
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) mklabel
New disk label type? GPT
Warning: The existing disk label on /dev/md0 will be destroyed and all data on this
disk will be lost. Do you want to continue?
Yes/No? yes
(parted) mkpart
Partition name?  []?
File system type?  [ext2]? ext4
Start? 0
End? 1GB
Warning: The resulting partition is not properly aligned for best performance.
Ignore/Cancel? Ignore
(parted) print
Model: Linux Software RAID Array (md)
Disk /dev/md0: 17.2GB
```

```
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:

Number  Start   End     Size    File system  Name  Flags
 1      17.4kB  1000MB  1000MB  ext4

(parted)
```

Отформатируем созданный раздел в файловую систему ext4:

```
sit@sit:~$ sudo mkfs.ext4 /dev/md0p1
```

Смонтируем созданный раздел:

```
sudo mount -t ext4 /dev/md0p1 /mnt/
```

Скопируем файлы на раздел с файловой системой ext4:

```
sudo cp -R /var/log/* /mnt/
```

Разрушим один диск и проверим целостность данных.

Наблюдаем процесс как диск горячей замены встает на место сбойного диска:

```
Every 1.0s: cat /proc/                                  Wed Sep 23 19:52:04 2015

Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
md0 : active raid10 sdf[4] sde[3] sdd[2] sdc[1] sdb[0](F)
      16760832 blocks super 1.2 512K chunks 2 near-copies [4/3] [_UUU]
      [====>.............]  recovery = 21.8% (1832192/8380416) finish=0.4min
speed=229024K/sec

unused devices: <none>
```

Убедимся в целостности данных на разделе:

```
sit@sit:~$ ls -la /mnt/
total 968
drwxr-xr-x  9 root root   4096 Sep 23 19:34 .
```

```
drwxr-xr-x 22 root root   4096 Sep 19 14:26 ..
-rw-r--r--  1 root root  18625 Sep 23 19:34 alternatives.log
drwxr-xr-x  2 root root   4096 Sep 23 19:34 apt
-rw-r-----  1 root root  41820 Sep 23 19:34 auth.log
-rw-r--r--  1 root root  63653 Sep 23 19:34 bootstrap.log
-rw-------  1 root root      0 Sep 23 19:34 btmp
drwxr-xr-x  2 root root   4096 Sep 23 19:34 dist-upgrade
-rw-r-----  1 root root     31 Sep 23 19:34 dmesg
-rw-r--r--  1 root root 339677 Sep 23 19:34 dpkg.log
-rw-r--r--  1 root root  32032 Sep 23 19:34 faillog
drwxr-xr-x  2 root root   4096 Sep 23 19:34 fsck
drwxr-xr-x  3 root root   4096 Sep 23 19:34 installer
-rw-r-----  1 root root 189514 Sep 23 19:34 kern.log
drwxr-xr-x  2 root root   4096 Sep 23 19:34 landscape
-rw-r--r--  1 root root 292292 Sep 23 19:34 lastlog
drwx------  8 root root  16384 Sep 23 19:32 lost+found
-rw-r-----  1 root root 173386 Sep 23 19:34 syslog
-rw-r-----  1 root root   3090 Sep 23 19:34 syslog.1
-rw-r-----  1 root root    591 Sep 23 19:34 syslog.2.gz
-rw-r-----  1 root root  30788 Sep 23 19:34 syslog.3.gz
drwxr-x---  2 root root   4096 Sep 23 19:34 unattended-upgrades
-rw-r--r--  1 root root   8832 Sep 23 19:34 wtmp


sit@sit:~$ sudo head -n 10 /mnt/auth.log
Sep 19 14:38:02 sit systemd-logind[506]: Watching system buttons on
/dev/input/event0 (Power Button)
Sep 19 14:38:02 sit systemd-logind[506]: Watching system buttons on
/dev/input/event1 (Sleep Button)
Sep 19 14:38:02 sit systemd-logind[506]: Watching system buttons on
/dev/input/event5 (Video Bus)
```

```
Sep 19 14:38:02 sit systemd-logind[506]: New seat seat0.
Sep 19 14:40:10 sit systemd-logind[508]: Watching system buttons on
/dev/input/event0 (Power Button)
Sep 19 14:40:10 sit systemd-logind[508]: Watching system buttons on
/dev/input/event1 (Sleep Button)
Sep 19 14:40:10 sit systemd-logind[508]: Watching system buttons on
/dev/input/event6 (Video Bus)
Sep 19 14:40:10 sit systemd-logind[508]: New seat seat0.
Sep 19 14:40:27 sit login[529]: pam_unix(login:session): session opened for user
sit by LOGIN(uid=0)
Sep 19 14:40:27 sit systemd-logind[508]: New session c1 of user sit.

sit@sit:~$ sudo head -n 10 /mnt/syslog
Sep 23 07:17:01 sit CRON[2263]: (root) CMD (   cd / && run-parts --report
/etc/cron.hourly)
Sep 23 08:17:01 sit CRON[2266]: (root) CMD (   cd / && run-parts --report
/etc/cron.hourly)
Sep 23 09:17:01 sit CRON[2269]: (root) CMD (   cd / && run-parts --report
/etc/cron.hourly)
Sep 23 10:17:01 sit CRON[2272]: (root) CMD (   cd / && run-parts --report
/etc/cron.hourly)
Sep 23 10:46:05 sit dhclient: DHCPREQUEST of 10.0.2.15 on eth0 to 10.0.2.2
port 67 (xid=0x6a9a8b24)
Sep 23 10:46:05 sit dhclient: DHCPACK of 10.0.2.15 from 10.0.2.2
Sep 23 10:46:05 sit dhclient: bound to 10.0.2.15 -- renewal in 42505 seconds.
Sep 23 11:17:01 sit CRON[2285]: (root) CMD (   cd / && run-parts --report
/etc/cron.hourly)
Sep 23 12:17:01 sit CRON[2288]: (root) CMD (   cd / && run-parts --report
/etc/cron.hourly)
```

```
Sep 23 13:17:01 sit CRON[2291]: (root) CMD (   cd / && run-parts --report
/etc/cron.hourly)
```

Сделаем имитацию замены извлечением и вставки нового диска.:

```
sit@sit:~$ sudo mdadm /dev/md0 -r /dev/sdb
mdadm: hot removed /dev/sdb from /dev/md0
sit@sit:~$ sudo mdadm /dev/md0 -a /dev/sdb
mdadm: added /dev/sdb
sit@sit:~$
```

Наблюдаем что диск sdb пометился как диск горячей замены.:

```
Every 1.0s: cat /proc/                          Wed Sep 23 19:59:09 2015

Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
md0 : active raid10 sdb[5](S) sdf[4] sde[3] sdd[2] sdc[1]
      16760832 blocks super 1.2 512K chunks 2 near-copies [4/4] [UUUU]

unused devices: <none>
```

Для того чтобы остановить RAID используется параметр **-stop** команды mdadm.

Для очистки записи принадлежности к программному RAID используется параметр **-zero-superblock** команды mdadm.

## LVM

LVM (Logical Volume Manager) – менеджер логических томов является уникальной системой управления дисковым пространством. Она позволяет с легкостью использовать и эффективно управлять дисковым пространством. Уменьшает общую нагруженность и сложность существующей системы. У логических томов, которые созданы через LVM, можно легко изменять размер, а названия, которые им даны, помогут в дальнейшем определить назначение тома.

PV, Physical Volume или физический том. Чаще всего это раздел на диске или весь диск. К ним относят устройства программного и аппаратного RAID массивов (которые могут включать в себя еще несколько физических дисков). Физические тома объединяются и образуют группы томов.

VG, Volume Group или группа томов. Это самый верхний уровень модели представления, которая используется в LVM. С одной стороны группа томов может состоять из физических томов, с другой – из логических томов и представлять собой единую структуру.

LV, Logical Volume или логический том. Раздел в группе томов, тоже самое, что раздел диска в не-LVM системе. Является блочным устройством и, как следствие, может содержать файловую систему.

PE, Physical Extent или физический экстент. Каждый физический том делится на блоки данных – физические экстенты. Они имеют размеры как и у логических экстентов.

LE, Logical Extent или логический экстент. Каждый логический том также делится на блоки данных – логические экстенты. Размеры логических экстентов не меняются в рамках группы томов.

Инициализация дисков и разделов

Перед тем, как начать использовать диск или раздел в качестве физического тома, важно его проинициализировать. Осуществляется это с помощью команды pvcreate. Данная команда создаст в начале диска или раздела дескриптор группы томов.

Для диска:

```
sit@sit:~$ sudo pvcreate /dev/sdb
[sudo] password for sit:
  Physical volume "/dev/sdb" successfully created
```

Для разделов:

```
sit@sit:~$ sudo pvcreate /dev/sdb1
[sudo] password for sit:
  Physical volume "/dev/sdb1" successfully created
```

Повторяем данную операцию для всех дисков или разделов которые необходимо пометить как физические тома LVM.

**В нашем случае это – sdb, sdc , sde, sdd, sdf.**

Если появилась ошибка инициализации диска с таблицей разделов, проверьте, что работаете с нужным диском. Убедившись в этом выполните следующие команды:

```
sudo dd if=/dev/zero of=/dev/sd* bs=1k count=1
sudo blockdev --rereadpt /dev/sd*
```

**Данные команды уничтожат существующую таблицу разделов на диске sd*.** Для разделов воспользуйтесь утилитой fdisk (parted или gdisk) и установите тип раздела в 0x8e (LVM).

Просмотреть диски (разделы) которые помечены как физические тома LVM можно с помощью команды **pvdisplay**.

```
sit@sit:~$ sudo pvdisplay
  --- Physical volume ---
  PV Name               /dev/sdb
  VG Name               storage
  PV Size               8.00 GiB / not usable 4.00 MiB
  Allocatable           yes
  PE Size               4.00 MiB
  Total PE              2047
  Free PE               2047
  Allocated PE          0
  PV UUID               dt4vrH-xpIo-IOAR-4sZD-Q9cT-St7Q-dRKInS

  --- Physical volume ---
  PV Name               /dev/sdc
  VG Name               storage
  PV Size               8.00 GiB / not usable 4.00 MiB
  Allocatable           yes
```

```
PE Size               4.00 MiB
Total PE              2047
Free PE               2047
Allocated PE          0
PV UUID               TD4x9x-t6dp-vrJ9-GnKk-eX1J-bU06-L17fnt

--- Physical volume ---
PV Name               /dev/sdd
VG Name               storage
PV Size               8.00 GiB / not usable 4.00 MiB
Allocatable           yes
PE Size               4.00 MiB
Total PE              2047
Free PE               2047
Allocated PE          0
PV UUID               qgJYg6-fNAu-9P2v-lBvt-u1H5-lfml-Pb186U

--- Physical volume ---
PV Name               /dev/sde
VG Name               storage
PV Size               8.00 GiB / not usable 4.00 MiB
Allocatable           yes
PE Size               4.00 MiB
Total PE              2047
Free PE               2047
Allocated PE          0
PV UUID               bKGRsE-ZNNV-XtqW-bXpn-yOI1-DMdC-8rANuv

--- Physical volume ---
PV Name               /dev/sdf
```

```
  VG Name               storage
  PV Size               8.00 GiB / not usable 4.00 MiB
  Allocatable           yes
  PE Size               4.00 MiB
  Total PE              2047
  Free PE               2047
  Allocated PE          0
  PV UUID               W6TBLw-3Yt6-ZJE2-lcOb-PMni-F95G-lxmyHW
```

Создание группы томов

Для создания группы томов необходимо воспользоваться командой vgcreate. На вход программы необходимо указать имя группы и диски (разделы) которые необходимо добавить в данную группу.

```
sit@sit:~$ sudo vgcreate storage /dev/sd[b-f]
  Volume group "storage" successfully created
```

Просмотреть группы томов в системе можно с помощью команды **vgdisplay**.

```
sit@sit:~$ sudo vgdisplay
  --- Volume group ---
  VG Name               storage
  System ID
  Format                lvm2
  Metadata Areas        5
  Metadata Sequence No  1
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                0
  Open LV               0
  Max PV                0
  Cur PV                5
```

```
Act PV              5
VG Size             39.98 GiB
PE Size             4.00 MiB
Total PE            10235
Alloc PE / Size     0 / 0
Free  PE / Size     10235 / 39.98 GiB
VG UUID             Nf04a2-sQ5O-zRfO-V3jc-wpTj-KjYx-aKpeCK
```

Удаление группы томов

Для удаления группы томов необходимо убедиться, что целевая группа томов не содержит логических томов. Далее необходимо деактивировать группу томов:

```
sudo vgchange -an storage
```

После чего удалить группу томов командой:

```
sudo vgremove storage
```

Для того, чтобы добавить ранее инициализированный физический том в существующую группу томов используется команда **vgextend**:

```
sudo vgextend storage /dev/sd*
```

Для того, чтобы удалить физический том из группы томов необходимо воспользоваться командой **vgreduce**:

```
sudo vgreduce storage /dev/sd*
```

Создание логического тома

Для того, чтобы например создать логический том «sit», размером 1800Мб, необходимо выполнить команду

```
sudo lvcreate -L1800 -n sit storage
```

Без указания суффикса размеру раздела, по умолчанию используется множитель M «мегабайт» (в системе СИ равный $10^6$ байт), что показано в примере выше. Суффиксы в верхнем регистре – KMGTPE соответствуют единицам в системе СИ с основанием 10. Например, G – гигабайт равен $10^9$ байт, а суффиксы в нижнем регистре – kmgtpe соответствуют единицам в системе IEC (с основанием 2), например g – гибибайт равен $2^{30}$ байт.

Для того, чтобы создать логический том размером 100 логических экстентов с записью по двум физическим томам и размером блока данных в 4 KB:

```
sudo lvcreate -i2 -I4 -l100 -n sit storage
```

Если необходимо создать логический том, который будет полностью занимать группу томов, то сперва используйте команду vgdisplay, чтобы узнать полный размер группы томов, а после этого выполните команду **lvcreate**.

```
sudo vgdisplay storage | grep "Total PE"
Total PE 10230
sudo lvcreate -l 10230 storage -n sit
```

Эти команды создают логический том sit, полностью заполняющий группу томов. Тоже самое можно реализовать командой:

```
lvcreate -l100%FREE storage -n sit
```

Удаление логических томов

Перед удалением логический том должен быть размонтирован:

```
sudo umount /dev/storage/sit
sudo lvremove /dev/storage/sit
lvremove -- do you really want to remove "/dev/storage/sit"? [y/n]: y
lvremove -- doing automatic backup of volume group "storage"
lvremove -- logical volume "/dev/storage/sit" successfully removed
```

Увеличение логических томов

Для того, чтобы увеличить логический том, необходимо указать команде lvextend размер, до которого будет увеличен том (в экстентах или в размере):

```
sudo lvextend -L15G /dev/storage/sit
    lvextend -- extending logical volume "/dev/storage/sit" to 15 GB
    lvextend -- doing automatic backup of volume group "storage"
    lvextend -- logical volume "/dev/storage/sit" successfully extended
```

В результате /dev/storage/sit увеличится до 15Гбайт.

Для изменения размера файловых систем ext2, ext3 и ext4 используйте **resize2fs**.

Создание снапшотов LVM

Для того, чтобы создать снапшот необходимо использовать **lvcreate -s**:

```
sudo lvcreate -s -L10GB -n backup /dev/storage/sit
```

Таким образом мы создадим снапшот в 10 GB с именем backup для хранения изменений.

Восстановление данных TestDisk

**TestDisk** – свободная программа для восстановления данных, предназначенная прежде всего для восстановления потерянных разделов на носителях информации, а также для восстановления загрузочного сектора, после программных или человеческих ошибок (например, потеря MBR).

- Установка <**sudo apt-get install testdisk**>.
- Запускаем TestDisk <**sudo testdisk**>.
- Появляется окошко приветствия TestDisk, нам предлагается вести лог работы (для выполнения данной работы лог не требуется).
- Выбираем нужный диск и нажимаем **Enter**.
- Предлагается выбрать тип таблицы разделов, обычно TestDisk определяет все правильно, так что нажимаем **Enter**.
- Выбираем **Analise**.
- Выбираем **QuickSearch**.
- Нам выводят таблицу разделов. Выбираем раздел и нажимаем **P**, чтобы вывести список файлов.
- Выбираем файлы для восстановления и нажимаем **C**.
- Выбираем папку, куда будут сохранены файлы и нажимаем **C**.

Восстановление данных PhotoRec

**PhotoRec** – это утилита, входящая в состав пакета TestDisk. Предназначена для восстановления испорченных файлов с карт памяти цифровых фотоаппаратов (CompactFlash, Secure Digital, SmartMedia, Memory

Stick, Microdrive, MMC), USB flash-дисков, жестких дисков и CD/DVD. Восстанавливает файлы большинства распространенных графических форматов, включая JPEG, аудио-файлы, включая MP3, файлы документов в форматах Microsoft Office, PDF и HTML, а также архивы, включая ZIP. Может работать с файловыми системами ext2, ext3, ext4 FAT, NTFS и HFS+, причем способна восстановить графические файлы даже в том случае, когда файловая система повреждена или отформатирована.

- Установка <**sudo apt-get install testdisk**>.
- Запускаем PhotoRec <**sudo photorec**>.
- Выбираем нужный диск и нажимаем **Enter**.
- В нижнем меню можно выбрать **File Opt**, чтобы выбрать типы файлов для восстановления (по умолчанию выбраны все).
- Чтобы начать восстановление нажмите **Enter**, выбрав **Search**.
- У нас выбрана система ext4, поэтому выбираем первый вариант [ ext2/ext3 ].
- Если выбрать пункт **FREE**, то поиск будет произведен в пустом пространстве и в этом случае будут восстановлены только удаленные файлы, а если выбрать **WHOLE**, то поиск будет произведен на всем диске.
- Теперь нужно указать директорию, куда будем сохранять нужные нам файлы. Выбираем нужную папку и нажимаем **C**.
- Выбираем файлы для восстановления и нажимаем **C**.

Восстановление данных Extundelete

**Extundelete** – утилита, позволяющая восстанавливать файлы, которые были удалены с разделов ext3/ext4.

- Установка: <**sudo apt-get install extundelete**>.
- Как только вы поняли, что удалили нужные файлы, необходимо отмонтировать раздел: <**umount /dev/<partition**> >.
- Зайдите в каталог, в который будут восстанавливаться удаленные данные. Он должен быть расположен на разделе отличном от того, на котором

хранились восстанавливаемые данные: **cd /<путь_к_каталогу_куда_восстанавливать_данные>**.

• Запустите **extundelete**, указав раздел, с которого будет происходить восстановление и файл, который необходимо восстановить: **sudo extundelete /dev/<partition> -restore-file /<путь к файлу>/<имя_файла>**.

• Можно так же восстанавливать содержимое каталогов: **sudo extundelete /dev/<partition> -restore-directory /<путь_к_директории>**.

Восстановление данных Foremost

Foremost - консольная программа, позволяющая искать файлы на дисках или их образах по hex-данным, характерным заголовкам и окончаниям. Программа проверяет файлы на предмет совпадения заранее определённых hex-кодов (сигнатур), соответствующих наиболее распространённым форматам файлов. После чего экстрагирует их из диска/образа и складывает в каталог, вместе с подробным отчётом о том, чего, сколько и откуда было восстановлено. Типы файлов, которые foremost может сразу восстановить: jpg, gif, png, bmp, avi, exe, mpg, wav, riff, wmv, mov, pdf, ole, doc, zip, rar, htm, cpp. Есть возможность добавлять свои форматы (в конфигурационном файле /etc/foremost.conf), о которых программа не знает.

• Установка: **<sudo apt-get install foremost>**.

• Пример использования для восстановления изображений с диска **/dev/sdb** в каталог **~/out_dir**: **<sudo foremost -t jpg,gif,png,bmp -i /dev/sdb -o ~/out_dir>**.

## Задания к лабораторной работе

Часть 1

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.

Часть 2

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 экстентов.

45. Расширить созданный логический том на размер добавленных экстентов.

46. Увеличить размер файловой системы.

47. Сделать снапшот логического тома.

48. Удалить группу томов и снапшот.

Часть 3

49. Добавьте в виртуальную машину виртуальный жесткий диск.

50. Запустите виртуальную машину с Linux.

51. Запустите fdisk (gdisk или parted) и создайте таблицу разделов MBR с разделами.

52. Отформатируйте созданные разделы в файловую систему ext4.

53. Установите TestDisk.

54. Удалите MBR (или таблицу разделов) с помощью команды DD.

55. Восстановите MBR (или таблицу разделов) с помощью TestDisk.

56. Смонтируйте восстановленные разделы и создайте там произвольные файлы.

57. Удалите созданные файлы.

58. С помощью TestDisk восстановите данные.

59. Создайте произвольный каталог и запишите туда данные каталога /var/log/ .

60. Удалите данные с созданного каталога.

61. С помощью PhotoRec восстановите данные.

62. Создайте произвольный каталог и запишите туда данные каталога /etc/ .

63. С помощью Extundelete или Foremost восстановите данные.

**Вопросы к лабораторной работе**

Часть 1

1. В чем достоинства и недостатки различных уровней RAID?

2. Что такое диск горячей замены RAID?

3. Как осуществить инициализацию физических дисков для использования их в качестве RAID массива?

4. Сколько минимально необходимо дисков для различных уровней RAID?

5. Сколько максимально может выйти из строя дисков в различных уровнях RAID массивов без потери данных?

6. Порядок действий для создания логического тома LVM.

7. Что такое Snapshot в LVM? Как его создать, и какое его функциональное назначение?

8. Что такое экстенты в LVM? Как создать логический том с определенным количеством экстентов?

9. Что такое логический том? Что такое физический том? В чем между ними отличие?

10. Как узнать количество экстентов в группе томов?

Часть 2

11. С помощью какой из программ, используемых в этой лабораторной работе, можно восстановить таблицу разделов?

12. Какие файловые системы поддерживает PhotoRec?

13. Какие форматы поддерживает PhotoRec?

14. Как Foremost восстанавливает файлы?

15. Можно ли восстановить данные с файловой системы NTFS, используя extundelete?

16. Все ли данные скопированные с каталога /var/log/ восстановились?

17. Все ли данные скопированные с каталога /etc/ восстановились?