УТВЕРЖДЕН

ЦАУВ.14001-01 91 01-ЛУ

Клиентская операционная система с интегрированными пользовательскими приложениями МСВСфера 6.3 АРМ

Руководство администратора ЦАУВ.14001-01 91 01

Дополнение № 1

Версия 1.1

2017

Изм.	Лист	№ докум	Подп	Дата

СОДЕРЖАНИЕ

Изм.	Лист	№ докум	Подп	Дата

1 РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

1.1 Основные сведения

Средства резервного копирования и восстановления МСВСфера 6.3 АРМ предоставляют следующие возможности:

- использование отказоустойчивых технических средств;
- резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы;
- контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование;
- периодическое резервное копирование информации на резервные машинные носители информации;
- обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий);
- контроль состояния и качества вычислительных ресурсов (мощностей), в том числе по передаче информации.

Возможности резервного копирования и восстановления реализуются с помощью следующих программных компонент:

- утилита tar;
- утилита cpio;
- система резервного копирования AMANDA;
- приложение "FirstAidKit";
- приложение "Менеджер архивов".

1.2 Утилита tar

Утилита tar предназначена для создания архивов файлов и каталогов. С помощью этой программы можно архивировать файлы, обновлять их в архиве и вводить в этот архив новые файлы. Можно архивировать и целые каталоги со всеми их файлами и подкаталогами. При необходимости все эти файлы и подкаталоги можно восстановить из архива. Архив можно создавать на любом устройстве, например на внешнем носителе или в архивном файле на диске.

Программа tar - идеальное средство для создания резервных копий файлов или объединения нескольких файлов в один с целью передачи его по сети.

Чтобы использовать программу tar для создания архивов на внешних устройствах и в файлах, необходимо указать опции "cf" с именем устройства или файла, которые часто называют именем архива. При создании файла для tar-архива к имени этого файла обычно добавляется расширение ".tar". Если указано имя каталога, то в архив включаются и все подкаталоги этого каталога. В следующем примере каталог mydir и все его подкаталоги сохраняются в файле myarch.tar.

tar cf myarch.tar mydir

Пользователь может извлекать каталоги из архива, применяя команду tar с опцией "x". Опция "xf" позволяет извлекать файлы из архивного файла или устройства. При извлечении формируются и все подкаталоги. В следующем примере посредством опции "xf" команде tar дается указание извлечь все файлы и подкаталоги из файла myarch.tar.

tar xf myarch.tar

Для добавления файлов в существующий архив служит опция "r". В приведенном ниже примере пользователь добавляет файлы из каталога letters в архив myarch.tar.

tar rf myarch.tar letters

Если нужно изменить какой-либо файл в архивированных ранее каталогах, можно с помощью опции "u" дать команде указание обновить архив, заменив некоторые файлы их новыми версиями. Программа tar сравнивает время последнего изменения каждого архивированного файла и соответствующего файла в каталоге и копирует в архив все файлы с более поздней датой модификации. В архив будут добавлены и все вновь созданные в этих каталогах файлы. В следующем примере пользователь обновляет файл myarch.tar, вводя в него все измененные и вновь созданные в каталоге mydir файлы.

tar uf myarch.tar mydir

Если вы хотите посмотреть, какие файлы хранятся в архиве, задайте команде tar опцию "t". В следующем примере показано, как с помощью этой команды можно вызвать список всех файлов, хранящихся в архиве myarch.tar.

tar tf myarch.tar

Для создания резервных копий файлов на определенном устройстве укажите имя этого устройства в качестве имени архива. В следующем примере создается архив на устройстве /dev/fd0 и копируются в него все файлы из каталога mydir.

tar cf /dev/tdO mydir

Для того, чтобы извлечь архивированные таким образом файлы, используйте опцию "xf".

tar xf /dev/fd0

Посредством опции "M" команде tar дается указание выводить сообщение о том, что текущий носитель заполнен. При архивировании файлов на дискете с использованием опции "M" в случае заполнения носителя программа tar предложит вам вставить новый носитель.

tar cMf /dev/fd0 mydir

Чтобы распаковать архив, записанный на нескольких носителях, вставьте первый и введите команду tar с опциями "x" и "M", как показано ниже. Программа подскажет вам, когда надо вставить следующий носитель.

tar xMf /dev/fd0

При использовании команды tar операция сжатия архивных файлов не выполняется. Если команда tar применяется с опцией "z", то сначала программа gzip выполняет сжатие, а затем tar архивирует файлы. Та же опция "z" обеспечит вызов gzip для распаковки файлов при извлечении их из архива.

tar czf myarch.tar mydir

Между сжатием отдельных файлов с последующим архивированием и сжатием всего архива есть разница. Во многих случаях архив создается, чтобы переслать по сети несколько файлов в виде одного tar-файла. Для сокращения времени передачи размер этого архива должен быть по возможности небольшим. Чтобы добиться этого, можно с помощью утилиты gzip сжать архивный tar-файл, уменьшив его размер, а затем переслать сжатую версию. Получатель распакует его и восстановит файл. В результате применения утилиты gzip к tar -файлам часто получаются файлы с расширением .tar.gz. Расширение .gz добавляется к сжатому gzip-файлу. В следующем примере создается сжатая версия файла myarch.tar под тем же именем, но с расширением .gz.

gzip myarch.tar

1.3 Утилита cpio

Утилита cpio (Copy Input/Outup) занимается копированием входящих файлов в выходящий архив и наоборот, развёртыванием входящего архива в выходящие файлы.

Администраторам утилита будет полезна как средство резервного копирования. При этом cpio необходимо использовать в сочетании с утилитой find.

Создадим резервную копию каталога /lib и запишем его на флеш-носитель. На рис.1 видно, что флеш-носитель смонтирован как устройство /mnt командой mount /dev/sdb4 /mnt. Командой find /lib/ | cpio -o > /mnt/2/backup.cpio создается резервная копия.

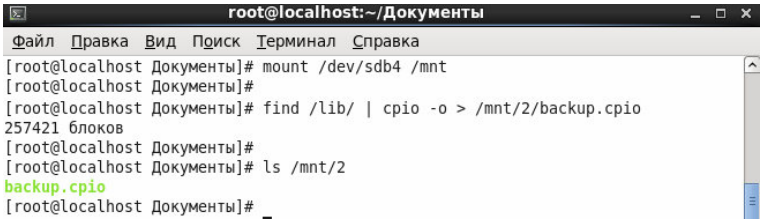


Рисунок 1 - Создание резервной копии с помощью утилиты cpio

Для того, чтобы восстановить все файлы в каталог /lib из созданной ранее копии, сохраняя время модификации и создания каталогов, необходимо выполнить команду cpio -ivmd /lib/* < /mnt/2/backup.cpio, как на рис.2. Извлеченные файлы копируются в указанную папку. Права доступа к файлам будут такими же, как и в момент выполнения соответствующей команды cpio -o. Пользователь и группа-владелец устанавливается на основе текущего пользователя, если только это не пользователь root. В этом случае владельцы будут такие же, как были при выполнении соответствующей команды cpio -o. Если команда cpio -i пытается создать файл, который уже существует, причем с той же датой изменения или более новый, выдается предупреждающее сообщение и cpio не заменит этот файл. Для безусловной перезаписи существующих файлов можно задать опцию "-u".

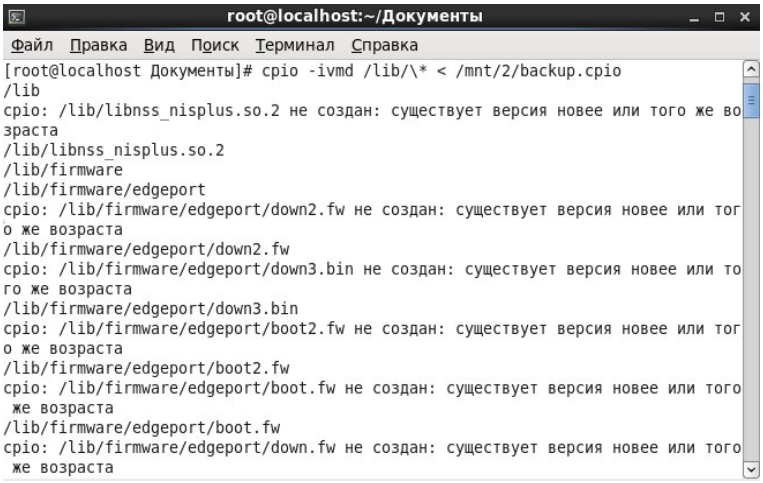


Рисунок 2 - Восстановление файлов из резервной копии

Для получения более подробной информации о возможностях find и cpio выполните команды man find и man cpio соответственно.

1.4 Система резервного копирования AMANDA

AMANDA ("Advanced Maryland Automatic Network Disk Archiver") - это система, предназначенная для архивирования информации и обладающая возможностью резервного копирования данных, постоянно хранящихся на множестве компьютеров в компьютерной сети. AMANDA использует клиент-серверную модель, включающую следующие компоненты:

- сервер резервного копирования и клиент для него;
- сервер лент;
- индексирующий сервер.

Система AMANDA включает в себя следующие программы и утилиты:

- Среди клиентских программ центральной является утилита amandad. Она взаимодействует с сервером системы AMANDA во время выполнения резервного копирования и вызывает по указанию сервера другие программы:
  - selfcheck — проверка конфигурации клиента;
  - sendsize — оценка объема резервной копии;
  - sendbackup — выполнение операции резервного копирования;
  - amcheck — проверка конфигурации AMANDA.
- Серверные программы используются в различных фазах резервного копирования. Главной программой является amdump, которая инициирует все операции резервного копирования, как правило, вызывается в cron, и контролирует выполнение других программ:
  - planner — опередилить, что копировать;
  - driver — интерфейс к внешнему устройству;
  - dumper — связывается с клиентским процессом amandad;
  - taper — запись данных на внешнее устройство;
  - amreport — подготовка сообщения о выполненном копировании.
- Административные программы:
  - amcheck — проверка системы AMANDA, чтобы убедиться, что система готова к работе;
  - amlabel — записать метку на сменный носитель перед использованием в системе AMANDA;
  - amcleanup — очистить систему AMANDA после системной аварии (не плановой перезагрузке сервера) или после не планового завершения операции резервного копирования;

- amflush — переписать данные из дискового кэша на внешний носитель;
- amadmin — выполнение большого количества различных административных операций.

- Конфигурационные файлы amanda.conf, disklist.
- Программы (утилиты) восстановления данных:
  - amrestore — программа, которая может быть использована для восстановления данных с носителей, на которых записаны резервные копии, выполненные системой AMANDA;
  - amrecover — программа для интерактивного восстановления данных с резервных копий; в своей работе эта утилита использует демоны amindex и amidxtaped.

Настройка AMANDA

Для корректной работы системы AMANDA необходимо знать IP адреса сервера и клиента.

Первоначально необходимо настроить сервер. Для этого нужно переключиться под пользователя amandabackup командой в терминале su - amandabackup и в каталоге /etc/amanda создать папку конфигурации "DailySet1", перейти в нее:

mkdir etc/amanda/DailySet1

cd DailySet1

В этой папке необходимо создать основной конфигурационный файл amanda.conf командой:

touch etc/amanda/DailySet1/amanda.conf

Далее необходимо настроить этот файл. Пример содержимого файла amanda.conf:

org "Test backup" *# заголовок*

mailto "admin@localhost" *# адрес для отправки отчета, после окончания дампа*

dumpcycle 4 days *# длина цикла резервного копирования*

tapecycle 4 *# число лент*

runtapes 1

tpchanger "chg-multi" *# директории на жестком диске*

changerfile "/etc/amanda/DailySet1/changer.conf"

logdir "/var/log/amanda/DailySet1"

indexdir "/etc/amanda/DailySet1/index"

infofile "/etc/amanda/DailySet1/curinfo"

```
amrecover_changer "chg-multi"
tapetype HARD-DISK
labelstr "^DailySet1[0-9][0-9]*$"
# по этой записи Amanda будет отличать «правильные» ленты от всех прочих
define tapetype HARD-DISK {
  comment "Hard disk instead of tape"
  length 20000 mbytes
}
 define dumptype global {
  comment "Global definitions"
  index yes
  record yes
}
define dumptype hard-disk-dump {
  global
  comment "Back up to hard disk instead of tape - using dump"
  holdingdisk no
  index yes
  priority high
}
define dumptype hard-disk-tar {
        hard-disk-dump
      comment "Back up to hard disk instead of tape - using tar"
      program "GNUTAR"
}
define interface local {
        comment "a local disk"
      use 1000 kbps
}
define interface eth0 {
  comment "100 Mbps ethernet"
  use 90 Mbps
}
```

После настройки конфигурационного файла нужно создать файл disklist, в котором будут перечислены все клиенты, для которых предназначено резервное копирование.

Содержимое файла можно представить следующим образом:

192.168.10.156 /tmp/second hard-disk-tar

Строка включает в себя три элемента. Первый ("192.168.10.156") задает ip-адрес, с которого будет сделана резервная копия, второй элемент ("/tmp/second") указывает путь к директории, из которой будут браться данные для резервного копирования, третий ("hard-disk-tar") – метод, описанный в файле amanda.conf.

Далее нужно создать директорию /var/log/amanda/DailySet1 командой в консоли:

mkdir /var/log/amanda/DailySet1

И заменить ее владельца на amandabackup командой:

chown amandabackup:disk /var/log/amanda/DailySet1

Все действия в AMANDA должны производиться от пользователя amandabackup, для того, чтобы зайти под ним, в терминале выполните команду:

su - amandabackup

Следующим шагом нужно создать папку, где будут храниться резервные копии, например, amanda/dump. В ней нужно создать папки с названиями ленточных накопителей "tape1", "tape2", "tape3", "tape4", и в каждой папке - папку "data".

Далее необходимо произвести маркировку лент, которые потребуются при восстановлении данных из резервной копии. Для этого выполняем следующие команды в консоли:

amlabel DailySet1 DailySet101 slot 1

amlabel DailySet1 DailySet102 slot 2

amlabel DailySet1 DailySet103 slot 3

amlabel DailySet1 DailySet104 slot 4

После маркировки лент нужно создать файл ".amandahosts" в папке /var/lib/amanda, который позволит ip-адресам получить доступ к ресурсам.

Содержимое файла ".amandahosts" может выглядеть следующим образом:

::ffff:192.168.10.156 root amindexd amidxtaped

::ffff:192.168.10.156 amandabackup amindexd amandabackup amdump

::ffff:192.168.10.156 amandabackup amindexd amidxtaped amrestore

localhost amandabackup

localhost.localdomain amandabackup

localhost root

localhost.localdomain root

Необходимо изменить имя владельца файла на amandabackup и изменить права доступа к файлу на 600 (чтение и запись файла только владельцем этого файла):

chmod 600 /var/lib/amanda/.amandahosts

Для корректной работы файла "amanda.conf" необходимо откорректировать флаг "disables" в файле /etc/xinetd.d/amanda, а именно значение флага disables изменить с "yes" на "no".

Пример содержимого файла /etc/xinetd.d/amanda:

```
service amanda
{
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = amandabackup
        group                   = disk
        server                  = /usr/sbin/amandad
        server_args             = -auth=bsd amdump amindexd amidxtaped
        disable                 = no
}
```

После произведенных изменений нужно перезапустить службу xinetd:

service xinetd restart

И создать в папке /etc/amanda/ файл "changer.conf", в котором описывается смена магнитных накопителей.

Пример содержимого файла /etc/amanda/changer.conf:

```
multieject 0
gravity 0
needeject 0
ejectdelay 0
statefile /var/lib/amanda/DailySet1/changer-status
firstslot 1
lastslot 4
slot 1 file:/amanda/dumps/tape01
```

slot 2 file:/amanda/dumps/tape02

slot 3 file:/amanda/dumps/tape03

slot 4 file:/amanda/dumps/tape04

Для настройки клиента, также как при настройке сервера, необходимо создать папку конфигурации /etc/amanda/DailySet1 с конфигурационным файлом amanda-client.conf.

Пример содержимого файла amanda-client.conf:

conf "DailySet1" *# имя конфигурации*

index_server "192.168.10.157" *# amindexd сервер*

tape_server "192.168.10.157" *# amidxtaped сервер*

auth "bsd"

unreserved-tcp-port 1025,65535

Для корректной работы файла amanda-client.conf необходимо заменить значение флага "disables" в файле /etc/xinetd.d/amanda с "yes" на "no".

Пример содержимого файла /etc/xinetd.d/amanda:

```
service amanda
{
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = amandabackup
        group                   = disk
        server                  = /usr/sbin/amandad
        server_args             = -auth=bsd amdump amindexd amidxtaped
        disable                 = no
}
```

После произведенных изменений нужно перезапустить службу:

service xinetd restart

После чего необходимо создать на клиенте файл ".amandahosts" в папке /var/lib/amanda, который позволит ip-адресам получить доступ к ресурсам.

Содержимое файла ".amandahosts" может выглядеть следующим образом:

::ffff:192.168.10.157 root amindexd amidxtaped

::ffff:192.168.10.157 amandabackup amindexd amandabackup amdump

::ffff:192.168.10.157 amandabackup amindexd amidxtaped amrestore

localhost amandabackup amdump

localhost root amindexd amidxtaped

localhost amanda

localhost.localdomain amanda

localhost amandabackup

localhost.localdomain amandabackup

localhost root

localhost.localdomain root

Необходимо изменить имя владельца файла на amandabackup и изменить права доступа к файлу на 600 (чтение и запись файла только владельцем этого файла):

chmod 600 /var/lib/amanda/.amandahosts

Для непосредственно резервного копирования необходимо выполнить команду в консоли на сервере от пользователя amandabackup:

amdump DailySet1

Проверку на сервере можно выполнить от пользователя amandabackup следующей командой:

/usr/sbin/amcheck DailySet1

Восстановление производится на клиенте от пользователя с правами root (рис. 3) командами:

amrecover DailySet1

sethost 192.168.10.156

setdisk /tmp/second

add *

list

extract

quit

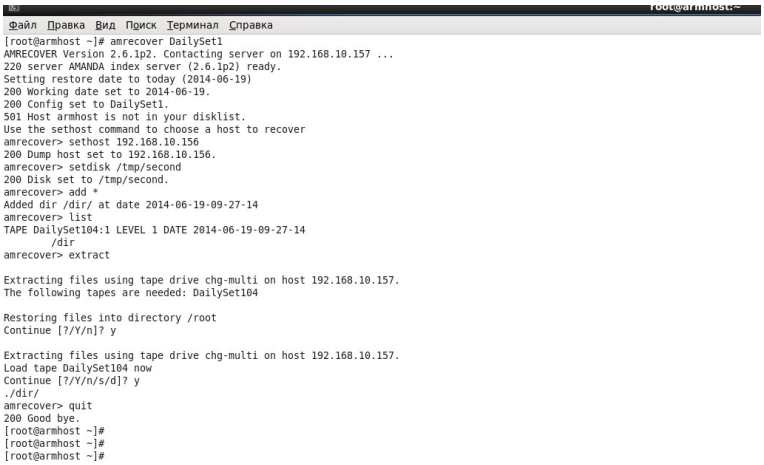


Рисунок 3 - Восстановление данных

В файле amanda.conf был указан email, на который AMANDA по завершению резервного копирования присылает сообщение (рис. 4).

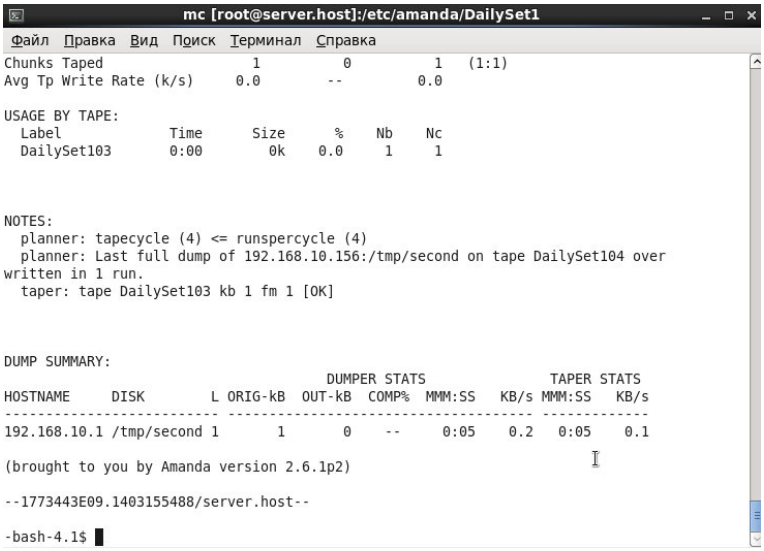


Рисунок 4 - Сообщение об удачном завершении резервного копирования

1.5 Приложение "FirstAidKit"

Приложение «Firstaidkit» предназначено для автоматизации процесса восстановления системы и вызывается из меню «Приложения->Системные->Firstaidkit». Приложение представляет интерактивное окружение для диагностики и восстановления неверно загружаемых систем.

Открывшееся окно состоит из двух вкладок: «Select task» (Выбор задачи) (рис.5) и «Result» (Результат). Для начала нужно выбрать задачу и для ее выполнения нажать кнопку «Start» (Старт). В окне так же можно установить следующие параметры:

–«Run interactive mode» – запустить в интерактивном режиме;

–«Be verbose in output» – запуск подробного режима выполнения;

–«Use experimental features» – использовать экспериментальные функции;

–«Do not use dependency mechanisms» – не использовать механизмы с зависимостями.

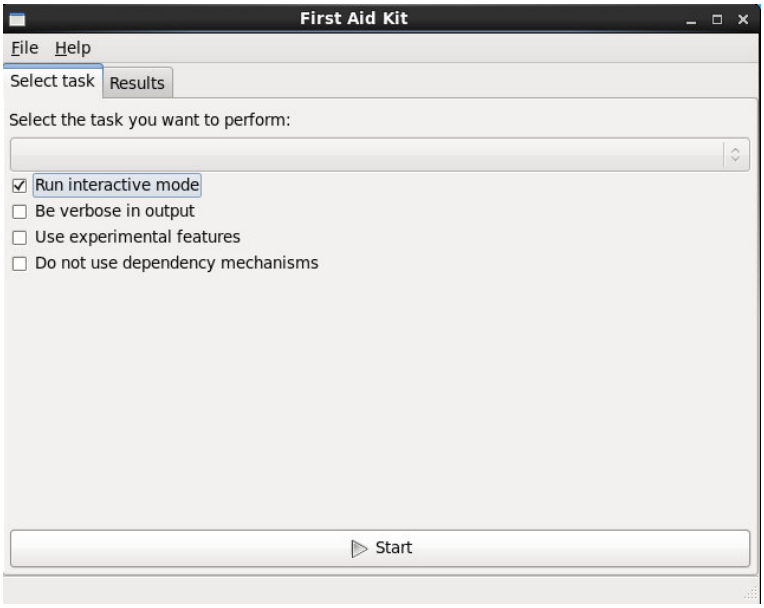


Рисунок 5 – Выбор задачи

Результат выполнения задачи можно просмотреть на вкладке «Result» в колонках "Name" (наименование), "Status" (статус), "Description" (описание). Для сохранения результата необходимо нажать кнопку "Save results", для сброса – "Reset", для остановки работы задачи – "Stop" (рис. 6).

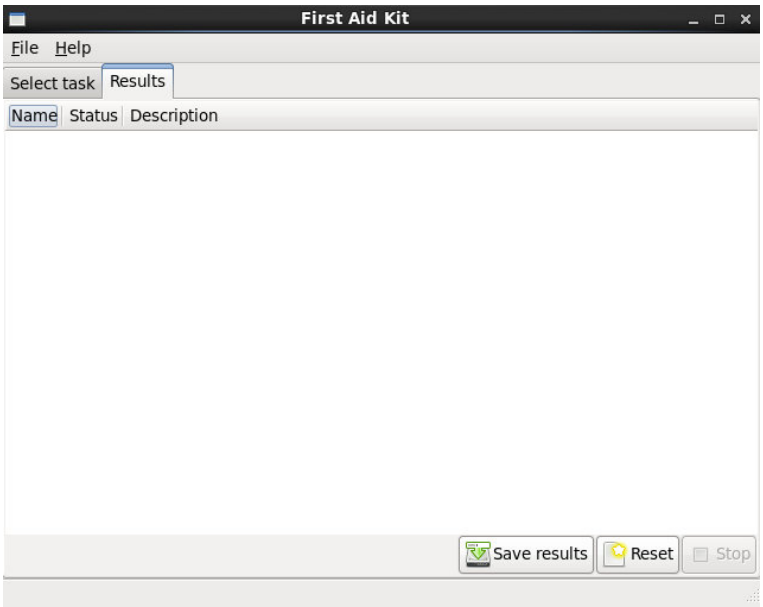


Рисунок 6 – Результат выполнения задачи

Опции команды "firstaidkit":

-c <cjnfig file> - расположение файла конфигурации;

-r <root path> - расположение корневого каталога;

-P <path> - добавить другой путь для плагин;

-v - подробный режим;

-l <method> - выбрать другой способ журналирования;

-x <piugin> - исключить плагин из серии;

-F <flag> - набор загрузочных флагов;

-g <gui> - внешний интерфейс для отображения результатов;

-g console – запуск внешнего интерфейса;

-g rtk – запуск внешнего интерфейса с использованием rtk;

-h - вызов справки;

--print-config – вывод результирующего файла;

--flags – список всех известных флагов;

--list – список всех плагинов;

--info <plugin> - получить информацию о плагине;

--nodeps – не использовать зависимый плагин;

--plugin-args=<plugin_name[/flow] args> - дополнительно передавать аргументы plugin_name.

1.6 Приложение "Менеджер архивов"

Для резервного копирования и восстановления данных полезно иметь под рукой приложение, которое бы позволяло сжимать несколько файлов в один, чтобы они занимали меньше дискового пространства. В системе МСВСфера 6.3 АРМ для создания, просмотра, изменения или распаковки архива используется приложение "Менеджер архивов" (рис. 7), которое вызывается из меню "Приложения->Стандартные->Менеджер архивов".

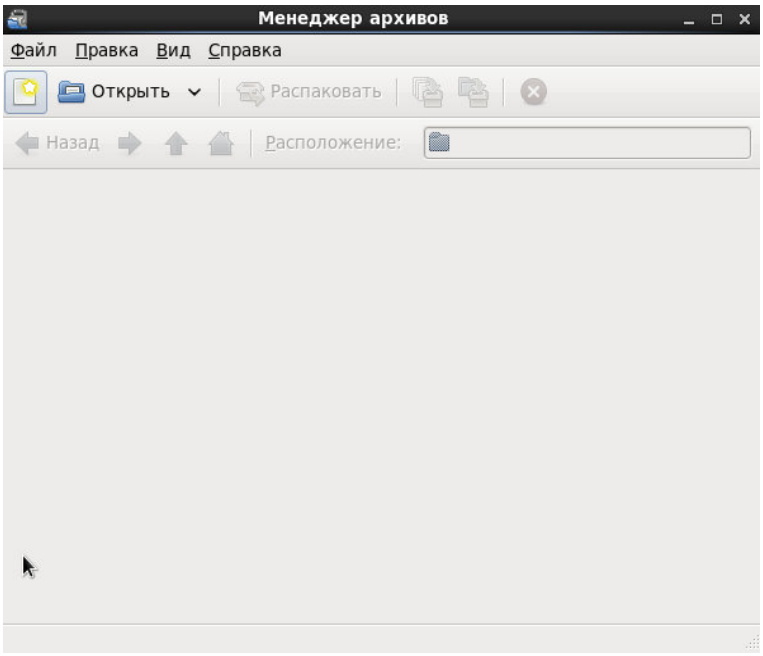
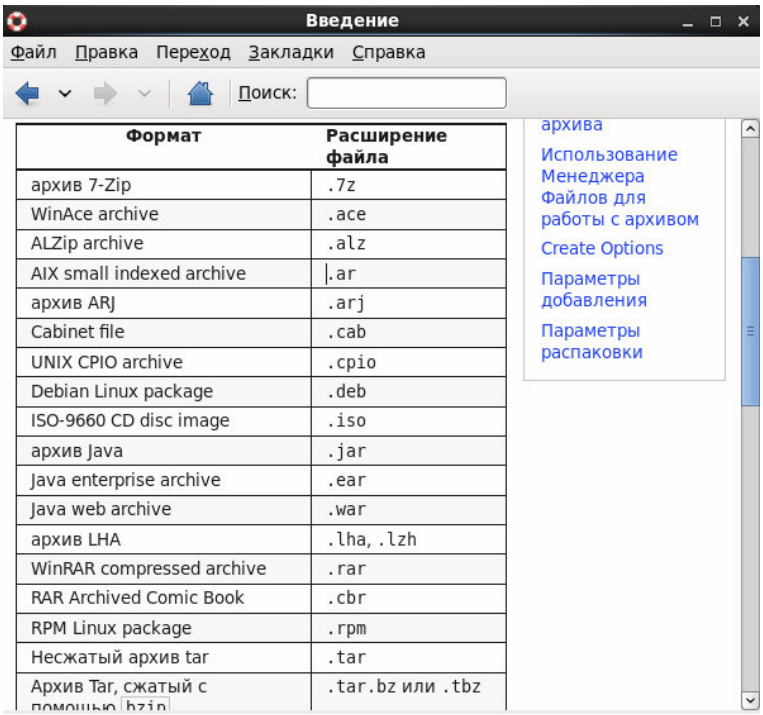


Рисунок 7 - Приложение "Менеджер архивов"

Вызвав справку в приложение с помощью пункта меню "Справка->Содержимое", в главе "Введение" можно прочитать какие виды архивов поддерживает приложение (рис. 8).



Формат	Расширение файла
архив 7-Zip	.7z
WinAce archive	.ace
ALZip archive	.alz
AIX small indexed archive	.ar
архив ARJ	.arj
Cabinet file	.cab
UNIX CPIO archive	.cpio
Debian Linux package	.deb
ISO-9660 CD disc image	.iso
архив Java	.jar
Java enterprise archive	.ear
Java web archive	.war
архив LHA	.lha, .lzh
WinRAR compressed archive	.rar
RAR Archived Comic Book	.cbr
RPM Linux package	.rpm
Несжатый архив tar	.tar
Архив Tar, сжатый с помощью bzip	.tar.bz или .tbz

Рисунок 8 - Таблица поддерживаемых форматов архивов

Для разархивирования или декомпрессии файла необходимо нажать на кнопку "Открыть" на панели инструментов, в появившемся окне выбрать нужный архивный файл. Архив откроется в окне просмотра, как на рис. 9.

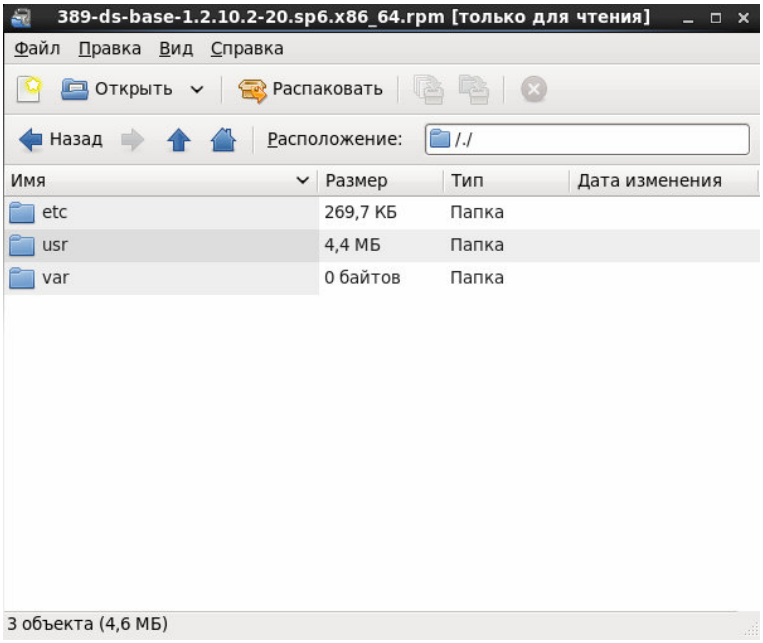


Рисунок 9 - Окно просмотра приложения "Менеджер архивов"

Приложение "Менеджер архивов" сохраняет структуру каталогов и подкаталогов. Чтобы получить отдельный файл или архив полностью, необходимо нажать на кнопку "Распаковать" на панели инструментов, а затем выбрать каталог, в который будут сохранены разархивированные файлы и нажать на кнопку "Распаковать".

Чтобы создать архив необходимо нажать на кнопку "Создать новый архив" на панели инструментов, в результате чего появится окно, в котором нужно указать имя и тип архива (рис. 10). В области "Дополнительные параметры" так же можно указать пароль для шифрования файлов и разделить архив на тома указанных размеров, после чего нужно нажать на кнопку "Создать".

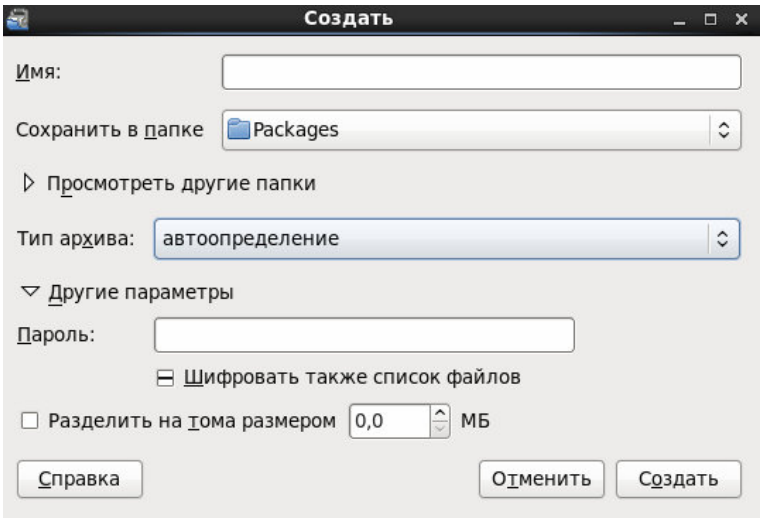


Рисунок 10 - Окно создания нового архива

В открывшемся окне можно добавить файлы и папки в архив, нажав соответственно на кнопку "Добавить в архив новые файлы и папки" или "Добавить папку в архив" на панели инструментов. При этом откроется окно (рис. 11), в котором нужно выбрать файлы и каталоги для архивирования, нажав на кнопку "Добавить". После чего можно закрыть архив, выбрав пункт меню "Файл-> Закрыть".

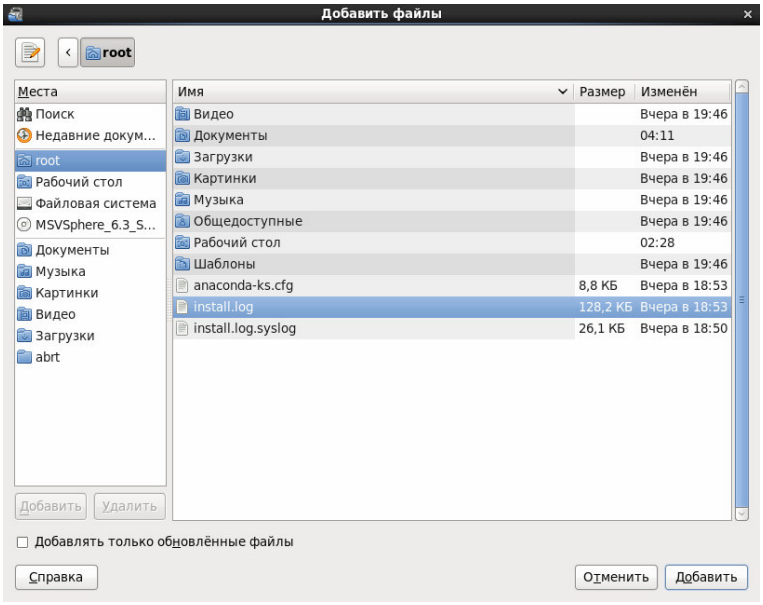


Рисунок 11 - Выбор файлов и папок для добавления в архив

Чтобы переконвертировать архив в другой формат, нужно его открыть и выбрать пункт меню "Файл-> Сохранить как". В открывшемся окне (рис. 12) необходимо выбрать тип архива, в который нужно переконвертировать текущий архив. Можно указать другое имя, после чего нужно нажать кнопку "Создать".

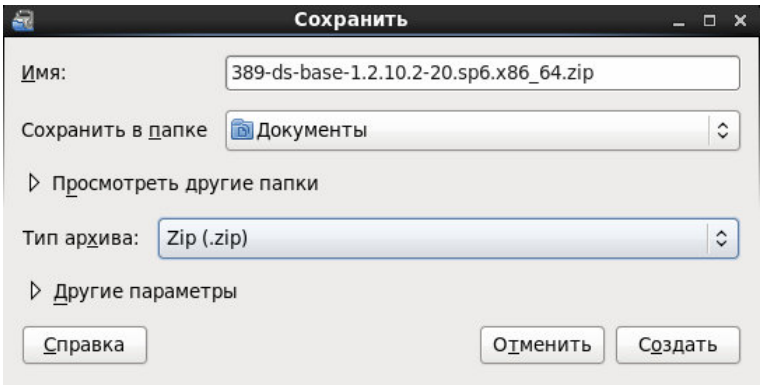


Рисунок 12 - Переконвертация архива

2 НАСТРОЙКА И ОГРАНИЧЕНИЕ ПРОГРАММНОЙ СРЕДЫ

2.1 Основные сведения

Средства настройки и ограничения программной среды МСВСфера 6.3 АРМ предоставляют следующие возможности:

- управление запуском компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения;
- управление установкой компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения;
- установка только разрешенного к использованию программного обеспечения и (или) его компонентов;
- управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов.

Вышеперечисленные возможности настройки и ограничения программной среды реализуются с помощью следующих приложений:

- приложение "Запускаемые приложения";
- приложение "Предпочтительные приложения";
- приложение "Настройка служб";
- приложение "Установка и удаление программ".

2.2 Приложение "Запускаемые приложения"

Для настройки автоматически запускаемых компонент системы в МСВСфера 6.3 АРМ включена программа "Запускаемые приложения" (рис. 13), которая запускается из меню "Система->Параметры->Запускаемые приложения". На вкладке "Автоматически запускаемые программы" указаны программные компоненты, дополнительно запускаемые при старте системы.

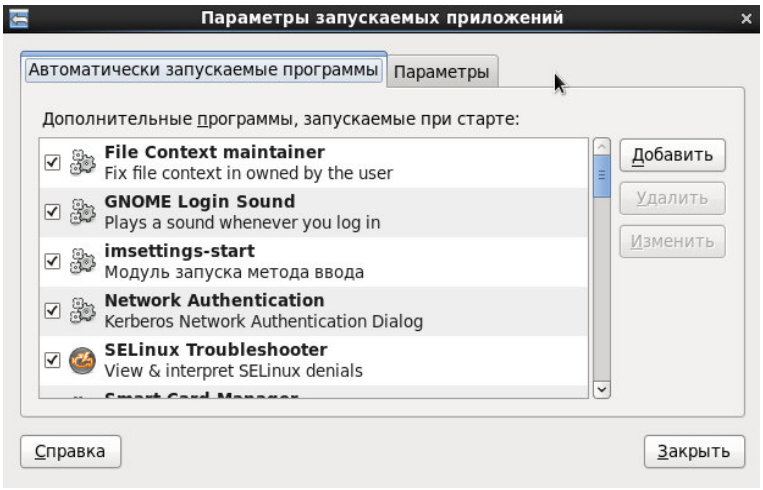


Рисунок 13 - Настройка параметров запускаемых приложений

Чтобы добавить программу, которая будет запускаться при старте, если ее еще нет в списке автоматически запускаемых программ, нужно нажать кнопку "Добавить" и в открывшемся диалоговом окне ввести название программы, команду, с помощью которой запускается программа, и комментарий в соответствующих полях (рис. 14).

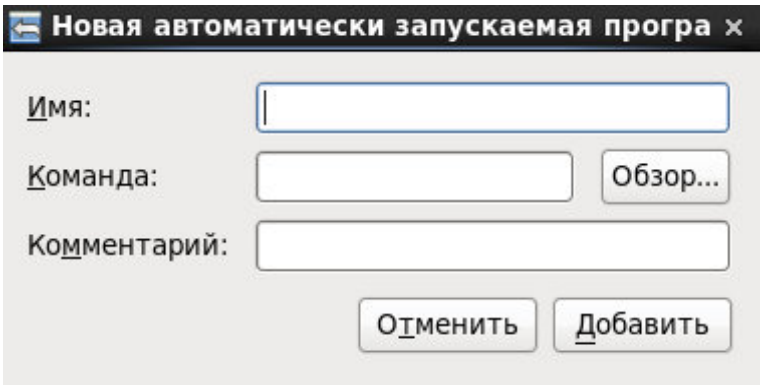


Рисунок 14 - Добавление автоматически запускаемых компонентов программ

Для изменения настроек запуска программы нужно нажать кнопку "Изменить", в открывшемся окне (рис. 15) заменить необходимые поля: "Имя", "Команда" или "Комментарий".

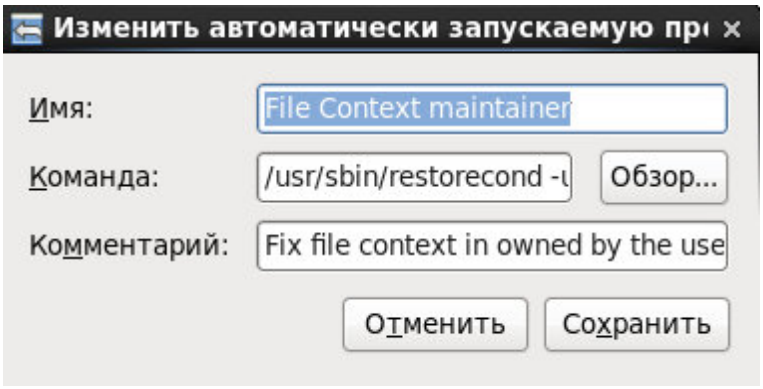


Рисунок 15 - Изменение параметров автоматически запускаемых программ

На вкладке "Параметры" можно задать автозапуск запущенных на данный момент приложений при старте системы с помощью кнопки "Запомнить запущенные приложения" или установить галочку на "Автоматически запоминать запущенные приложения при выходе из сеанса" (рис. 16), если вы хотите продолжать каждый раз незаконченную рабочую сессию. После установки нужных параметров - нажать кнопку "Закрыть".

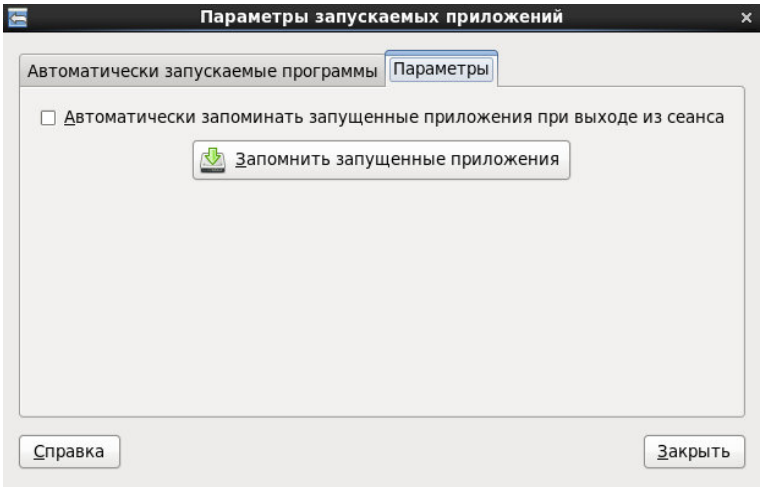


Рисунок 16 - Параметры автозапуска

2.3 Приложение "Предпочтительные приложения"

Для выбора приложений-обработчиков по умолчанию в системе МСВСфера 6.3 АРМ используется приложение "Предпочтительные приложения" (рис. 17), которое вызывается из меню "Система->Параметры->Предпочтительные приложения".

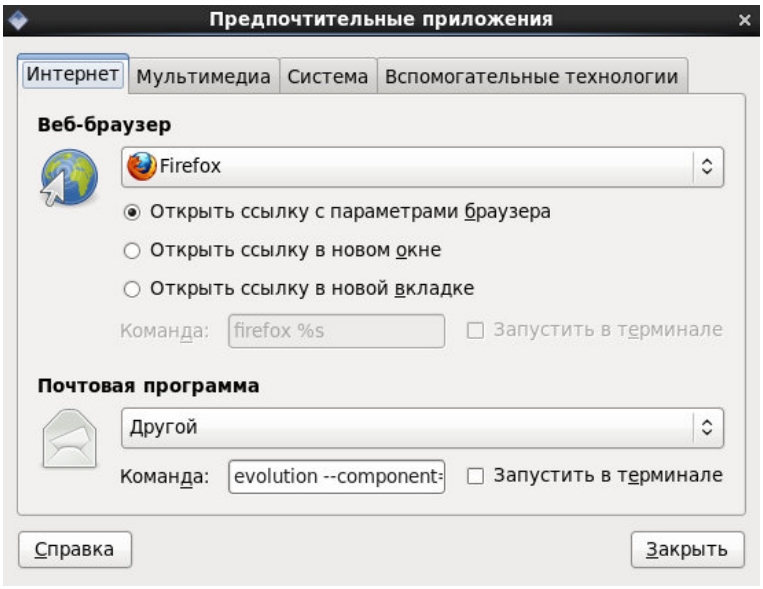


Рисунок 17 - Вкладка "Интернет"

На вкладке "Интернет" можно выбрать приложения для обработки web-страниц, такие как Firefox и Konqueror, и для работы с электронной почтой, такие как KMail и Mutt. Если необходимо указать дополнительные флаги при запуске приложения, их можно задать в поле "Команда".

Для работы с мультимедиа используется одноименная вкладка, где можно выбрать проигрыватель по умолчанию (рис. 18). Это могут быть Totem, Rhythmbox или другие.

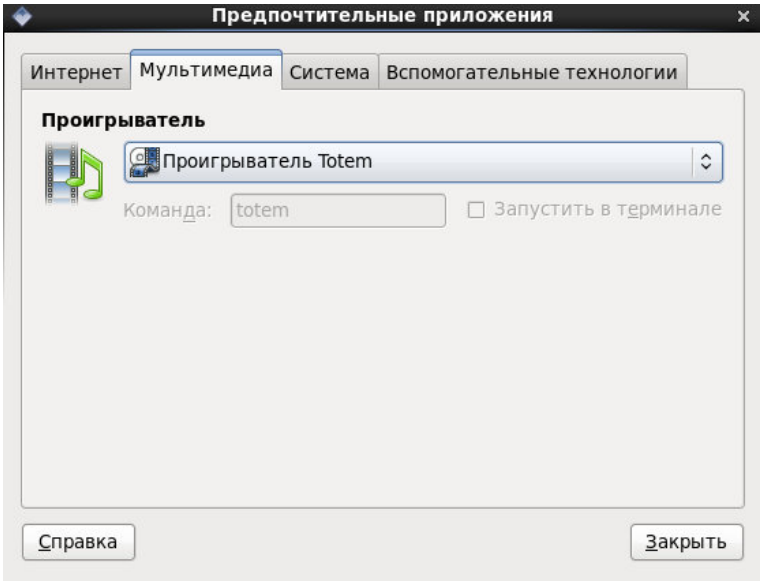


Рисунок 18 - Вкладка "Мультимедиа"

Изм.	Лист	№ докум	Подп	Дата

На вкладке "Система" определяется программа - эмулятор терминала (рис. 19), например, терминал GNOME, KDE Konsole, стандартный X-терминал или Konsole.

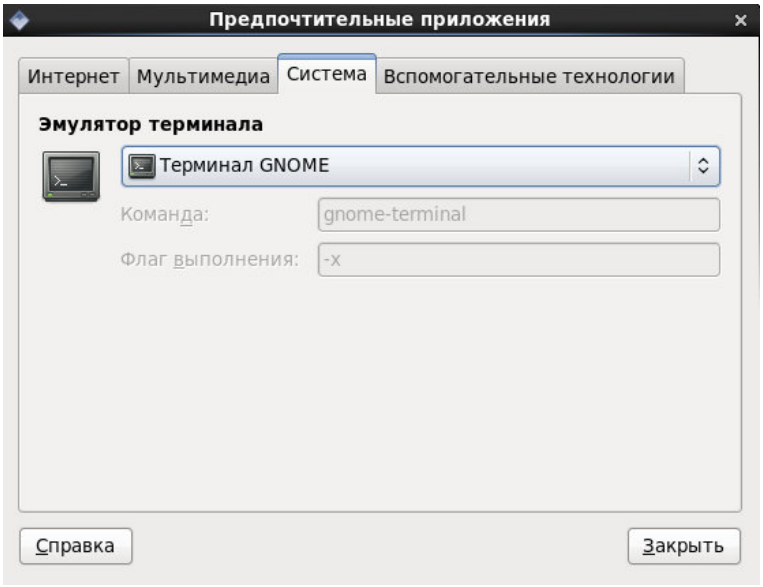


Рисунок 19 - Вкладка "Система"

На вкладке "Вспомогательные технологии" (рис. 20) можно выбрать программу работы с экраном, такую как Orca, Orca с увеличителем экрана, увеличитель GNOME без чтения с экрана или увеличитель KDE без чтения с экрана, и программу мобильности, такую как экранный увеличитель GNOME, а так же запускать эти программы по умолчанию при входе.

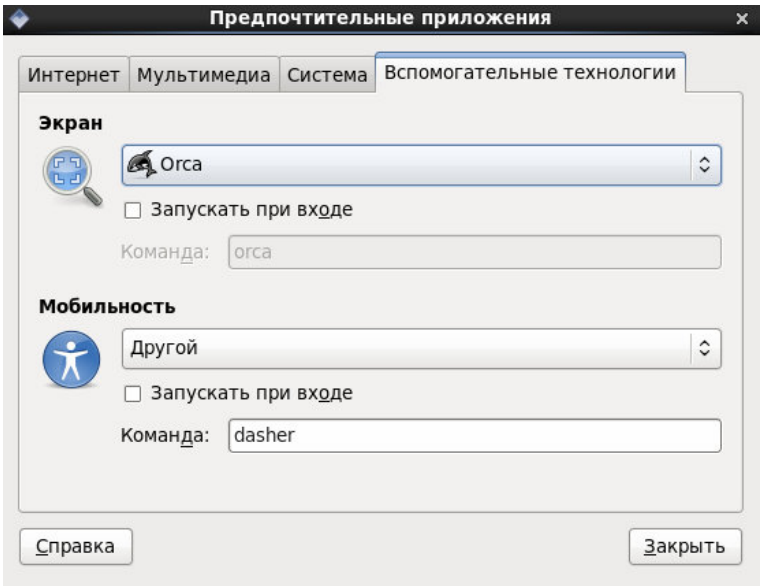


Рисунок 20 - Вкладка "Вспомогательные технологии"

2.4 Приложение "Настройка служб"

Настройка доступа к службам в системе МСВСфера 6.3 АРМ осуществляется с помощью приложения "Настройка служб" (рис. 21), которое вызывается из меню "Система->Администрирование->Службы".

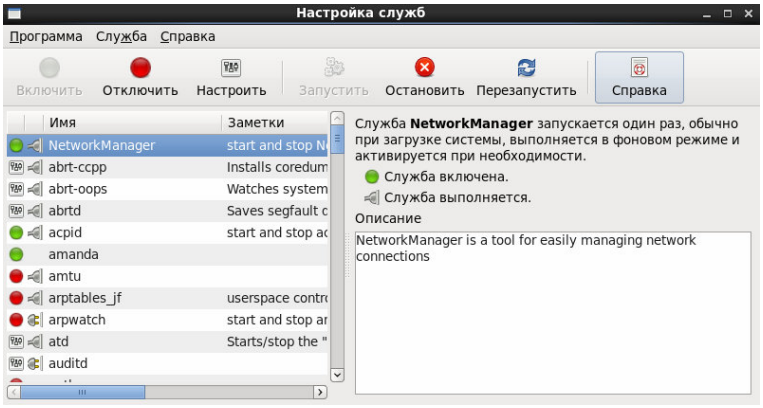


Рисунок 21 - Окно приложения "Службы"

Приложение "Настройка служб" показывает службы из каталога /etc/rc.d/init.d, а также службы, управляемые xinetd. Чтобы просмотреть краткое описание службы и её состояние, нужно выбрать службу по названию в списке, расположенном в левой части окна приложения.

Чтобы запустить, отключить, остановить или перезапустить службу, выберите ее из списка и нажмите соответствующую кнопку на панели инструментов или выберите действие в меню "Служба". Если служба работает под управлением xinetd, доступны только кнопки включения и отключения службы. Чтобы изменить текущий уровень запуска служб, нужно выбрать пункт меню "Служба->Настроить" и задать соответствующий уровень или уровни выполнения.

Когда вы сохраняете изменения служб xinetd, демон xinetd перезапускается и изменения вступают в силу немедленно. Когда же вы сохраняете изменения настроек других служб, уровень выполнения изменяется, но изменения не вступают в силу немедленно.

2.5 Приложение "Установка и удаление программ"

Для управления установкой программных компонентов в МСВСфера 6.3 АРМ предназначено приложение "Установка и удаление программ" (рис. 22), которое вызывается из меню "Система->Администрирование->Установка и удаление программ".

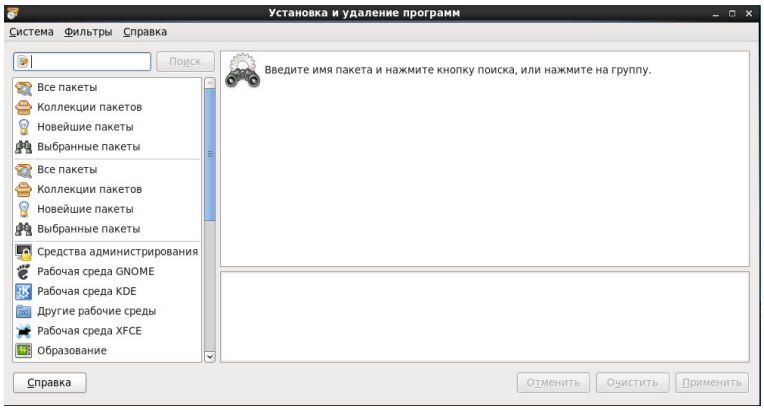


Рисунок 22 - Окно приложения "Установка и удаление программ"

Чтобы добавить источник установки программ, нужно выбрать меню приложения "Система->Источники программ" и в открывшемся диалоговом окне выбрать из предложенных источников необходимый, установив рядом с ним галочку. Можно так же добавить текстовые и отладочные источники программ, установив соответствующий флажок. После чего нажать кнопку "Закрыть".

Чтобы отфильтровать пакеты, нужно выбрать группу программного обеспечения ("Все пакеты", "Коллекции пакетов", "Новейшие пакеты", "Выбранные пакеты", "Средства администрирования" и т.д.) на левой боковой панели. В результате пакеты будут отфильтрованы по выбранной категории. Или использовать пункт меню "Фильтры" и в нем определять группы ("Только установленные", "Только пользовательские", "Только новейшие пакеты" и т.д.).

Для поиска программы и относящихся к ней пакетов необходимо ввести название программы в свободное поле. Например, поиск программы Emacs будет выглядеть, как на рис. 23. После нажатия кнопки "Поиск" будут выведены результаты поиска, описание для каждого пакета.

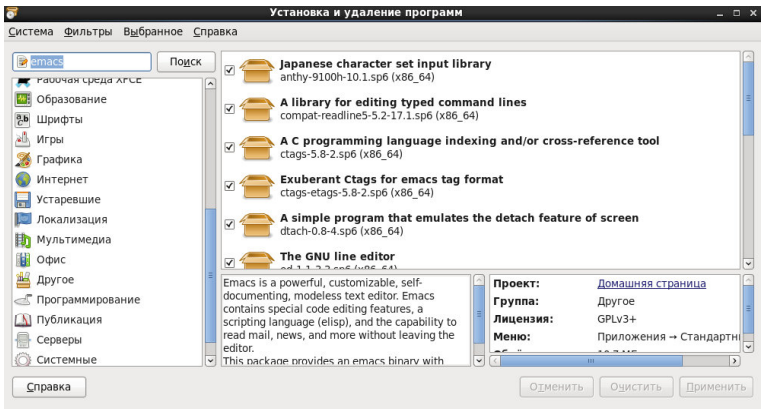


Рисунок 23 - Поиск пакетов, относящихся к программе Emacs

Чтобы установить пакет, нужно найти его и выбрать в списках, как на рис. 24. Или отметить несколько пакетов галочками.

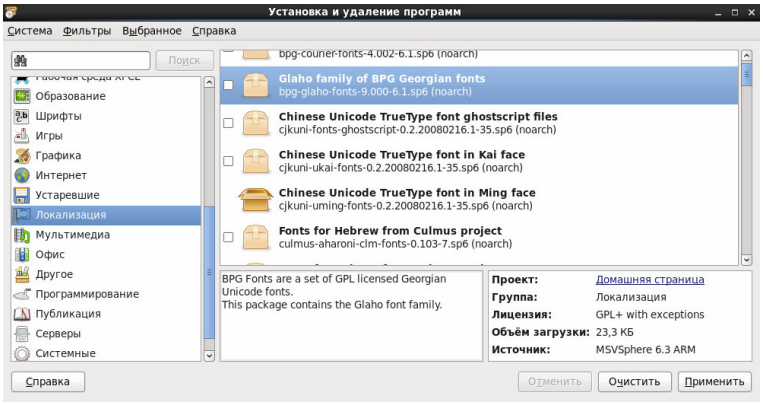


Рисунок 24 - Выбор пакета

Далее нужно перейти к пункту меню "Выбранное->Install". В результате пакет будет помечен, как на рис. 25. После этого необходимо нажать кнопку "Применить".

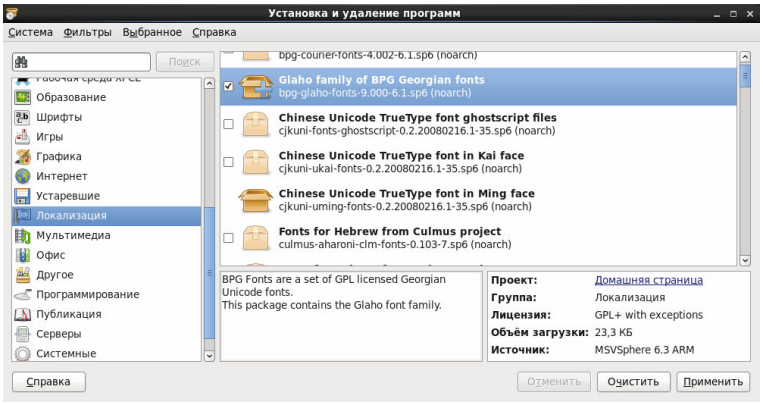


Рисунок 25 - Пометка пакета для установки

Программой-установщиком будут определены зависимости приложения, которые будут предложены для установки в диалоговом окне, как на рис. 26. После чего необходимо нажать кнопку "Установить".

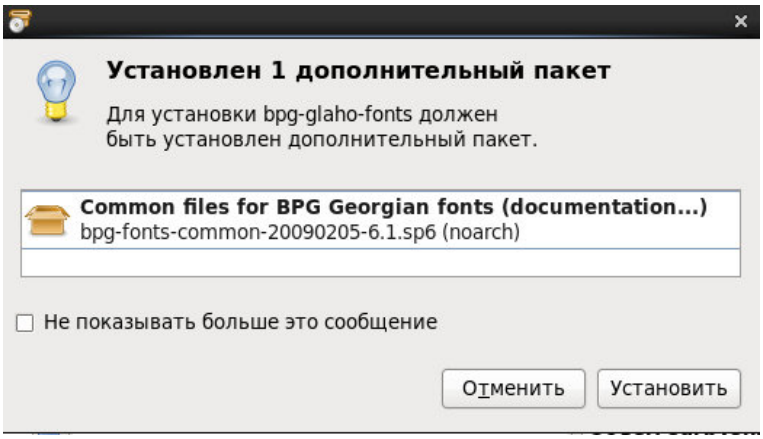


Рисунок 26 - Установка зависимостей

После установки дополнительного пакета появится диалоговое окно подтверждения. Если вы доверяете указанному источнику пакетов и идентификатору подписи, то нажмите кнопку "Да" (рис. 27).

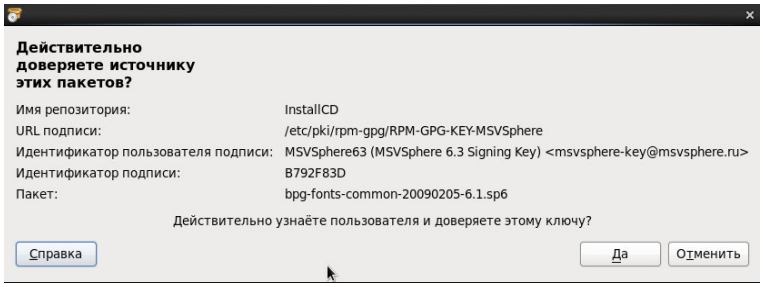


Рисунок 27 - Диалоговое окно подтверждения

В результате пакет будет установлен и помечен значком, как на рис. 28.

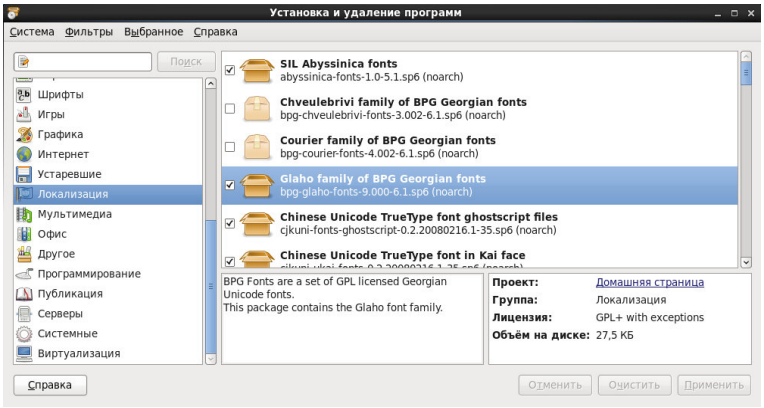


Рисунок 28 - Окно установки и удаления программ

Чтобы удалить пакет нужно его выбрать и перейти к пункту меню "Выбранное->Remove". В результате пакет будет отмечен, как на рис. 29. После чего нужно нажать кнопку "Применить".

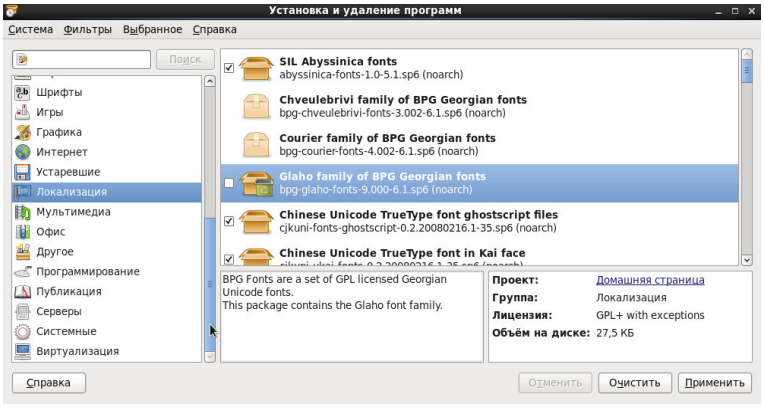


Рисунок 29 - Отметка для удаления файла

Программа предложит удалить дополнительный пакет, который зависит от удаления основной программы, в диалоговом окне (рис.30). Подтвердите удаление кнопкой "Удалить".

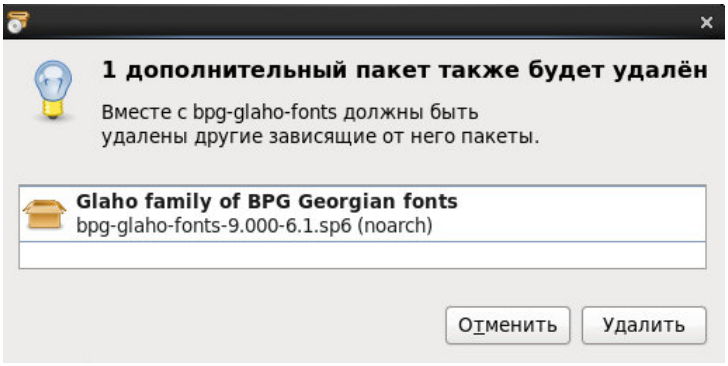


Рисунок 30 - Удаление дополнительного пакета

В результате в списке пакетов вы увидите удаленный пакет (рис.31).

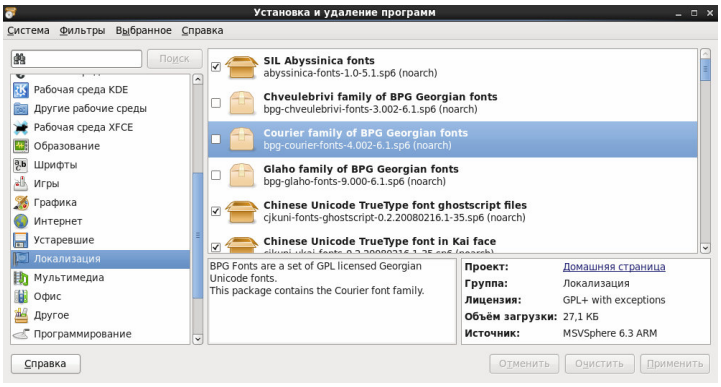


Рисунок 31 - Окно установки и удаления программ

Для определения домашней страницы выбранного проекта перейдите в пункт меню "Выбранное->Project homepage". Чтобы запустить программу перейдите в пункт меню "Выбранное->Run program". На примере приложения Emacs, программа выдаст диалоговое окно с вопросом о необходимости выполнения указанного приложения (рис.32). Нажмите кнопку "Выполнить".

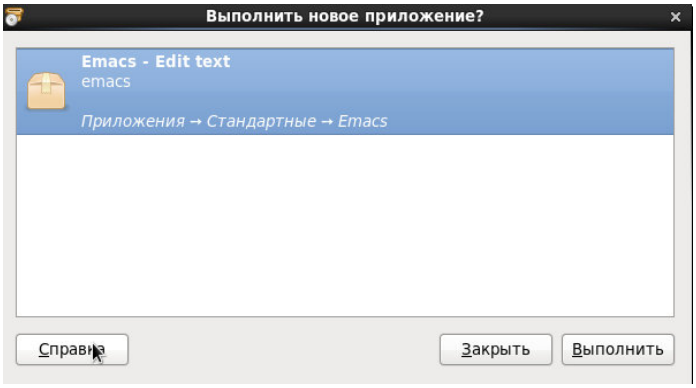


Рисунок 32 - Диалоговое окно запроса выполнения приложения

После выполненных действий запустится редактор Emacs (рис. 33).

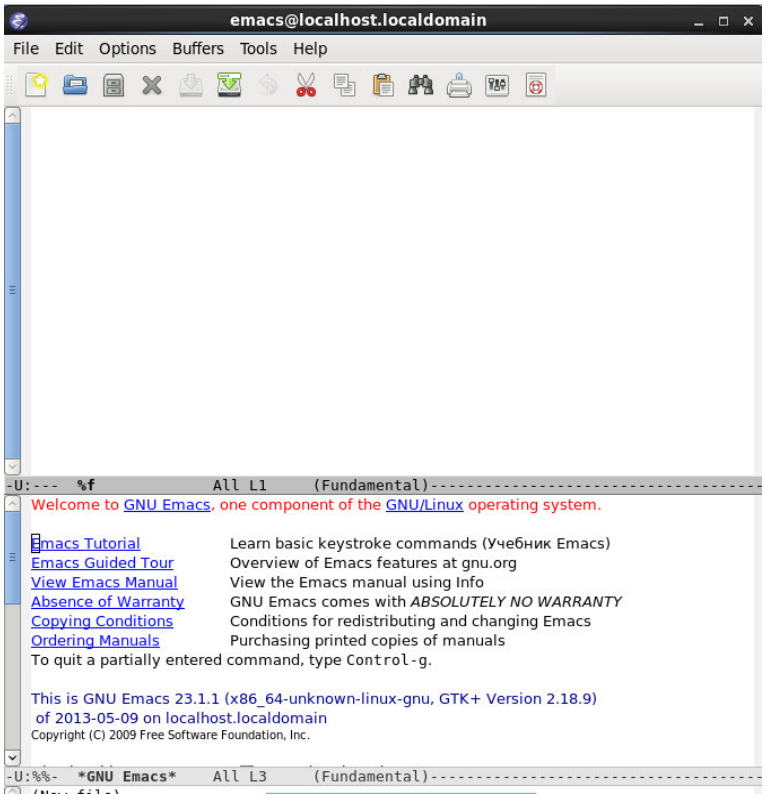


Рисунок 33 - Приложение Emacs

Для определения зависимостей выберите пакет и перейдите в пункт меню "Выбранное->Depends on". В результате программа выдаст диалоговое окно, в котором будут перечислены зависимости (рис. 34).

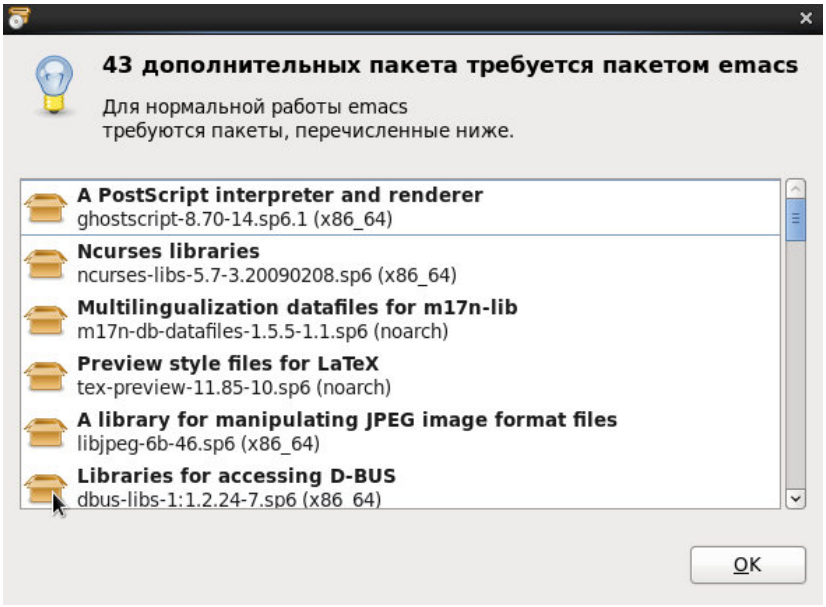


Рисунок 34 - Определение зависимостей для пакета

Чтобы определить какие пакеты зависят от выбранного приложения, нужно перейти в пункт меню "Выбранное->Required by" (рис. 35).

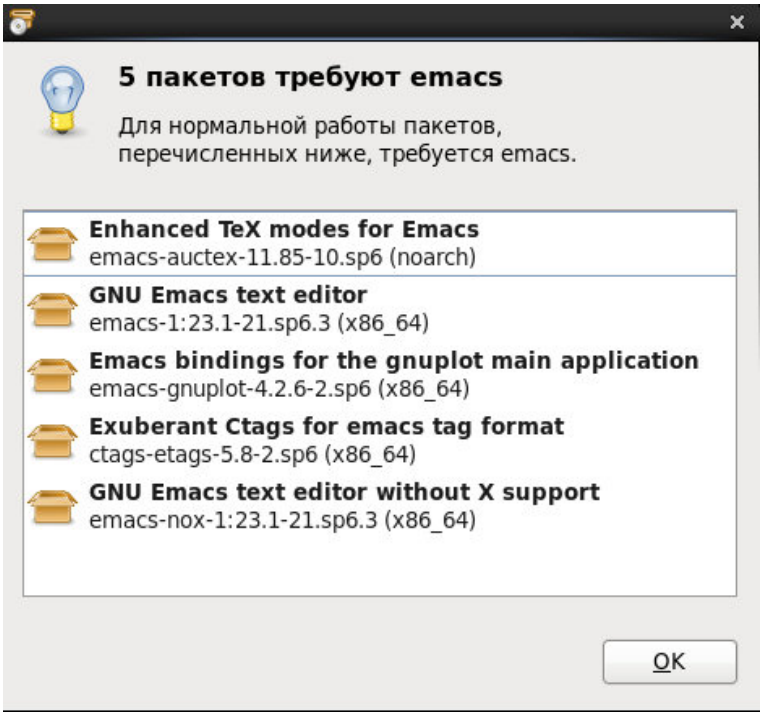


Рисунок 35 - Перечень пакетов, для которых необходима выбранная программа

Если установленные пакеты не зависят от выбранного, то в результате данной операции будет выведено сообщение, как на рис. 36.

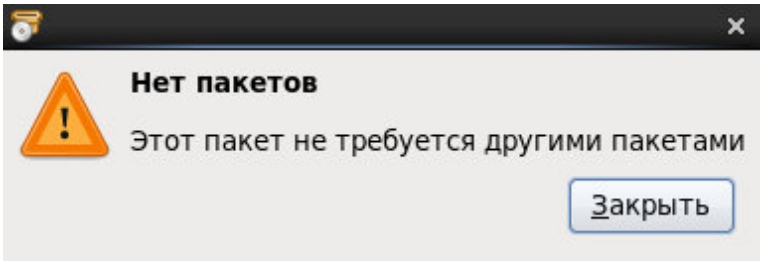


Рисунок 36 - Сообщение об отсутствии зависящих пакетов

Чтобы посмотреть список установленных файлов, нужно перейти в пункт меню "Выбранное->Get file list" (рис. 37).

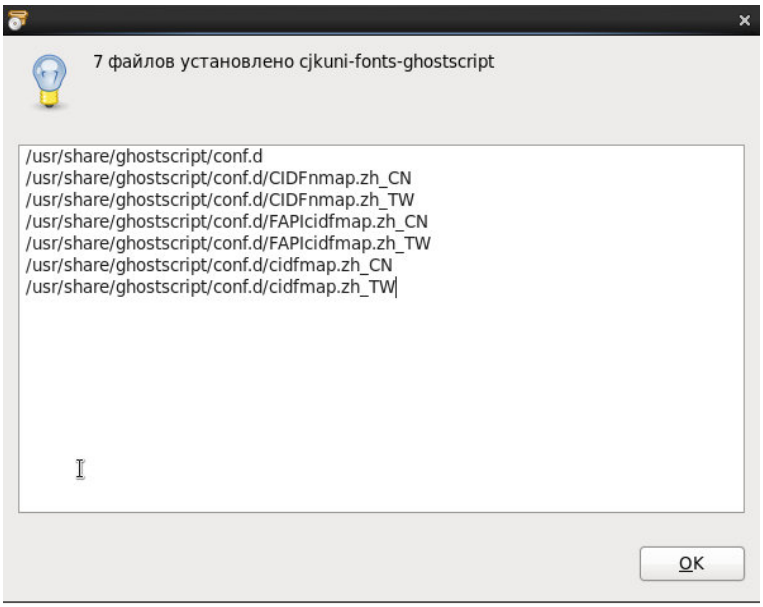


Рисунок 37 - Список установленных файлов

3 МОНИТОРИНГ СИСТЕМЫ

3.1 Основные сведения

Средства мониторинга системы МСВСфера 6.3 АРМ предоставляют следующие возможности:

- слежение за выполнением приложения и определение его работоспособности;
- диагностика приложения или системы, в которых возникают ошибки;
- сбор информации о процессах и пользователях;
- мониторинг оборудования и производительности системы;
- сбор статистики об использовании памяти и дискового пространства;
- анализ защищенности и обнаружение вторжений.

Вышеперечисленные возможности мониторинга системы реализуются с помощью следующих программных компонент:

- инструмент мониторинга сети iputils;
- утилита logwatch;
- утилита lsof;
- утилита mtr;
- утилита nmap;
- утилита ps;
- программа psacct;
- утилита quota;
- утилита tcpdump;
- утилита top;
- утилита free;
- утилита df;
- утилита du;
- программа OProfile;
- приложение "Wireshark Network Analizer";
- приложение "KDiskFree";
- приложение "KSystemLog";
- приложение "Анализатор использования дисков";

- приложение "Системный монитор";
- приложение "Диагностика проблем SELinux".

3.2 Пакет утилит iputils

Пакет iputils содержит базовые утилиты мониторинга сети:

- clockdiff - измеряет рассинхронизацию между двумя системами;
- ping/ping6 - посылает пакеты ICMP ECHO_REQUEST хостам сети;
- arping - отправляет ARP-запрос окружающим хостам;
- rdisc - демон поиска сетевого шлюза;
- tracepath/tracepath6 - показывает маршрут по сетевым узлам с MTU.

Утилита clockdiff

Команда clockdiff измеряет рассинхронизацию между текущей и удаленной системой с точностью в 1 мс (рис. 38), используя пакеты ICMP TIMESTAMP или опцию IP TIMESTAMP, иногда совместно с ICMP ECHO. Формат команды:

clockdiff [-o] [-o1] <удаленная система>

Опции команды:

-o использовать IP TIMESTAMP с ICMP ECHO вместо сообщений ICMP TIMESTAMP;

-o1 немного отличается от -o, а именно - использует трех-условный IP TIMESTAMP с предзаданными адресами пересылки, вместо четырех-условного.

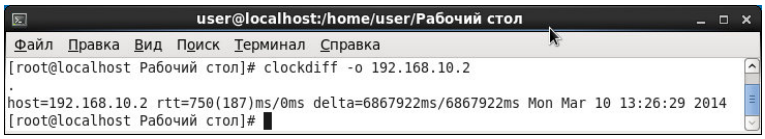


Рисунок 38 - Выполнение команды clockdiff

Утилита ping/ping6

Команда ping, аналогично как и ping6, использует обязательные датаграммы ECHO_REQUEST протокола ICMP для получения по этому протоколу ответов ECHO_RESPONSE от хоста или шлюза.

Датаграммы ECHO_REQUEST состоят из заголовков IP и ICMP, структуры данных struct timeval и произвольного числа байтов для заполнения пакета.

Формат команды:

ping [-LRUbdfnqrvVaAB] [-c <количество>] [-i <интервал>] [-l <преднагрузка>]
[-p <шаблон>] [-s <размер_пакета>] [-t ttl] [-w <ограничение_на_время_работы>]
[-F <идентификатор_потока>] [-I <адрес>] [-M <указание>] [-Q <тип_обслуживания>]
[-S <буфер_отправки>] [-T <параметр_временной_метки>]
[-W <время_ожидания_ответа>] [<переход>...] <назначение>

Опции команды:

-a сопровождать работу программы звуком;

-A адаптировать интервал между отправками пакетов к длительности их доставки и возврата. Таким образом, если только не выполняется преднагрузка, в любой момент времени может быть не больше одного пакета, на который не получен ответ;

-b разрешить использование широковещательного адреса в качестве целевого;

-B запретить изменение исходного адреса для пакетов во время работы программы. Исходный адрес определяется в начале работы ping;

-c <количество> остановить работу после передачи заданного количества пакетов ECHO_REQUEST. Если задано ограничение на время работы, программа будет ждать указанное количество ответных пакетов ECHO_REPLY в указанный период;

-d устанавливает параметр SO_DEBUG на используемый сокет;

-F <идентификатор_потока> устанавливать <идентификатор_потока> в отправляемых пакетах (только для ping6). Если указан нуль, <идентификатор_потока> будет генерироваться случайно ядром;

-f лавинообразный режим, для каждого пакета ECHO_REQUEST выводится точка ('.'), для каждого ответного пакета ECHO_REPLY - забой (удаление последней точки). Это позволяет наглядно представлять число потерянных пакетов. Если интервал между отправками не задан, последние производятся с наибольшей скоростью, по мере получения ответов, или со скоростью 100 раз в секунду, в зависимости от того, в каком случае получается большая скорость. Задавать нулевой интервал между отправками может только суперпользователь;

-i <интервал> интервал в секундах между отправкой пакетов. По умолчанию между отправкой пакетов делается пауза в 1 секунду, либо, в случае лавинообразного режима, отправка производится без пауз. Задавать значения меньше 0.2 может только суперпользователь;

-I <адрес> установить адрес источника в указанный. В качестве аргумента может выступать числовой IP-адрес или имя устройства. Этот параметр обязателен при отправке запросов на локально соединённый адрес IPv6;

-l <преднагрузка> послать с максимальной скоростью указанное количество пакетов, не дожидаясь ответов, и затем перейти в обычный режим работы. Значения больше 3 может указывать только суперпользователь;

-L подавлять циклические петли для широковещательных пакетов. Этот ключ применяется только если в качестве целевого адреса указан широковещательный;

-n только цифровой вывод, не расшифровывать имена (символьный вид) адресов;

-p <шаблон> можно указать до 16 несмысловых байтов для заполнения пакетов. Это полезно при диагностике проблем в сети. Например, "-p ff" заполнит все пакеты единицами символами;

-Q <тип_обслуживания> разряды байта QoS (Quality of Service - качество обслуживания) для датаграмм ICMP. <Тип-обслуживания> может быть либо десятичным либо шестнадцатеричным числом. Обычно (согласно RFC 1349) это значение интерпретируется так: младший (нулевой) разряд зарезервирован (сейчас используется для управления событиями при переполнении), разряды 1-4 используются для указания собственно типа обслуживания, и разряды 5-7 для приоритета (IP-предпочтения). Возможные типы обслуживания: минимизация стоимости - 0x02, максимизация надёжности - 0x04, максимизация пропускной способности - 0x08 минимизация задержек - 0x10. Одновременно можно указывать только один из четырёх перечисленных разрядов. Возможный диапазон значения приоритета - от приоритетного (0x20) до управляемого сетью (0xe0). Для указания высокого приоритета необходимы права суперпользователя (точнее, должно быть доступна возможность CAP_NET_ADMIN). Разряд 0x01 можно устанавливать только если в ядре включен ECN. В RFC 2474 этот байт переопределён как DS (Differentiated Services - дифференцированные службы): разряды 0-1 отведены для отдельных данных (тут будет использоваться ECN) разряды 2-7 для DSCP (Differentiated Services Codepoint - точка кода дифференцированных служб);

-q выводить только начальные и итоговые данные, не выводить информацию об отдельных запросах;

-R записывать маршрут. Для пакетов ECHO_REQUEST будет включен параметр RECORD_ROUTE и на экран будет выведен буфер маршрута для возвращённых пакетов. Заметим, что в заголовок IP помещается не больше 9 таких маршрутов. Многие узлы игнорируют или не отбрасывают этот параметр;

-r не использовать обычные таблицы маршрутизации и передавать данные прямо на компьютер, подключенный к интерфейсу. Если компьютер не находится в сети с прямым подключением, то возвращается сообщение об ошибке. Этот параметр, по которому не идет маршрутизация, может использоваться вместе с "-I" для проверки локальной системы через интерфейс;

-s <размер_пакета> размер пакетов для пересылки. По умолчанию - 56, что соответствует размеру 64 байта после добавления 8 байтов заголовка ICMP;

-S <буфер_отправки> размер буфера отправки соединения. По умолчанию буферизируется не больше одного пакета;

-t ttl время актуальности пакета IP (ttl - Time to Live);

-T <параметр_временной_метки> параметры временной метки IP. Возможные значения <параметра_временной_метки>: tsonly (только временная метка), tsandaddr (временная метка и адреса) и tsprespec <хост1> [<хост2> [<хост3> [<хост4>]]] (отмечать переходы);

-M <указание> стратегия обнаружения маршрута MTU. Возможные значения: do (запретить фрагментацию, даже локальную), want (выполнять обнаружение PMTU, фрагментировать локально если размер пакета слишком большой) и dont (не устанавливать флаг DF);

-U выводить полное время прохода. По умолчанию выводится сетевое время прохода, которое может отличаться от реального, например из-за ошибок DNS;

-v выводить подробную информацию;

-V вывести информацию о версии и закончить работу;

-w <ограничение_на_время_работы> время, по истечении которого ping завершит свою работу независимо от количества посланных и принятых пакетов. При указании этого параметра время ожидания для одного пакета игнорируется и работа может быть завершена ранее указанного срока только в случае получения информации об ошибке;

-W <время_ожидания_ответа> время ожидания (в секундах) ответного пакета. Принимается во внимание только если не было принято ни одного ответа. В противном случае программа ожидает получения двух ответов;

При использовании команды ping для локализации неполадки сначала запустите её с адресом локального хоста для проверки работоспособности локального сетевого интерфейса. Затем проверяйте связь посредством ping со всё более удалёнными компьютерами и шлюзами. Время прохождения сигналов в обе стороны и потери пакетов подсчитываются и

анализируются позднее. Если принимаются дублированные пакеты, то они не включаются в статистику утерянных пакетов, хотя время прохода таких пакетов включается в статистику минимального/среднего/максимального времени. После отправки и получения указанного количества пакетов или при прерывании работы программы сигналом SIGINT выводится краткий итог работы. Более краткую статистику можно получить без прерывания процесса с помощью сигнала SIGQUIT.

Если ответные пакеты не будут получены, то программа завершит работу с кодом выхода 1. Если указаны количество пакетов и ограничение на время работы, но по истечении этого времени принято менее запрошенного числа пакетов, то программа также завершит работу с кодом выхода 1. При других ошибках выход будет произведен с кодом 2. Иначе программа завершает работу с кодом 0. Эти значения позволяют использовать коды выхода для определения доступности серверов и компьютеров в сети.

Эта программа предназначена для тестирования сетей, управления сетями и измерения производительности. Из-за нагрузок, которые она создаёт в сети, неразумно использовать ping в рабочее время или в автоматических сценариях.

Описание пакетов ICMP

Заголовок IP без параметров имеет размер 20 байтов. Пакет ICMP ECHO_REQUEST содержит дополнительные 8 байтов, предназначенные для заголовка ICMP, и произвольное количество заполняющих байтов для обеспечения требуемого размера пакета, определяемое аргументом <размер_пакета> данных (по умолчанию 56). Поэтому количество полученных данных из пакета IP типа ICMP ECHO_REPLY всегда будет на 8 байтов (заголовок ICMP) больше, чем задаваемое.

Если заданный размер данных не меньше размера struct timeval, то программа включает в них временную метку, используемую для измерения времени прохода сигнала в обе стороны. В противном случае такое время не будет измеряться.

Повторяющиеся и поврежденные пакеты

Программа выводит сообщения о дублированных и повреждённых пакетах. Дублированные пакеты свидетельствуют о ненадёжной связи на уровне канала. Они могут появляться в разных ситуациях и если это происходит с небольшой частотой, то на это можно не обращать внимания.

Повреждённые пакеты являются прямым свидетельством неполадок в аппаратной части на одном из участков сети, через который проходили пакеты.

Тестирование на различных данных

Сетевая часть механизма передачи данных не должна обрабатывать пакеты по-разному, в зависимости от содержащихся в них данных. К сожалению, такие проблемы часто встречаются в сетях и остаются невыявленными достаточно долго. Во многих случаях оказывается, что некорректно обрабатывается некоторый вырожденный шаблон, например, состоящий из одних нулей или единиц, либо близкий к нему. Простой проверки по вырожденным шаблонам данных недостаточно, т.к. речь идёт о данных на уровне канала данных, которые могут соотноситься с указываемыми вами данными самым сложным образом.

В любом случае, такие проблемы означают, что вам предстоит очень много работ по тестированию и выявлению вышедшего из строя элемента. Если вам повезёт, то вы найдёте файл, который вообще не будет передаваться по сети, или будет передаваться очень долго по сравнению с файлами такого же размера, и затем сможете исследовать его на предмет возможных проблемных шаблонов, проверить которые можно с помощью ключа -p программы ping.

Время актуальности (TTL)

Значение TTL для пакетов IP задаёт максимальное количество IP-маршрутизаторов, через которое пакет ещё будет доставляться, а не считаться утерянным. Сейчас каждый маршрутизатор в Интернете уменьшает поле TTL при обработке пакета на единицу.

Согласно спецификации TCP/IP значение поля TTL для пакетов TCP должно быть равно 60.

Максимальное значение данного поля равно 255 и многие Unix-системы устанавливают поле TTL для пакетов ICMP ECHO_REQUEST в 255. Поэтому иногда получается, что вы можете проверить связь командой ping до некоторых компьютеров, но не можете связаться с ними программами telnet или ftp.

В обычном режиме ping выводит значения времени актуальности принятых (возвращённых) пакетов. При приёме пакета удалённой системой она может выполнить одно из трёх возможных действий с полем TTL в ответ:

- не изменять его, TTL в принятом пакете будет 255 минус количество пройденных маршрутизаторов на пути в обе стороны;
- установить его в 255, в этом случае значение TTL в принятом пакете будет 255 минус количество пройденных маршрутизаторов от удалённой системы до исходной;
- установить его в какое-либо другое значение, некоторые машины устанавливают его равным используемому для TCP пакетов, например, либо 30 либо 60.

Пример выполнения утилиты ping приведен на рис. 39.

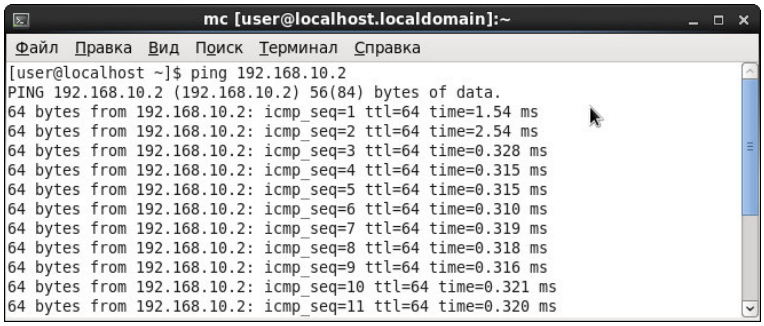


Рисунок 39 - Пример выполнения утилиты ping

Утилита arping

Утилита arping отправляет ARP-запрос устройству с MAC адреса через сетевой интерфейс, используя адрес отправителя. Формат команды:

arping [-AbDfhqUV] [-c <счетчик>] [-w <дедлайн>] [-s <отправитель>]
-I <интерфейс> <адресат>

Опции, используемые командой:

-A аналогично -U, но используются пакеты ARP REPLY вместо ARP REQUEST;

-b отправляет только широковещательные пакеты уровня MAC. Обычно arping сначала отправляет широковещательные пакеты, а после приема ответа - только адресату;

-c <счетчик> останавливает отправку после отсылки счетчик пакетов ARP REQUEST. С <дедлайн> опцией, arping ожидает счетчик пакетов ARP REPLY, пока не истечет указанное время;

-D режим дублированного обнаружения адреса, возвращает 0, если дублированное определение адреса прошло успешно, т.е. ответы не приняты;

-f завершает работу после первого приема ответа;

-I <интерфейс> наименование сетевого устройства (интерфейса), через который отправляются пакеты ARP REQUEST. Указание интерфейса для этой опции обязательно;

-h отображает страницу помощи и завершает работу;

-q вывод не отображается;

-s <отправитель> IP адрес отправителя, использующийся в ARP пакетах. Если эта опция не указана, используется следующий адрес отправителя:

- в режиме сдублированного определения адреса (с опцией -D) - 0.0.0.0;
- в обычном ARP-режиме (с опцией -U или -A) используется адресат;
- в других случаях адрес вычисляется по таблице маршрутизации.

-U предоставляет содержимое кэша ARP для обновления ARP кэшей соседних систем, ответы не ожидаются;

-V показывает номер версии программы и завершает работу;

-w <дедлайн>указывает таймаут в секундах перед тем, как arping завершит работу и отобразит сколько пакетов было отправлено или принято. В этом случае arping не останавливается после отправки счетчик пакетов, он ожидает, пока дедлайн истечет или пока не будет принято <счетчик> ответов.

Пример работы утилиты arping приведен на рис. 40.

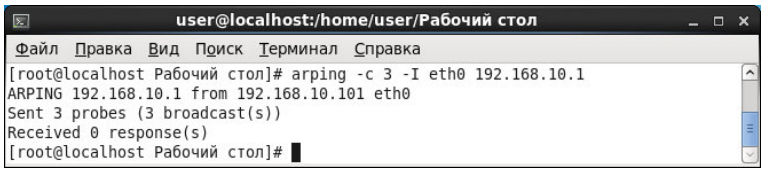


Рисунок 40 - Пример работы утилиты arping

Утилита rdisc

Утилита rdisc выступает клиентом протокола поиска шлюза по ICMP. rdisc вызывается при загрузке для получения таблиц маршрутизации сети с шлюзами по умолчанию.

rdisc прослушивает широковещательный адрес ALL_HOSTS (224.0.0.1) или <receive_address>, если он указан в параметрах, ожидая сообщения шлюзов типа ROUTER_ADVERTISE. Сообщения шлюзов, не входящих в текущую сеть, игнорируются. Среди оставшихся адресов шлюзы с самым высоким приоритетом используются как шлюзы по умолчанию и каждый из них добавляется в таблицу маршрутизации ядра.

Опционально, rdisc может пропускать режим ожидания объявления шлюзов, отсылая несколько сообщений ROUTER_SOLICITATION на адрес ALL_ROUTERS (224.0.0.2) или <send_address>, который указан в параметрах.

Каждому адресу шлюза назначается таймер и, в случае если время таймера истекло прежде, чем получено очередное сообщение с анонсом этого шлюза, этот шлюз не добавляется в таблицу маршрутизации. Адрес будет также исключён из рассмотрения если хост получает пакет с анонсом с максимально отрицательным приоритетом.

Сторона сервера протокола нахождения шлюзов поддерживается Cisco IOS и другими более или менее полными демонами маршрутизации, например, gated.

Формат команды:

rdisc [-abdfstvV] [<send_address>] [<receive_address>]

Опции, используемые командой:

-a принимать все шлюзы независимо от приоритета, который указан в их анонсах. Обычно rdisc принимает и добавляет в таблицы маршрутизации ядра только шлюзы с наивысшим приоритетом;

-b противоположно опции -a, т.е. добавляет только шлюзы с наивысшим приоритетом;

-d записывать сообщения отладки в syslog;

-f запускает rdisc на всё время, даже если шлюзы не найдены. Обычно rdisc ждет три пакета с анонсом и, в случае, если шлюзы не найдены, выходит с ненулевым значением. Если опция -f не указана, то должна быть указана опция -s;

-s посылает сначала три запроса, чтобы быстро определить шлюзы при загрузке системы. Если не найдены шлюзы, -s обеспечивает выход из rdisc с ненулевым значением. Может быть отменено опцией -f;

-t режим проверки. Не проводите в фоновом режиме;

-v выводить более подробные сведения в syslog;

-V вывести версию и выйти.

Утилита tracepath/tracepath6

Команда tracepath, как и tracepath6, показывает маршрут до указанного адреса с MTU. Программа использует указанный порт UDP или другой случайный порт.

Формат команды:

tracepath <адрес> [<порт>]

Пример выполнения команды "tracepath" показан на рис. 41.

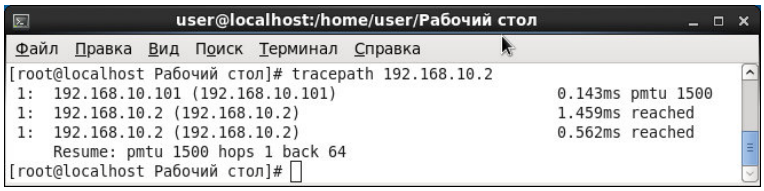


Рисунок 41 - Пример выполнения команды tracepath

Первая колонка показывает TTL шагов с двоеточием. Обычно значение TTL получается из сетевого отклика, но иногда отклик не содержит необходимой информации и делается попытка предположения данных. В этом случае после номера выводится "?".

Вторая колонка показывает сетевой сегмент, который ответил на тест. Это либо адрес маршрутизатора, либо слово [LOCALHOST], если пакет не был отправлен в сеть.

Остальная часть строки содержит различную информацию о сегменте маршрута. Как правило, это содержимое RTT. Кроме того, может быть показан MTU сегмента, если он меняется.

Последняя строка суммирует информацию обо всех маршрутах до указанного адреса, показывает общее значение MTU, количество сегментов до адреса и свою предполагаемую оценку количества сегмента из адресата к нам, которые могут различаться, когда маршруты асимметричны.

3.3 Утилита logwatch

Утилита logwatch производит анализ логов системы по различным критериям с возможностью составления отчёта.

Основной файл конфигурации logwatch находится в /usr/share/logwatch/default.conf/logwatch.conf и прежде, чем редактировать, скопируйте его следующей командой:

cp /usr/share/logwatch/default.conf/logwatch.conf /etc/logwatch/conf/

Файл logwatch.conf хорошо самодокументирован и прост, поэтому ниже будет приведено описание только основных опций, обычно затрагиваемых при конфигурации:

LogDir — путь к каталогу, в котором программа будет искать файлы, обычно это /var/log;

TmpDir — путь к каталогу, в котором утилита будет размещать временные файлы. По умолчанию это /var/cache/logwatch, который мы с вами создали ранее;

Output — указывает программе метод вывода отчёта. Может быть: stdout (в поток стандартного вывода), mail (почтовым сообщением) или file (в файл);

Format — определяет формат отчёта. Может иметь значение text или html;

MailTo — определяет адрес получателя отчёта, если Output = mail;

MailFrom — определяет адрес отправителя отчёта, если Output = mail;

Filename — задаёт путь к файлу отчёта, если Ouput = file;

Archives — используется для указания утилите необходимости анализа не только текущих лог-файлов, но и архивных (например messages.1, messages.2.gzи т. п.). Принимает значения Yes или No;

Range — за какой период времени отбирать анализируемые сообщения: All, Today или Yesterday;

Detail — определяет уровень детализации отчёта. Может принимать как числовые значения от 0 (минимум детализации) до 10 (максимум). Также можно использовать синонимы: Low, Med и High, которые соответственно равны числовым 0, 5 и 10;

Service — этот параметр указывает программе имя службы, логи которой необходимо анализировать. Может иметь значение All или имя службы (имя файла из каталога /usr/share/logwatch/scripts/services/). Если необходимо анализировать логи более одной службы, но не всех, то опцию Service следует определить несколько раз с указанием имён нужных служб, по одной за раз. Если же необходимо анализировать лог-файлы всех служб, кроме некоторых, то необходимо сначала определить Service = All, а затем перечислить мена ненужных служб, предварив их знаком «минус», например: Service = «-zz-network»;

Настраиваемые параметры анализатора для каждой службы можно найти в /usr/share/logwatch/default.conf/services, а пути размещения лог-файлов каждой службы — в /usr/share/logwatch/default.conf/logfiles. Обычно значений параметров, определённых в этих файлах, достаточно для корректной работы, если в вашей системе все файлы хранятся в каталогах по умолчанию и имеют стандартные имена. Если же у вас в системе некоторые файлы расположены в специфических местах, то вам следует указать logwatch, где их искать.

После того, как файлы конфигурации готовы и проверены, достаточно лишь запустить командой в консоли утилиту logwatch.

Отрывок из вывода команды представлен на рис. 42.

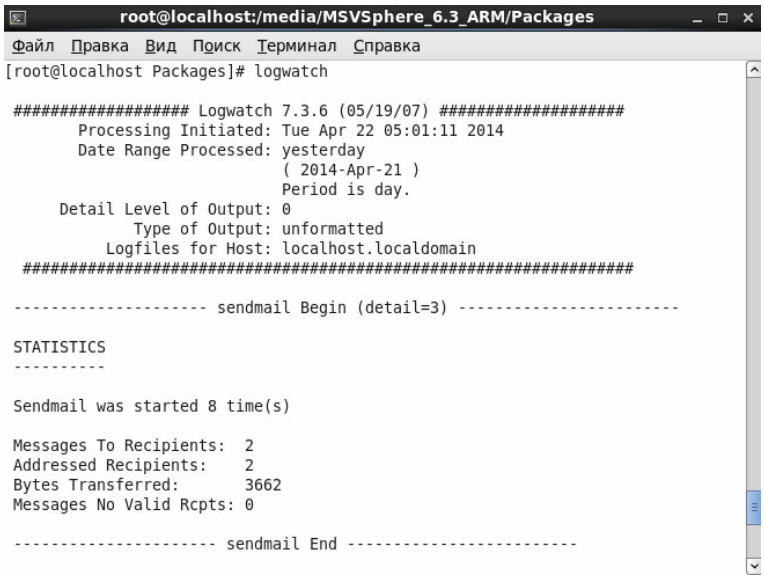


Рисунок 42 - Вывод команды logwatch

3.4 Утилита lsof

Утилита lsof (LiSt of Open Files) предназначена для вывода информации о том, какие файлы используются теми или иными процессами.

Запуск lsof без каких-либо опций выводит список всех открытых файлов всеми возможными процессами.

Чтобы посмотреть какие процессы или пользователи использует файл, нужно выполнить команду lsof <путь_к_файлу>. Так же можно указать несколько файлов, в результате чего будут выведены все процессы, которые используют данные файлы. Например, чтобы определить какие пользователи используют файл /etc/passwd нужно выполнить команду, как на рис. 43.

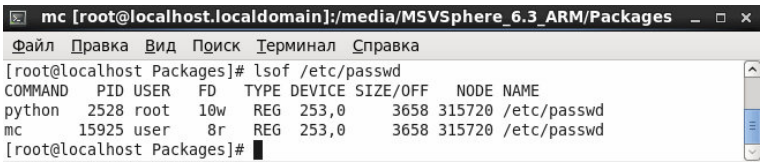


Рисунок 43 - Вывод информации об использовании файла /etc/passwd

Формат команды рекурсивного поиска всех открытых файлов, начиная с указанной директории, выглядит следующим образом:

lsof +D <директория>

Список всех файлов открытых пользователем можно вывести командой lsof -u <имя_пользователя>, например:

lsof -u user

Вы можете использовать список разделенный запятой, если хотите узнать информацию сразу по нескольким пользователям.

Чтобы найти все файлы открытые программой, например, редактором gedit, нужно выполнить следующую команду:

lsof -c gedit

Параметр -c выбирает список файлов принадлежащих процессу, чье имя начинается с gedit.

Опции lsof могут комбинироваться. Действие по умолчанию между опциями определяется как "ИЛИ". Параметр -a комбинирует опции с условием "И". Например:

lsof -a -u user -c gedit

Список всех файлов открытых всеми пользователями кроме root:

lsof -u ^root

Список всех файлов открытых процессом с определенным PID выводится следующей командой:

lsof -p <идентификатор процесса>

Параметр -p фильтрует вывод, отображая список файлов открытых программой с указанным id.

Список всех сетевых соединений:

lsof -i

Список всех TCP соединений:

lsof -i tcp

Список всех UDP соединений:

lsof -i udp

Чтобы определить процессы, использующие TCP или UDP с портом 25, нужно выполнить:

lsof -i :25

Также можно указать название порта:

lsof -i :smtp

Найти все сетевые действия пользователя можно командой:

lsof -a -u user -i

Список всех файлов для процессов, принадлежащих определенной группе можно определить, например, с помощью команды:

lsof -g 1234

Групповые процессы используются для логической группировки процессов. Этот пример покажет список всех файлов, открытых процессами, принадлежащими к группе с PGID 1234.

Несколько специальных значений, таких как mem, которые работают с файлами, отображаемыми в память:

lsof -d mem

Или txt программ загруженных и выполняемых в памяти:

lsof -d txt

Повторяющийся листинг файлов:

lsof -r 1

Аргумент -r заставляет lsof повторять список файлов, до тех пор пока он не будет остановлен. Аргумент 1 говорит, что необходимо повторять листинг через каждую секунду. Эту опцию лучше всего комбинировать с поисковым запросом, производящим мониторинг сетевой пользовательской активности:

lsof -r 1 -u user -i -a

С помощью утилиты lsof можно, например, просмотреть список процессов, работающих с CD ROM, как на рис. 44.

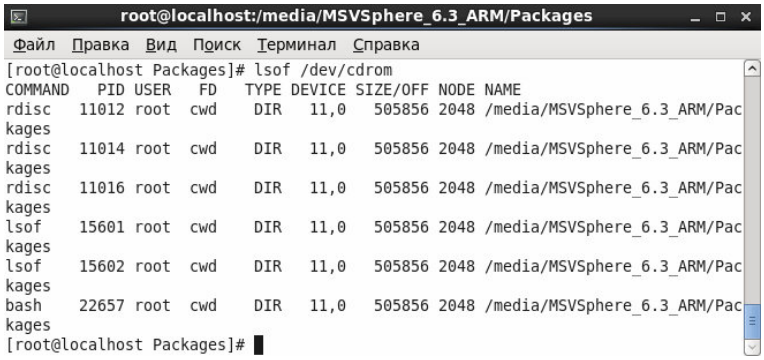


Рисунок 44 - Вывод списка процессов, работающих с CD ROM

Для получения дополнительной информации, обратитесь к странице man утилиты lsof.

3.5 Утилита mtr

Утилита mtr – это интерактивная программа, способная постоянно выводить обновленную статистику по трассировкам, позволяет выполнять диагностику сети в удобном и наглядном режиме.

mtr [-hvrctglspni46] [--help] [--version] [--report] [--report-cycles <COUNT>] [--curses] [--split] [--raw] [--no-dns] [--gtk] [--address <IP_ADDRESS>] [--interval <SECONDS>] [--psize <BYTES> | -s <BYTES>] <HOSTNAME> [<PACKET_SIZE>]

Опции команды:

-h, --help вывод справочной информации;

-v, --version вывод версии программы

-r, --report переводит mtr в режим отчета. В этом режиме, mtr обработает количество циклов, определенных опцией -c, затем отобразит статистику и завершит работу. Этот режим полезен для генерации статистики о качестве сети;

-c <COUNT>, --report-cycles <COUNT> установить количество циклов, после которых mtr завершит работу;

-s <BYTES>, --psize <BYTES> размер посылаемых пакетов;

-t вынуждает mtr использовать curses based terminal interface, если доступно;

-n, --no-dns не использовать DNS, отображать IP-адреса и не пытаться получить их имена хостов;

-g, --gtk используйте эту опцию для того, чтобы использовать оконный интерфейс X11 GTK+ , если он доступен. Чтобы это работало, GTK+ должен присутствовать в системе при сборке;

-p, --split используйте эту опцию для перевода в режим вывода в "расщепленном" формате (новые замеры отображаются не поверх существующих, а следующими строками вывода);

-l, --raw используйте эту опцию для перевода в режим вывода "сырых" данных. Этот формат лучше подходит для архивирования результатов замеров. Его можно подвергнуть разбору для представления в любом другом из методов отображения;

-a <IP_ADDRESS>, --address <IP_ADDRESS> используйте эту опцию, чтобы связать исходящие сокет пакеты для конкретного интерфейса, так чтобы любой пакет мог быть отправлен через этот интерфейс;

-i <SECONDS>, --interval <SECONDS> используйте эту опции для задания позитивного числа секунд между запросами ICMP ECHO, по умолчанию это одна секунда;

-4 использовать только IPv4;

-6 использовать только IPv6.

Пример выполнения команды mtr -n показан на рис. 45.

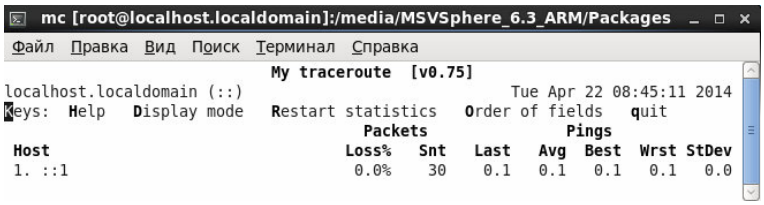


Рисунок 45 - Вывод команды mtr -n

Изм.	Лист	№ докум	Подп	Дата

3.6 Утилита nmap

Утилита nmap предназначена для настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети.

Nmap использует множество различных методов сканирования, таких как UDP, TCP (connect), TCP SYN (полуоткрытое), FTP-proxy (прорыв через ftp), Reverse-ident, ICMP (ping), FIN, ACK, Xmas tree, SYN- и NULL-сканирование. Nmap также поддерживает большой набор дополнительных возможностей, а именно: определение операционной системы удалённого хоста с использованием отпечатков стека TCP/IP, «невидимое» сканирование, динамическое вычисление времени задержки и повтор передачи пакетов, параллельное сканирование, определение неактивных хостов методом параллельного ping-опроса, сканирование с использованием ложных хостов, определение наличия пакетных фильтров, прямое (без использования portmapper) RPC-сканирование, сканирование с использованием IP-фрагментации, а также произвольное указание IP-адресов и номеров портов сканируемых сетей.

nmap [<типы_сканирования>] [<опции>] {<цель_сканирования>}

Для определения цели сканирования можно использовать сетевые имена, IP адреса, сети и т.д., например, scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254, и опции:

-iL <имя_входного_файла> использовать список хостов/сетей из файла;

-iR <количество_хостов> выбрать произвольные цели;

--exclude <хост1[,хост2][,хост3],...> исключить хосты/сети;

--excludefile <имя_файла> исключить список из файла.

Для обнаружения хостов используются следующие опции:

-sL сканирование с целью составления списка целей;

-sP пинг сканирование - просто определить, работает ли хост;

-PN расценивать все хосты как работающие - пропустить обнаружение хостов;

-PS/PA/PU [список_портов] TCP SYN/ACK или UDP пинг заданных хостов;

-PE/PP/PM пинг с использованием ICMP эхо запросов, запросов временной метки и сетевой маски;

-PO [список_протоколов] пинг с использованием IP протокола;

-n/-R никогда не производить DNS разрешение / всегда производить разрешение [по умолчанию: иногда];

--dns-servers <сервер1[,сервер2],...> задать собственные DNS сервера;

--system-dns использовать системный DNS преобразователь.

Различные приемы сканирования производятся с помощью опций:

-sS/sT/sA/sW/sM TCP SYN/c использованием системного вызова Connect()/ACK/Window/Maimon сканирования;

-sU UDP сканирование;

-sN/sF/sX TCP Null, FIN и Xmas сканирования;

--scanflags <флаги> задать собственные TCP флаги;

-sI <зомби_хост[:порт]> "ленивое" (Idle) сканирование;

-sO сканирование IP протокола;

-b <FTP_хост> FTP bounce сканирование;

--traceroute отслеживать путь к хосту;

--reason выводить причину нахождения порта в определенном состоянии.

Для определения портов и порядка сканирования необходимо использовать следующие опции:

-p <диапазон_портов> сканирование только определенных портов, например, p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080;

-F быстрое сканирование - сканирование ограниченного количества портов;

-r сканировать порты последовательно - не использовать случайный порядок портов;

--top-ports <количество_портов> сканировать <количество_портов> наиболее распространенных портов;

--port-ratio <рейтинг> сканировать порты с рейтингом большим, чем <рейтинг>.

Для определения служб и их версий подходят опции:

-sV исследовать открытые порты для определения информации о службе/версии;

--version-intensity <уровень> устанавливать от 0 (легкое) до 9 (пробовать все запросы);

--version-light ограничиться наиболее легкими запросами (интенсивность 2);

--version-all использовать каждый единичный запрос (интенсивность 9);

--version-trace выводить подробную информацию о процессе сканирования (для отладки).

Для сканирования с использованием скриптов необходимо воспользоваться следующими опциями:

-sC эквивалентно опции --script=default;

--script=<Lua_скрипты> <Lua_скрипты> - это разделенный запятыми список директорий, файлов скриптов или категорий скриптов;

--script-args=<имя1=значение1,[имя2=значение2,...]> передача аргументов скриптам;

--script-trace выводить все полученные и отправленные данные;

--script-updatedb обновить базу данных скриптов.

Для определения операционной системы подходят следующие опции:

-O активировать функцию определения операционной системы;

--osscan-limit использовать функцию определения операционной системы только для "перспективных" хостов;

--osscan-guess угадать результаты определения операционной системы.

Опции управления временем и производительностью, принимающие аргумент <время>, задаются в миллисекундах, пока вы не добавите 's' (секунды), 'm' (минуты), или 'h' (часы) к значению, например, "30m". Среди них основные опции:

-T[0-5]установить шаблон настроек управления временем;

--min-hostgroup/max-hostgroup <кол_хостов> установить размер групп для параллельного сканирования;

--min-parallelism/max-parallelism <кол_хостов> регулирует распараллеливание запросов;

--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <время> регулирует время ожидания ответа на запрос;

--max-retries <количество_попыток> задает максимальное количество повторных передач запроса;

--host-timeout <время> прекращает сканирование медленных целей;

--scan-delay/--max-scan-delay <время> регулирует задержку между запросами;

--min-rate <число> посылать запросы с интенсивностью не меньше чем <число> в секунду;

--max-rate <число> посылать запросы с интенсивностью не больше чем <число> в секунду.

Для обхода брандмауэров/IDS используются следующие опции:

-f; --mtu <значение> фрагментировать пакеты (опционально с заданным значением MTU);

-D <фикт_хост1,фикт_хост2[,ME],...> маскировка сканирования с помощью фиктивных хостов;

-S <IP_адрес>изменить исходный адрес;

-e <интерфейс> использовать конкретный интерфейс;

-g/--source-port <номер_порта> использовать заданный номер порта;

--data-length <число> добавить произвольные данные к посылаемым пакетам;

--ip-options <опции> посылать пакет с заданным ip опциями;

--ttl <значение> установить IP поле time-to-live (время жизни);

--spoof-mac <MAC_адрес/префикс/название производителя> задать собственный MAC адрес;

--badsum посылать пакеты с фиктивными TCP/UDP контрольными суммами.

Для вывода результатов используются опции:

-oN/-oX/-oS/-oG <файл> выводить результаты нормального, XML, ScriptKiddie и Grepable формата вывода, соответственно, в заданный файл;

-oA <базовове_имя_файла> использовать сразу три основных формата вывода;

-v увеличить уровень вербальности;

-d[уровень] увеличить или установить уровень отладки (до 9);

--open показывать только открытые (или возможно открытые) порты;

--packet-trace отслеживание принятых и переданных пакетов;

--iflist вывести список интерфейсов и роутеров (для отладки);

--log-errors записывать ошибки/предупреждения в выходной файл нормального режима;

--append-output добавлять в конец, а не перезаписывать выходные файлы;

--resume <имя_файла> продолжить прерванное сканирование;

--stylesheet <путь/URL> устанавливает XSL таблицу стилей для преобразования XML вывода в HTML;

--webxml загружает таблицу стилей с Nmap.Org;

--no-stylesheet убрать объявление XSL таблицы стилей из XML.

В работе будут так же полезны следующие опции:

-6 включить IPv6 сканирование;

-A активировать функции определения ОС и версии, сканирование с использованием скриптов и трассировку;

--datadir <имя_директории> определяет место расположения файлов Nmap;

--send-eth/--send-ip использовать сырой уровень ethernet/IP;

--privileged подразумевать, что у пользователя есть все привилегии;

--unprivileged подразумевать, что у пользователя нет привилегий для использования сырых сокетов;

-V вывести номер версии;

-h вывести эту страницу помощи.

Например, для отслеживания принятых и переданных пакетов нужно выполнить команду.

nmap --packet-trace 192.168.10.1

Для получения большей информации об опциях утилиты nmap обратитесь к странице man команды.

3.7 Утилита ps

Команда ps ax показывает список работающих в системе процессов, включая процессы, принадлежащие другим пользователям. Чтобы просмотреть также и владельцев этих процессов, выполните команду ps au**x** (рис. 46).

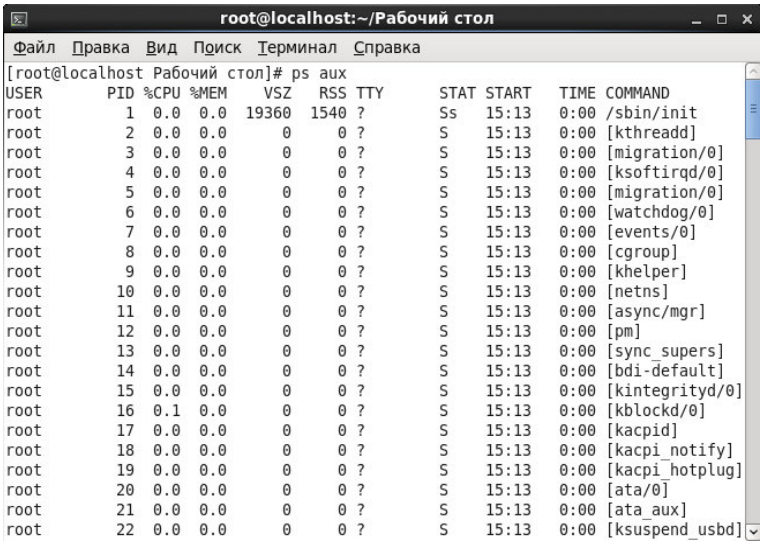


Рисунок 46 - Вывод списка работающих в системе процессов и их владельцев

Команда ps может вывести много информации. Чтобы она задержалась на экране, выполните команду ps aux | less, как на рис. 47.

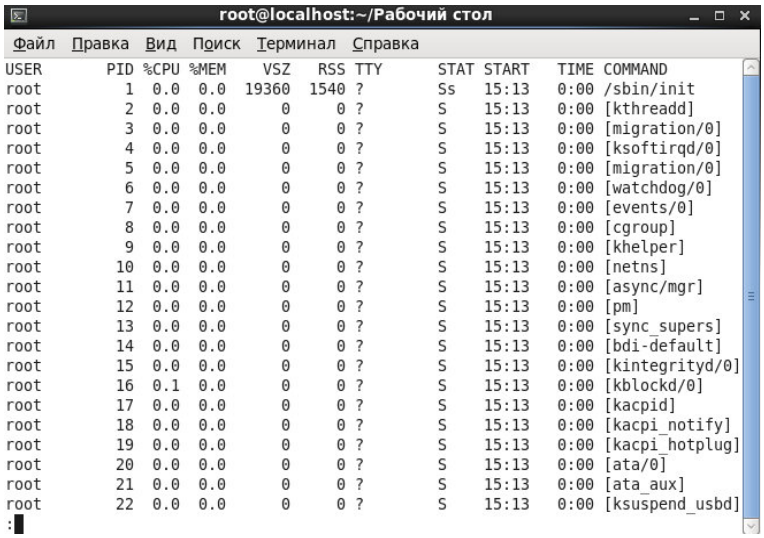


Рисунок 47 - Выполнение команды "ps aux | less"

Чтобы проверить, работает ли какой-то определённый процесс, выполните команду ps в сочетании с командой grep. Например, чтобы определить, работает ли Emacs, выполните команду ps ax | grep emacs, как на рис. 48.

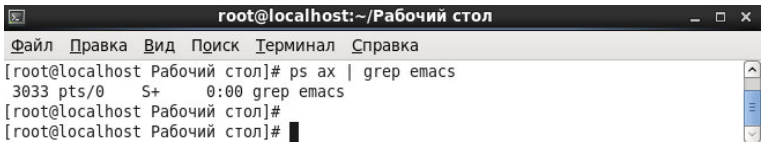


Рисунок 48 - Вывод информации по процессу emacs

3.8 Пакет утилит psacct

Psacct - это инструмент для мониторинга пользователей и приложений, которые работают или работали в системе. Программа работает в режиме background и собирает в log-файлы информацию. Программа позволяет отслеживать количество ресурсов, потребляемых тем или иным приложением.

По умолчанию сервис выключен и его нужно запускать вручную. Командой /etc/init.d/psacct status можно проверить состояние сервиса. Из рис. 49 видно, что сервис отключен. Запустить его нужно командой /etc/init.d/psacct start, после чего вновь проверить его статус и убедиться, что учет процессов включен.

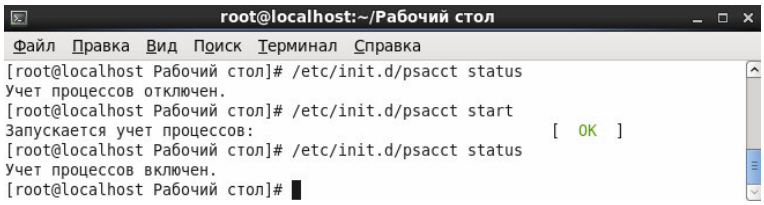


Рисунок 49 - Запуск сервиса psacct

Пакет psacct состоит из следующих утилит:

– ac – печатает статистику о времени, которое пользователи провели, находясь в системе;

– sa – собирает информацию о выполненных командах и запущенных приложениях и т.д.;

– lastcomm – просматривает последние выполненные команды;

– accton – включает/выключает сбор информации.

Как уже было описано выше, утилита **ac** показывает время (в часах), которое пользователь провел в системе. Чтобы вывести активность пользователя за день, при том не только текущий, нужно выполнить команду, как на рис. 50, время, проведенное за год, определяется, как на рис. 51.

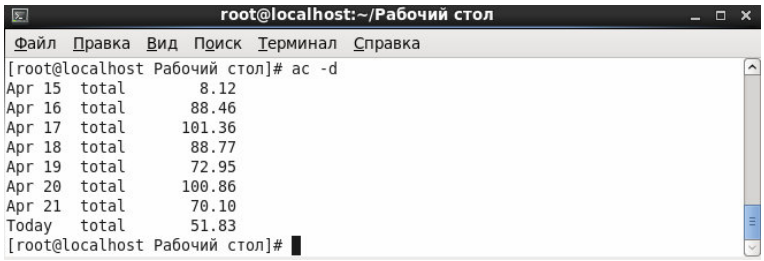


Рисунок 50 - Вывод активности пользователя в часах

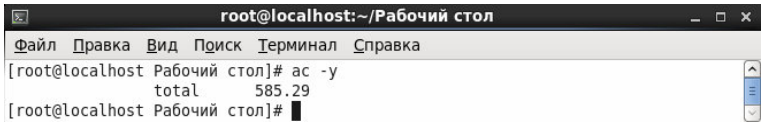


Рисунок 51 - Вывод времени, проведенного за год

Вывод проведенного времени в системе каждым пользователем приведен на рис. 52.

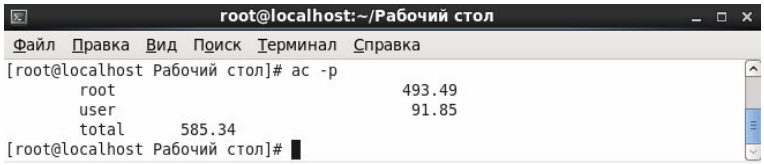


Рисунок 52 - Вывод проведенного времени в системе каждым пользователем

Утилита lastcomm выводит информацию по последним действиям пользователя, т.е. какие программы использовал и т.д.

Посмотреть последние действия определенного пользователя можно, как на рис. 53.

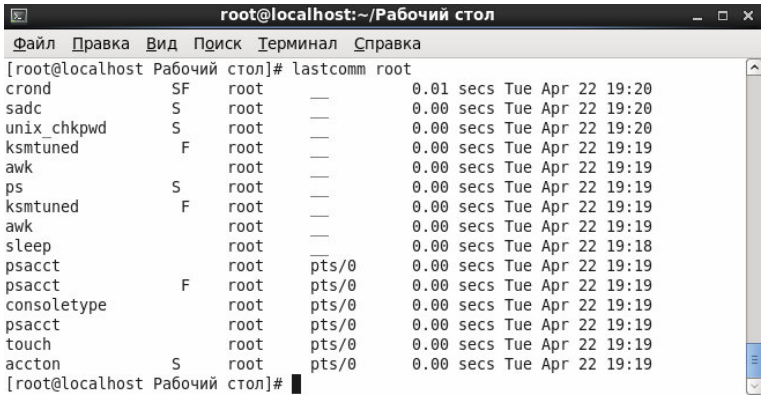


Рисунок 53 - Вывод последних действий пользователя root

Чтобы посмотреть какие пользователи и когда пользовались той или иной программой, нужно выполнить команду lastcomm <имя_программы>, например, как на рис. 54.

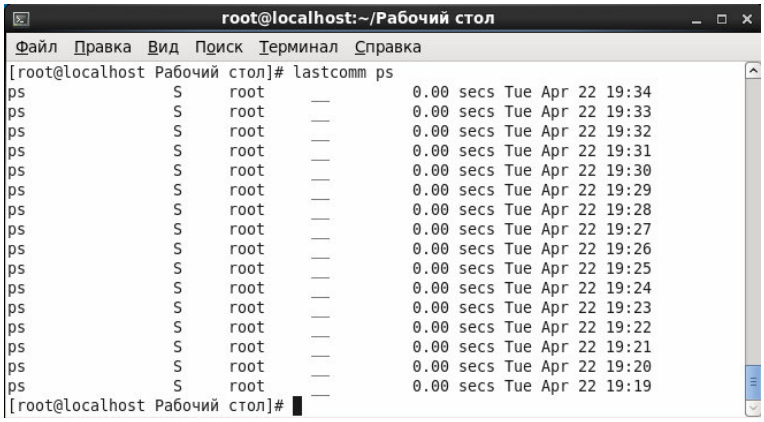


Рисунок 54 - Вывод использования утилиты ps

Команда sa –u показывает какие пользователи запускали какие программы, а так же сколько ресурсов (процессорного времени и памяти) использовали программы, которые были ими запущенны (рис. 55).

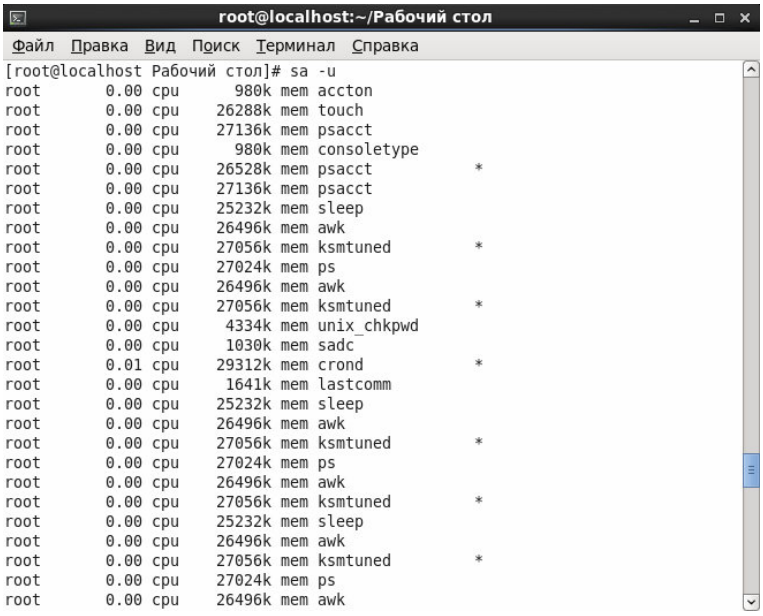


Рисунок 55 - Вывод команды sa -u

Количество процессов и количество использованного CPU времени, которые уже были использованы до настоящего времени выводятся командой sa –m (рис. 56).

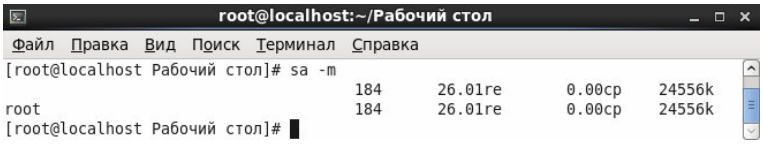


Рисунок 56 - Вывод команды sa -m

Чтобы вывести список программ, которые были запущенны на используемой машине, нужно выполнить команду sa -a, как на рис. 57.

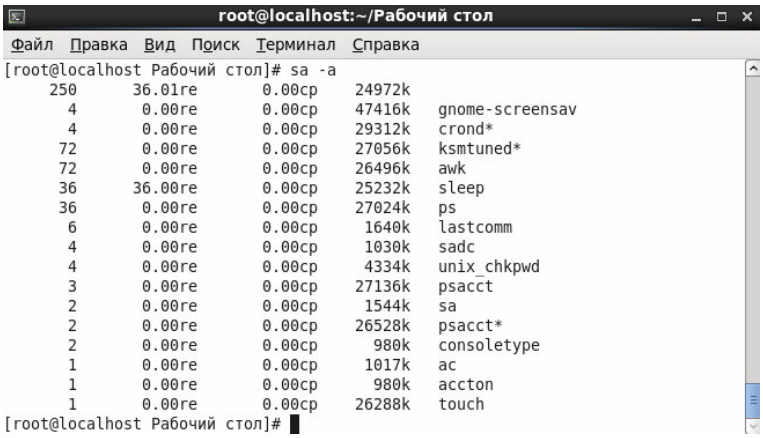


Рисунок 57 - Вывод списка программ, которые были запущенны

3.9 Утилита quota

Утилита quota отображает ограничения для пользователя на использование дисков. По умолчанию печатается информация для текущего пользователя.

Основные опции, используемые командой:

quota [-u] [-g] [-v | -q] <user> <group> , где:

-g <group> вывод квоты для групп, в которых пользователь является членом группы. Дополнительный параметр group позволяет просмотреть ограничения для конкретной группы, однако обычный пользователь может увидеть информацию только по группам, членом которых он является. Для просмотра информации об остальных группах необходимо иметь права супер-пользователя root и использовать команду sudo;

-u <user> вывод информации о дисковых ограничениях для указанного пользователя <user>. Совместное использование параметров **-**u и -g выдаст информацию, как о групповых квотах, так и индивидуальных квотах для пользователя. Для просмотра информации об ограничениях для других пользователей требуются права супер-пользователя;

-v вывод квоты файловой системы, где не выделяется место под хранение данных;

-q вывод краткой информации, только о файловых системах, где превышены квоты, имеет приоритет над параметром -v.

Первым делом необходимо отредактировать файл /etc/fstab, чтобы система знала, к каким разделам применять квоты. Далее в примерах предположим, что каталог /home в системе смонтирован из отдельного раздела. Поскольку мы собираемся управлять квотами для пользователей, то добавим опцию монтирования usrquota, как на рис. 58. Для включения квот для групп необходимо аналогично добавить опцию grpquota.

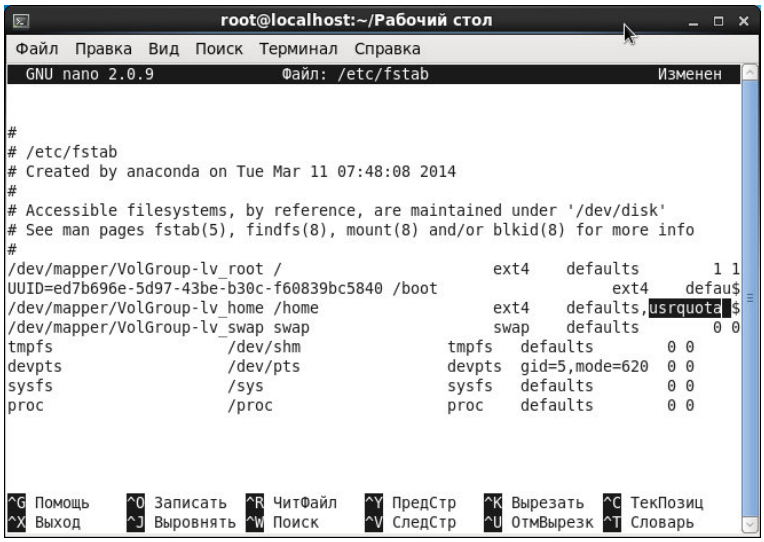


Рисунок 58 - Добавление опции монтирования usrquota

После сохранения файла соответствующая файловая система должна быть смонтирована заново, чтобы изменения вступили в силу. Прежде, чем вы перемонтируете файловую систему, убедитесь в том, что она никем не используется, а потом выполните команду в консоли:

mount -o remount /home

Далее необходимо определить какие пользователи и сколько занимают дискового пространства в данный момент. Для этого существует утилита quotacheck. Для того, чтобы построить таблицы использования дискового пространства пользовательскими файлами, необходимо запустить quotacheck с опцией -c, а также опцией, определяющей, нужно ли использовать квоты только для пользователей или только для групп, или же для тех и других одновременно:

quotacheck -cu /home

После того, как программа закончит свою работу, необходимо запустить её заново, только с другими опциями:

quotacheck -avu

Опция -a заставляет утилиту проверить все смонтированные разделы с включёнными квотами, а опция -v активирует подробный вывод сообщений о ходе работы программы.

После того, как quotacheck завершит свою работу, будет получена инициализированная база данных, содержащая всю необходимую информацию об использовании пользователями диска. Теперь необходимо настроить квоты для пользователей.

Чтобы определять дисковую квоту для каждого пользователя используется команда edquota <имя_пользователя>. Например, edquota user, в результате чего запустится текстовый редактор по умолчанию, как на рис. 59.

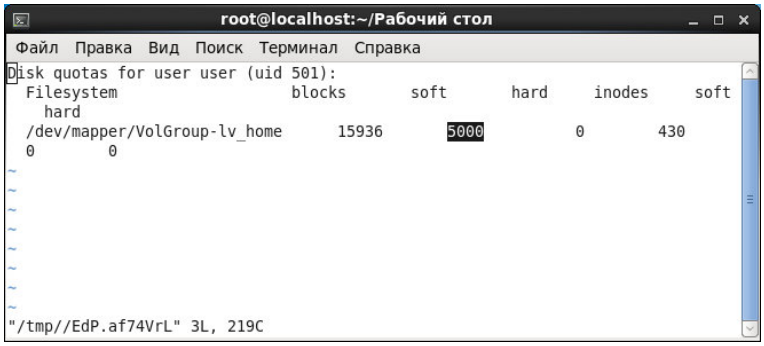


Рисунок 59 - Определение дисковой квоты для пользователя user

Всё, что вам нужно — это отредактировать hard и soft-лимиты. Hard-лимит (жёсткий лимит) определяет объём дискового пространства, больше которого пользователь не сможет занять никогда. Soft-лимит (мягкий лимит) определяет объём дискового пространства, больше которого пользователь сможет занять своими файлами в течение определённого, так называемого, grace-периода.

Чтобы убедиться в том, что квота была установлена успешно, нужно выполнить команду quota -u user, как на рис. 60.

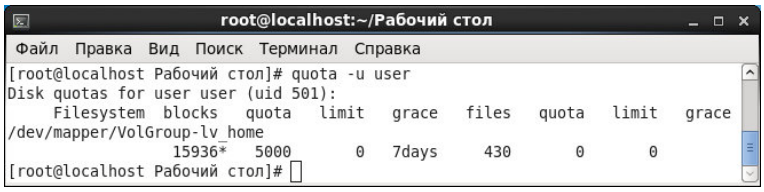


Рисунок 60 - Выполнение команды quota -u user

Для просмотра статистики по использованию дисковых квот в системе воспользуйтесь командой repquota –a, как на рис. 61.

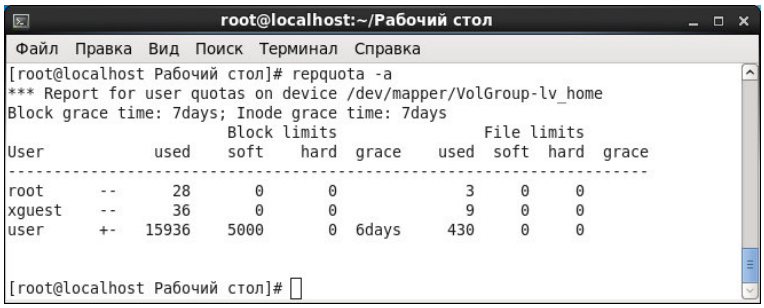


Рисунок 61 - Просмотр статистики по использованию дисковых квот

3.10 Утилита tcpdump

Для поиска и анализа подозрительной сетевой активности в системе могут использоваться анализаторы трафика. Анализатор трафика - это программа, предназначенная для прослушивания и последующего анализа сетевого трафика. Ее использование в некоторых случаях позволяет обнаружить выполнение вредоносного программного обеспечения.

Программа tcpdump - это утилита, позволяющая перехватывать и анализировать сетевой трафик, проходящий через компьютер, на котором запущена данная программа.

Для выполнения программы требуется наличие прав администратора и прямой доступ к устройству. Утилита tcpdump предназначена для отладки сетевых приложений и сетевой конфигурации в целом.

Программа состоит из двух основных частей: части захвата пакетов и части отображения захваченных пакетов, которая на уровне исходного кода является модульной, и для поддержки нового протокола достаточно добавить новый модуль.

Часть захвата пакетов при запуске передаёт «выражение выбора пакетов», идущее после всех параметров командной строки, напрямую библиотеке захвата пакетов, которая проверяет выражение на синтаксис, компилирует его во внутренний формат данных, а затем копирует во внутренний буфер программы сетевые пакеты, проходящие через выбранный интерфейс и удовлетворяющие условиям в выражении.

Часть отображения пакетов выбирает захваченные пакеты по одному из буфера, заполняемого библиотекой, и выводит их в воспринимаемом человеком виде на стандартный вывод построчно в соответствии с заданным в командной строке уровнем детальности.

Если задан подробный вывод пакетов, программа проверяет, для каждого сетевого пакета имеется ли у неё модуль расшифровки данных, и, в случае наличия соответствующей

подпрограммой извлекает и отображает тип пакета в протоколе или передаваемые в пакете параметры.

Если tcpdump запустить без параметров, будет выведена информация обо всех сетевых пакетах, как на рис. 62.

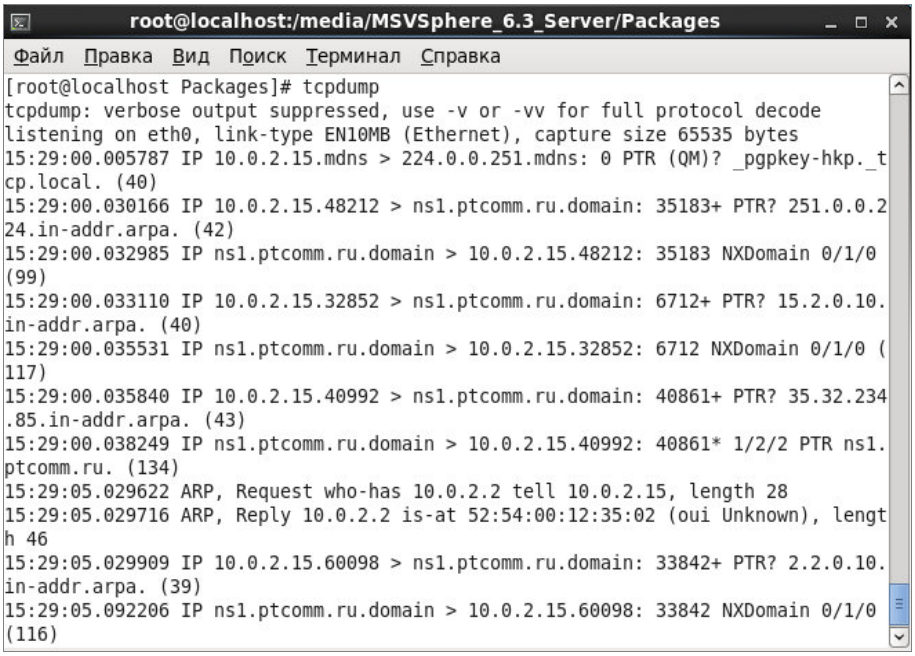


Рисунок 62 - Вывод информации о сетевых пакетах

С помощью параметра "-i" можно указать сетевой интерфейс, с которого следует принимать данные, например:

tcpdump -i eth2

Чтобы узнать получаемые или отправляемые пакеты от определенного хоста, необходимо его имя или IP-адрес указать после ключевого слова host:

tcpdump host nameofserver

Следующим образом можно узнать о пакетах, которыми обмениваются nameofserverA и nameofserverB:

tcpdump host nameofserverA and nameofserverB

Для отслеживания только исходящих пакетов от какого-либо узла нужно указать следующее:

tcpdump src host nameofserver

Только входящие пакеты:

tcpdump dst host nameofserver

Порт отправителя и порт получателя соответственно:

tcpdump dst port 80

tcpdump src port 22

Чтобы отслеживать один из протоколов TCP, UDP, ICMP, его название следует указать в команде. Использование операторов and (&&), or (||) и not (!) позволяет задавать фильтры любой сложности.

Пример фильтра, отслеживающего только UDP-пакеты, приходящие из внешней сети:

tcpdump udp and not src net localnet

Опции утилиты tcpdump:

-i **<**интерфейс**>** - задает интерфейс, с которого необходимо анализировать трафик;

-n - отключает преобразование IP в доменные имена, если указано **-**nn, то запрещается преобразование номеров портов в название протокола;

-e - включает вывод данных канального уровня (например, MAC-адреса);

-v - вывод дополнительной информации (TTL, опции IP);

-s **<**размер**>** - указание размера захватываемых пакетов (по-умолчанию - пакеты больше 68 байт);

-w **<**имя_файла**>** - задать имя файла, в который сохранять собранную информацию;

-r **<**имя_файла**>** - чтение дампа из заданного файла;

-p - захватывать только трафик, предназначенный данному узлу (по-умолчанию - захват всех пакетов, в том числе широковещательных);

-q - переводит tcpdump в "бесшумный режим", в котором пакет анализируется на транспортном уровне (протоколы TCP, UDP, ICMP), а не на сетевом (протокол IP);

-t - отключает вывод меток времени.

3.11 Утилита top

Команда top показывает список работающих в данный момент процессов и важную информацию о них, включая использование ими памяти и процессора. Этот список интерактивно формируется в реальном времени. Пример работы команды top показан на рис. 63.

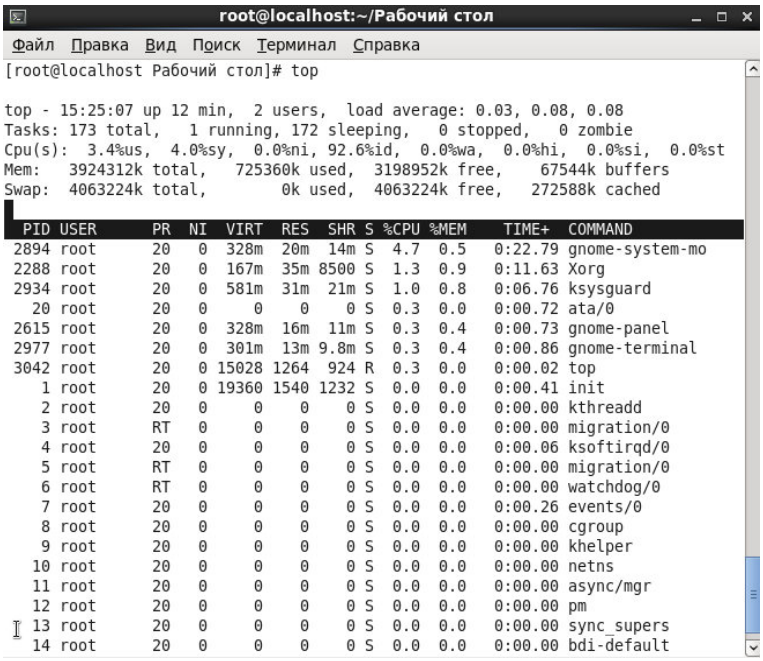


Рисунок 63 - Вывод списка работающих процессов и информации о них

Команда top имеет полезные флаги, такие как:

[Пробел] немедленно обновить содержимое экрана;

[h] вывести справку о программе;

[k] уничтожить процесс, программа запрашивает у вас код процесса и сигнал, который будет ему послан;

[n] изменить число отображаемых процессов. Вам предлагается ввести число;

[u] сортировать по имени пользователя;

[M] сортировать по объёму используемой памяти;

[P] сортировать по загрузке процессора.

Чтобы выйти из программы top, нажмите клавишу [q]. За дополнительными сведениями обратитесь к странице руководства man top.

3.12 Приложение "Системный монитор"

Графический интерфейс утилиты top реализован приложением «Системный монитор» на вкладке «Процессы» (рис. 64), которое запускается из главного меню «Приложения->Системные->Системный монитор» или вводом команды в консоли gnome-system-monitor. Системный монитор позволяет найти процесс в списке работающих процессов, а также просмотреть список всех, ваших или активных процессов.

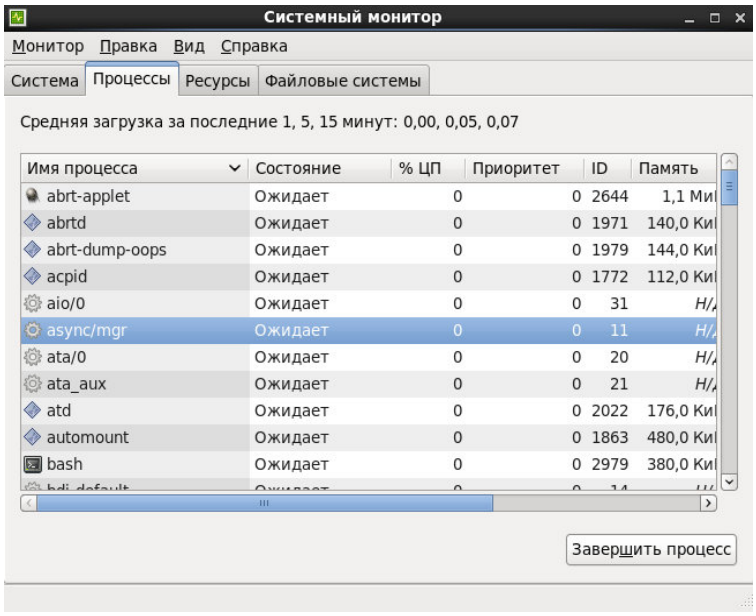


Рисунок 64 - Вкладка "Процессы" приложения "Системный монитор"

Чтобы остановить процесс, выберите его и в контекстном меню нажмите кнопку «Завершить процесс». Эта функция может пригодиться для процессов, не отвечающих на запросы пользователя.

Чтобы отсортировать информацию в определённом столбце, щелкните заголовок этого столбца. Столбец, по которому отсортирована информация, выделяется тёмно-серым цветом.

Чтобы отфильтровать процессы по принадлежности к группам "Активные процессы", "Все процессы" или "Мои процессы" - выберите пункт меню "Вид" и установите соответствующее значение (рис. 65).

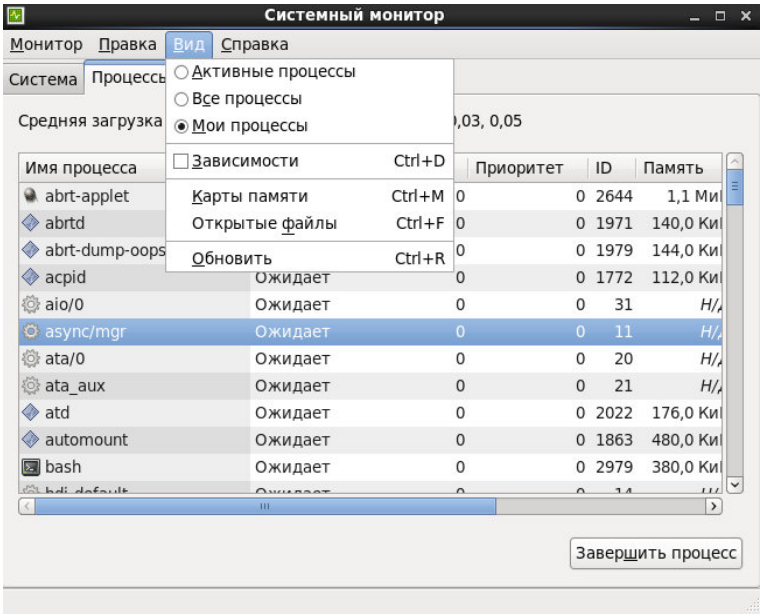


Рисунок 65 - Определение вида процессов

Чтобы получить больше информации о процессах, нужно добавить информационные поля, выбрав пункт меню "Правка->Параметры" (рис. 66).

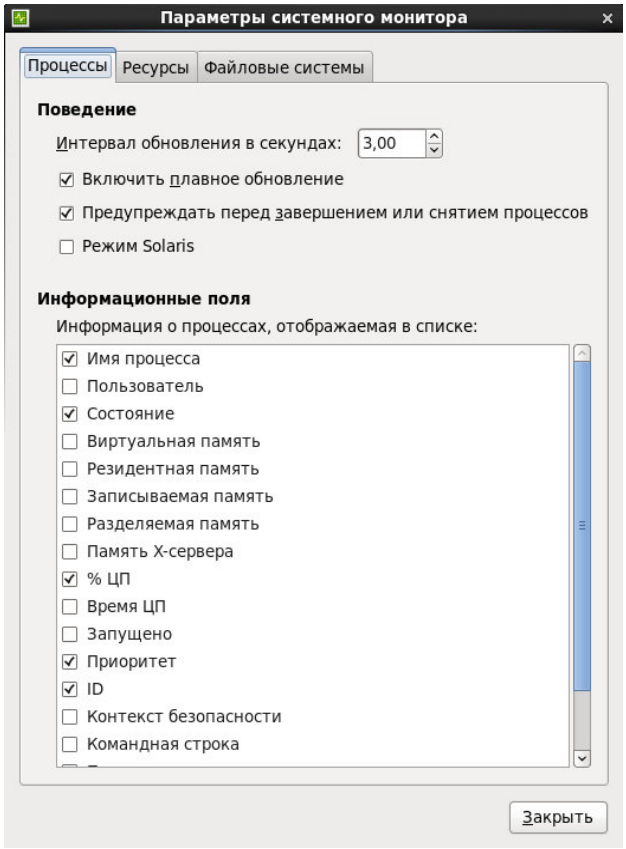


Рисунок 66 - Параметры системного монитора

На вкладке «Ресурсы» приложения «Системный монитор» (рис. 67) представлены диаграммы использования процессора, памяти, пространства подкачки и сети.

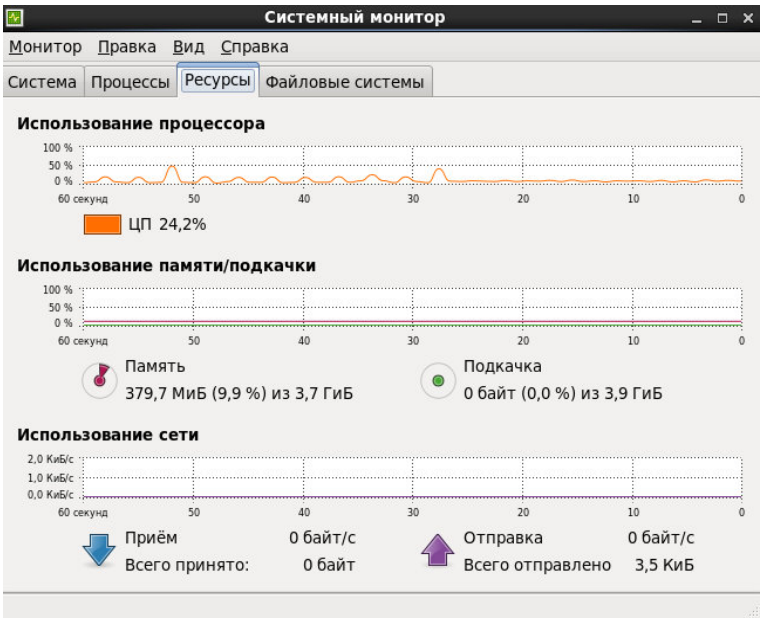


Рисунок 67 - Вкладка "Ресурсы" приложения "Системный монитор"

На вкладке «Файловые системы» приложения «Системный монитор» (рис. 68) представлен список файловых систем, включая их тип, каталог подключения, размер свободного и занятого пространства.

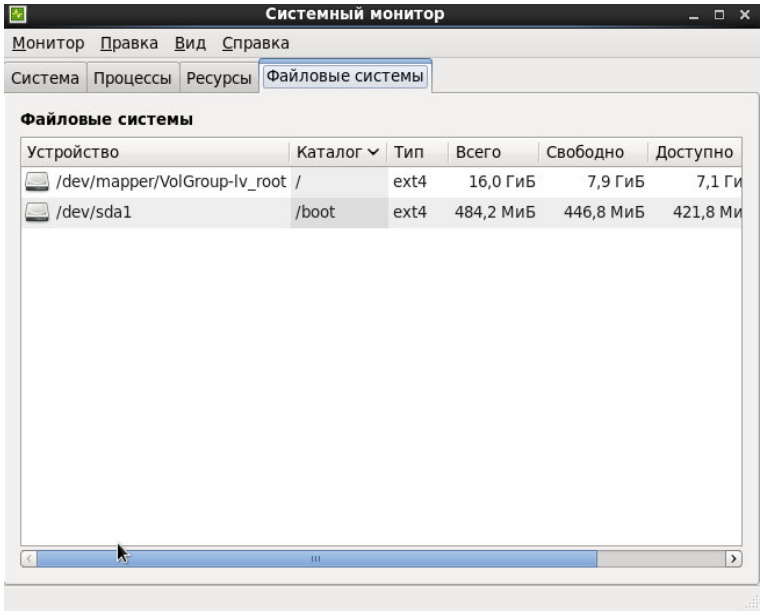


Рисунок 68 - Вкладка "Файловые системы" приложения "Системный монитор"

Чтобы получить больше информации о файловых системах, нужно добавить информационные поля, выбрав пункт меню "Правка->Параметры", перейдя на вкладку "Файловые системы" (рис. 69). Чтобы в список были добавлены все файловые системы, нужно установить галочку в поле "Отображать все файловые системы".

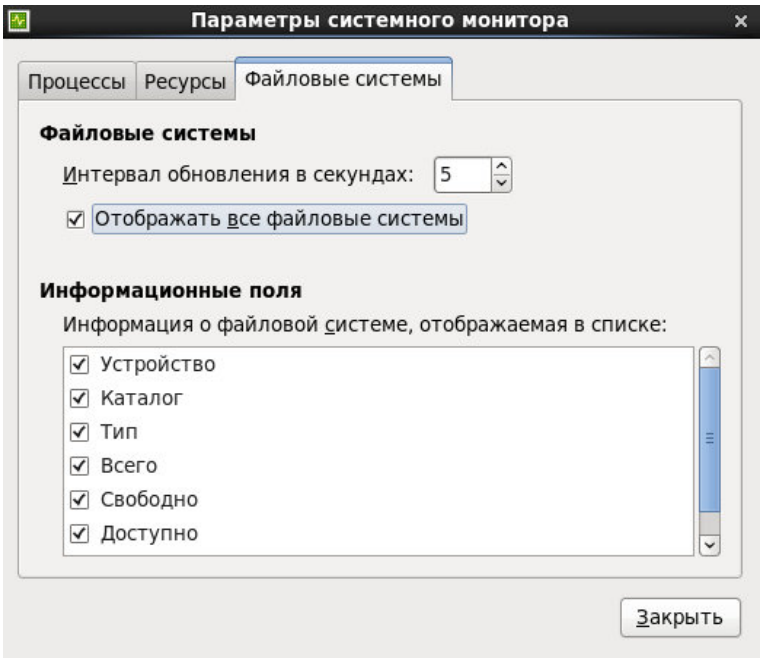


Рисунок 69 - Параметры файловых систем

3.13 Утилита free

Команда free показывает полный объём физической памяти и раздела подкачки в системе, а также объём используемой, свободной, разделяемой памяти, размер буферов ядра и кэша (рис. 70).

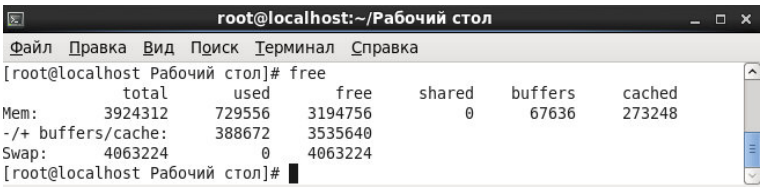


Рисунок 70 - Вывод полного объёма физической памяти и раздела подкачки в системе

Команда free -m выводит ту же информацию в мегабайтах, что облегчает её восприятие (рис. 71).

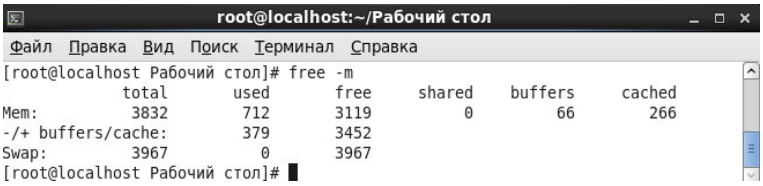


Рисунок 71 - Вывод полного объёма физической памяти и раздела подкачки в системе в мегабайтах

Если вы предпочитаете использовать графический интерфейс утилиты free, вы можете использовать приложение «Системный монитор» на вкладке «Ресурсы», описание которой приведено в подразделе 3.12.

3.14 Утилиты df и du

Команда df выводит отчёт об использовании дискового пространства. Если вы выполните в приглашении оболочки команду df, то на экране появится отчёт (рис. 72).

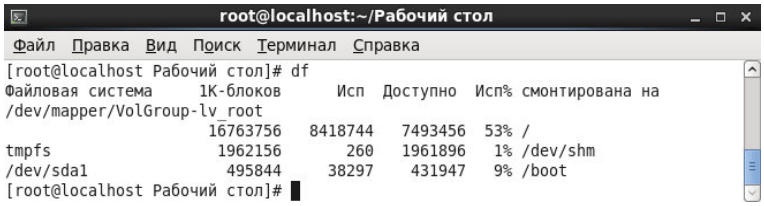


Рисунок. 72 - Вывод отчёта об использовании дискового пространства

По умолчанию эта программа показывает размер раздела в килобайтных блоках, а также объём используемого и свободного места на диске в килобайтах. Чтобы получить эту информацию в мегабайтах и гигабайтах, выполните команду df -h. Параметр -h включает формат, воспринимаемый человеком (Human-readable format), как на рис. 73.

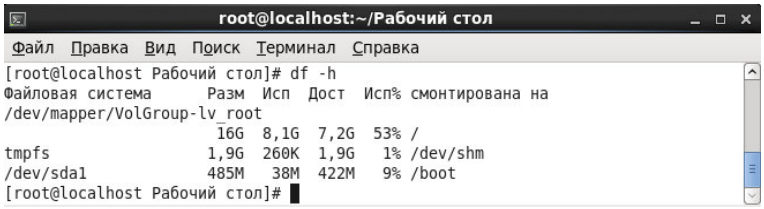


Рисунок 73 - Вывод отчёта об использовании дискового пространства

В списке смонтированных разделов присутствует запись /dev/shm. Эта запись представляет файловую систему виртуальной памяти.

Команда du выводит на экран приблизительный объём, занимаемый файлами каталога на диске. Если вы введёте в приглашении оболочки команду du, в списке будет показан объём дискового пространства, занимаемого каждым из подкаталогов (рис. 74). В последней строке этого списка также будет показан суммарный размер текущего каталога и его подкаталогов. Если вы не хотите видеть размеры всех подкаталогов, введите команду du -hs, чтобы увидеть

только общий размер каталога в легко воспринимаемом формате. Выполните команду du --help, чтобы узнать о дополнительных параметрах.

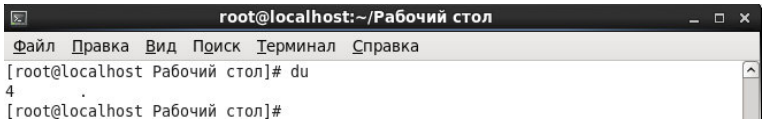


Рисунок 74 - Вывод приблизительного объёма,
занимаемого файлами каталога на диске

3.15 Программа OProfile

OProfile — это средство мониторинга производительности системы, оказывающее минимальное влияние на её работу. Эта программа использует встроенные в процессор аппаратные возможности мониторинга производительности и собирает сведения о ядре и исполняемых модулях, в частности, статистику использования памяти, число обращений к кэшу второго уровня и полученных аппаратных прерываний.

При настройки OProfile необходимо выбрать, включить мониторинг ядра или нет с помощью утилиты opcontrol. Чтобы включить мониторинг ядра, выполните команду:

opcontrol --setup --vmlinux=/usr/lib/debug/lib/modules/`uname - r`/vmlinux

Если в вашей системе отсутствуют соответствующие папки или файл, то выполните предварительно команды, как на рис. 75. А потом включите мониторинг ядра.

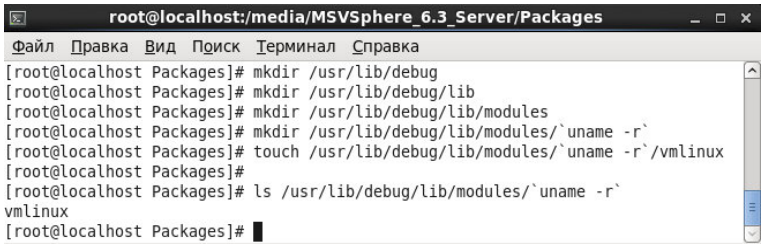


Рисунок 75 - Выполнение предварительных мер

Чтобы отключить мониторинг ядра необходимо выполнить команду:

opcontrol --setup --no-vmlinux

С помощью счётчиков процессора OProfile отслеживает определённые события. В разных процессорах доступно разное число счётчиков.

Число одновременно отслеживаемых событий определяется числом счётчиков процессора. Для определения числа доступных счётчиков, необходимо выполнить следующую команду cat /dev/oprofile/cpu_type, как на рис. 76.

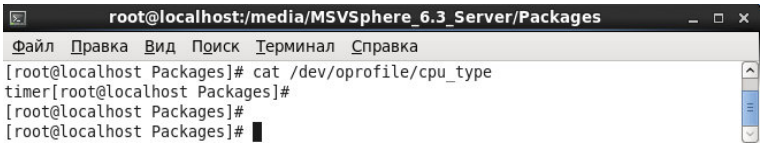


Рисунок 76 - Определение числа доступных счётчиков

Тип timer применяется в случае, если у процессора нет поддерживаемых аппаратных средств мониторинга производительности, а значит и назначить события для процессора нельзя. Вместо счётчиков используется прерывание по таймеру.

Чтобы определить, какие события можно отслеживать, необходимо выполнить команду op_help, результаты команды зависят от типа процессора.

Чтобы назначить событие для счётчика и частоту выборки, необходимо выполнить команду:

opcontrol --event=<название_события>:<число_событий_между_выборками>

Чтобы запустить мониторинг системы с помощью OProfile, необходимо выполнить команду opcontrol –start (рис. 77).

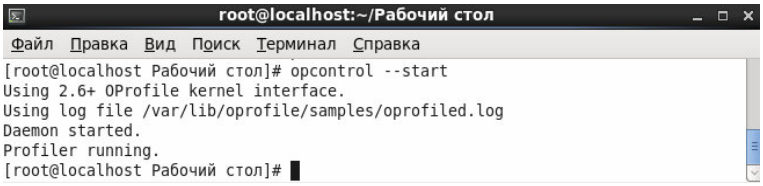


Рисунок 77 - Запуск OProfile

Чтобы остановить мониторинг, выполните от имени root команду opcontrol --shutdown (рис. 78).

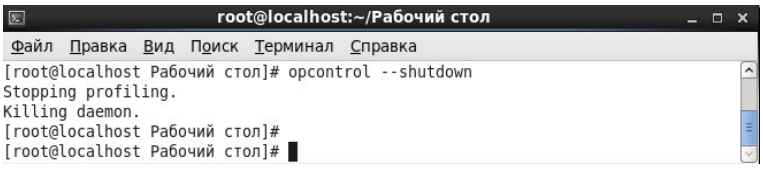


Рисунок 78 - Остановка мониторинга

Для анализа данных используются утилиты opreport и opannotate. Программа opreport предоставляет отчет по всем отслеживаемым исполняемым модулям (рис. 79).

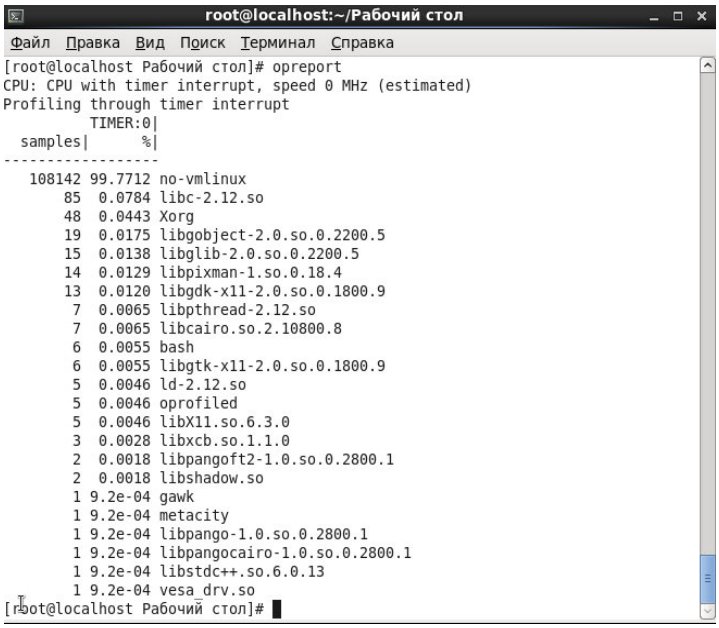


Рисунок 79 - Сводка по всем отслеживаемым исполняемым модулям

Для каждого исполняемого модуля отводится отдельная строка. В первом столбце указывается число выборок, сделанных для исполняемого модуля. Во втором столбце указывается процентное отношение этого числа к общему числу выборок. В третьем столбе указывается имя исполняемого модуля.

Чтобы вывести более подробный отчет, необходимо выполнить команду opreport -l -d, фрагмент результата показан на рис. 80.

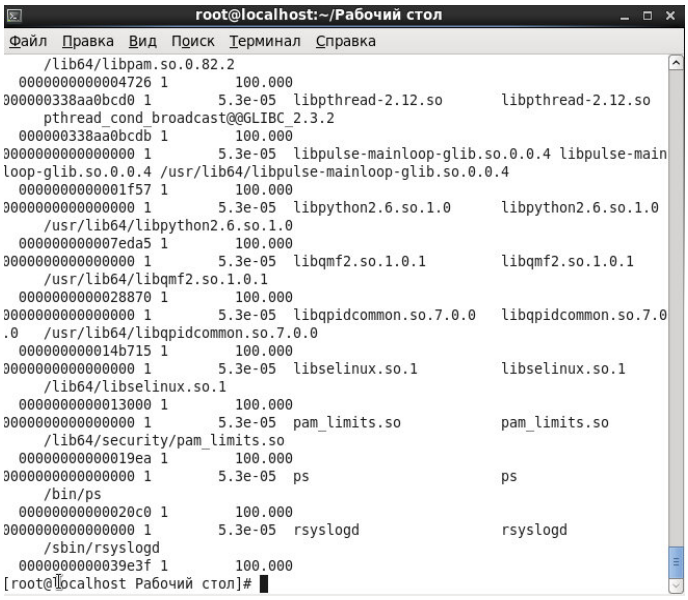


Рисунок 80 - Вывод данных выборки командой opreport -l -d

Утилита opannotate предоставляет отчет из выборок, полученных при выполнении конкретных инструкций:

opannotate --search-dirs <каталог_анализируемого_исходного_кода> --source <исполняемая_программа>

Чтобы запустить графический интерфейс OProfile, выполните команду oprof_start (рис. 81).

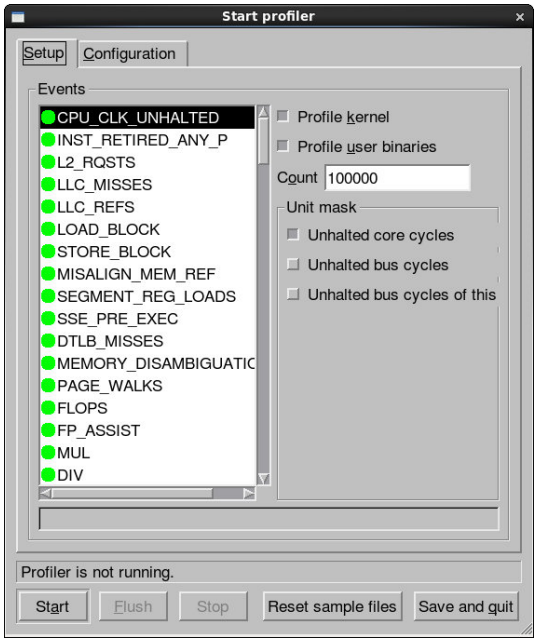


Рисунок 81 - Графический интерфейс утилиты OProfile, вкладка "Setup"

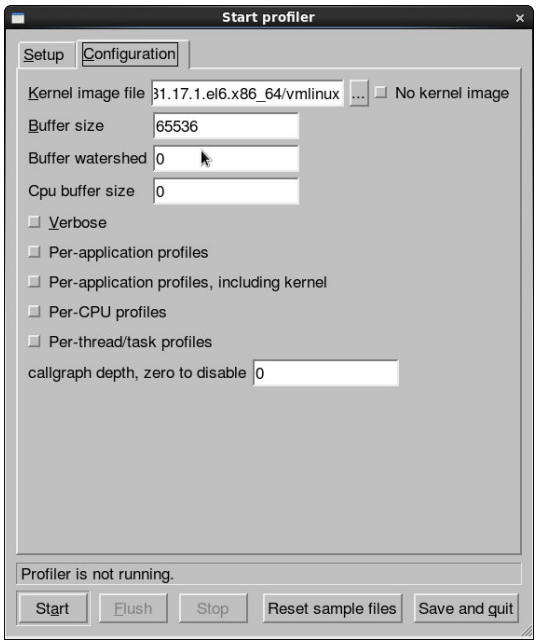


Рисунок 82 - Графический интерфейс утилиты OProfile, вкладка "Configuration"

На вкладке "Setup" можно задать параметры событиям, для этого нужно выбрать событие в списке и указать необходимые параметры. Параметр "Profile kernel" (Профилировать ядро) необходим, чтобы учитывать выборки текущего события в режиме ядра. Параметр "Profile user binaries" (Профилировать двоичный код пользователя) предназначен для того, чтобы учитывать выборки текущего события в пользовательском режиме. В поле "Count" (Счётчик) выводится частота выборки текущего события. Если для события определены маски, то они отображаются в области "Unit Masks". Чтобы задать маску для события, нужно отметить расположенный рядом с ней флажок.

В текстовой области под списком появляется короткое описание события.

Чтобы включить мониторинг ядра, на вкладке "Configuration" укажите имя и расположения файла vmlinux для отслеживаемого ядра в текстовом поле «Файл» образа ядра (Kernel image file). Чтобы OProfile не выполнял мониторинг ядра, отметьте флажок "No kernel image" (Без образа ядра). Так же можно указать соответствующие размеры буферов.

Если установлен флажок "Verbose" (Подробно), в журнал демона oprofiled будет выводиться дополнительная информация. Флажок "Per-application profiles" отвечает за выбор профилей по приложениям, "Per-application profiles, including kernel" - выбор профилей по приложениям, включенным в ядро, "Per-CPU profiles" - выбор профилей по CPU, "Per-thread/task profiles" - выбор профилей по потокам или задачам.

Изменив параметры, сохраните их, нажав кнопку "Save and quit" (Сохранить и выйти). При этом параметры записываются в файл /root/.oprofile/daemonrc и приложение завершает работу. Чтобы запустить OProfile в графическом интерфейсе, нажмите кнопку «Start» (Запустить). Чтобы остановить его, нажмите «Stop» (Остановить). При завершении этого приложения OProfile не прекращает сбор данных. Чтобы принудительно сбросить данные в файлы с выборками нажмите кнопку «Flush» (Сбросить данные). Этот флажок соответствует команде opcontrol --dump.

3.16 Приложение "Wireshark Network Analizer"

Wireshark Network Analizer - это программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других. Она имеет графический пользовательский интерфейс и вызывается из меню системы "Приложения->Интернет->Wireshark Network Analyzer" (рис. 83). Функциональность, которую предоставляет tcpdump, очень схожа с возможностями программы Wireshark.

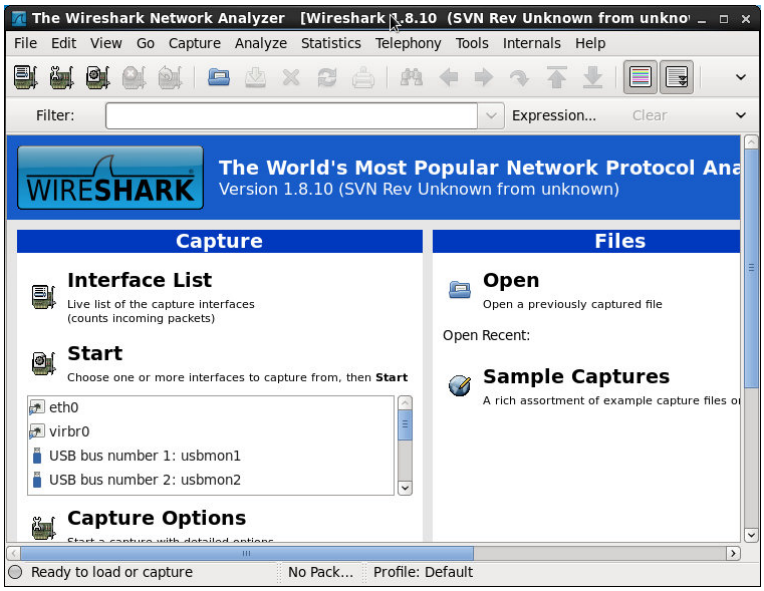


Рисунок 83 - Окно приложения "The Wireshark Network Analyzer"

Приложение Wireshark имеет больше возможностей по сортировке и фильтрации информации. Программа позволяет пользователю просматривать весь проходящий по сети трафик в режиме реального времени, переводя сетевую карту в так называемый неразборчивый режим (promiscuous mode).

Wireshark - это приложение, которое знает структуру самых различных сетевых протоколов, умеет работать с множеством форматов входных данных и позволяет разобрать сетевой пакет, отображая значение каждого поля протокола любого уровня.

Для начала сборки перехваченных программой пакетов сообщений по сети выберите пункт главного меню "Capture->Interfaces" или кнопку на верхней панели инструментов "List the available capture interfaces" – после этого на экране появится диалоговое окно, как на рис. 84.

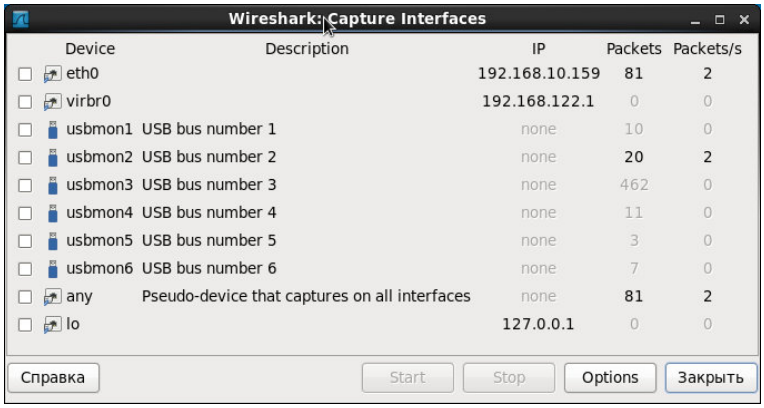


Рисунок 84 - Окно настройки интерфейсов

С помощью кнопки "Options" возможна установка желаемых параметров работы программы (рис. 85). В открывшемся окне настройки разделены на пять областей: "Capture" (Захват), "Capture File(s)" (Захват файлов), "Stop Capture..." (Остановить захват), "Display Options" (Показать настройки), "Name Resolution" (Разрешение имен).

В области "Capture" отображается список интерфейсов, двойным щелчком по которым можно задать их основные свойства (рис. 86). В открывшемся окне можно указать название интерфейса (Interface), тип заголовка канального уровня (Link-layer header type), по умолчанию Ethernet, размер буфера в мегабайтах (Buffer size). Если необходимо, выбрать захват пакетов в беспорядочном режиме (Capture packets in promiscuous mode), захват пакетов в режиме контроля (Capture packets in monitor mode), ограничение каждого пакета в байтах (Limit each packet to ... bytes). Так же можно указать фильтр захвата (Capture Filter).

В области "Capture File(s)" нужно указать путь к файлу (File), установить галочку на использование нескольких файлов (Use multiple files). Если использована опция "Use multiple files", то нужно указать еще ограничение в мегабайтах или минутах для каждого следующего файла (Next file every), количество файлов для кольцевого буфера (Ring buffer with ... files), количество файлов, после которых захват будет остановлен (Stop capture after ... file(s)).

В области "Stop Capture..." нужно указать ограничение в количестве пакетов (... after packet(s)), мегабайт (... after megabyte(s)) и минут (... after minute(s)).

В области "Display Options" нужно выбрать, нужны ли следующие опции: обновление списка пакетов в режиме реального времени (Update list of packets in real time), автоматическая прокрутка во время захвата (Automatic scrolling in live capture), скрыть информационный диалог о захвате (Hide capture info dialog).

В области "Name Resolution" нужно указать, будут ли использоваться следующие опции: включить разрешение MAC имени (Enable MAC name resolution), включить разрешение имен сети (Enable network name resolution), включить разрешение транспортных имен (Enable transport name resolution).

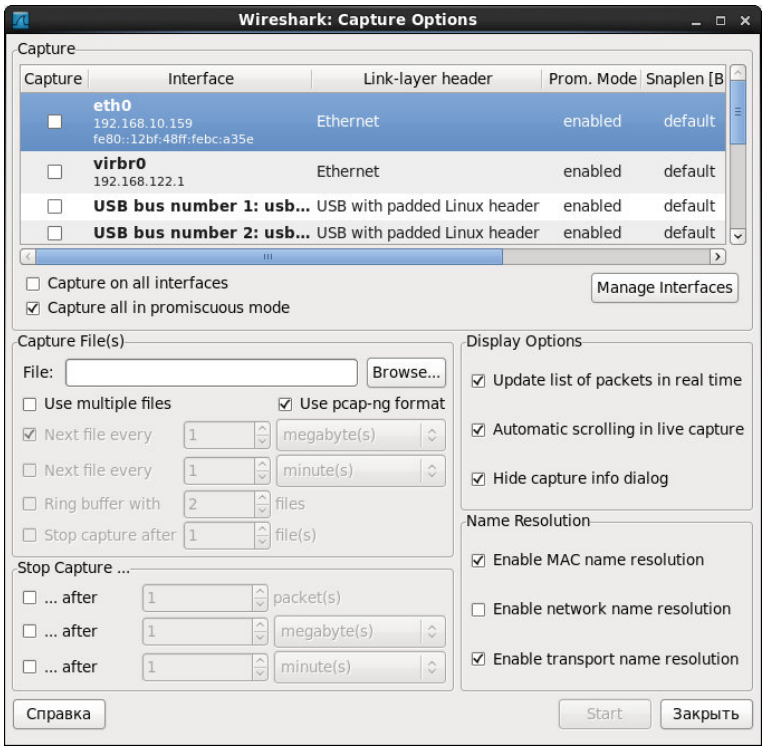


Рисунок 85 - Окно настройки параметров работы программы

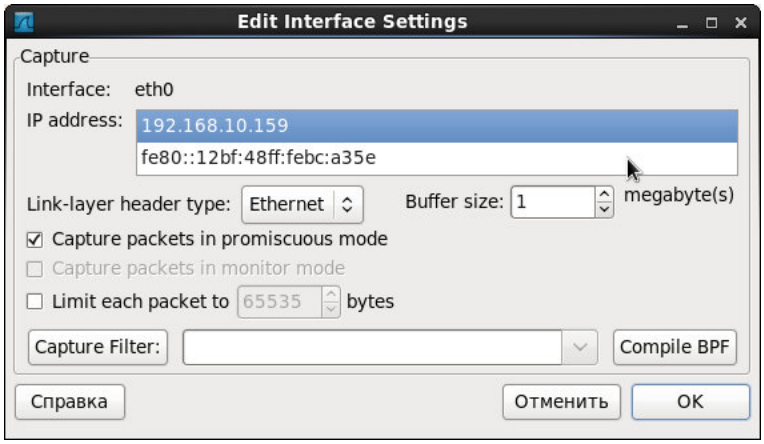


Рисунок 86 - Окно настройки интерфейса eth0

Выберем интерфейс eth0. Для того чтобы начать процедуру захвата, необходимо нажать кнопку Start, после чего интерфейс программы примет вид, как на рис. 87. Для выбора настроек интерфейса нужно выбрать пункт меню "Capture->Options", для остановки захвата - "Capture->Stop", для перезапуска - "Capture->Restart", для фильтрации запроса - "Capture->Capture Filters...".

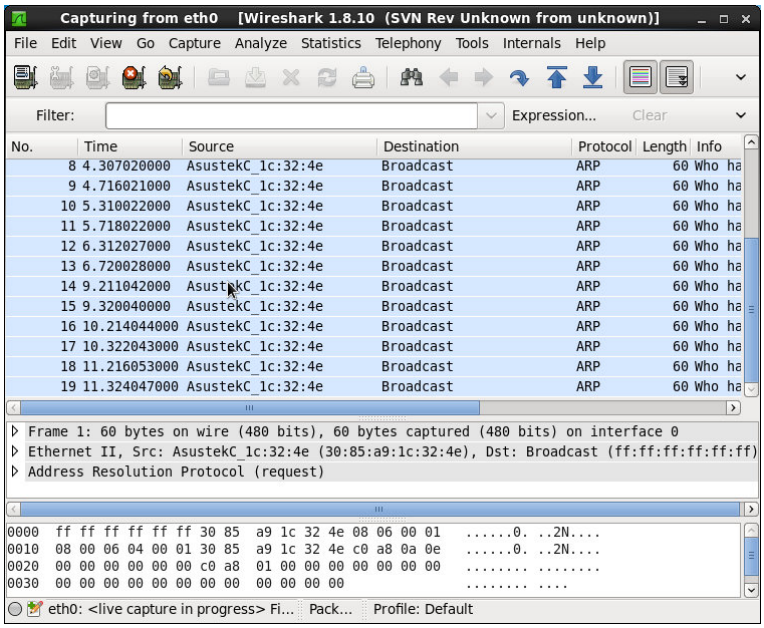


Рисунок 87 - Захват пакетов для интерфейса eth0

На рис. 87 видно, что окно Wireshark включает в себя три области просмотра с различными уровнями детализации. Верхнее окно содержит список собранных пакетов с кратким описанием, в среднем окне показывается дерево протоколов, инкапсулированных в кадр. Ветви дерева могут быть раскрыты для повышения уровня детализации выбранного протокола. Последнее окно содержит дамп пакета в шестнадцатеричном или текстовом представлении.

В верхней области данные разделены на семь колонок – номера пакета в списке собранных, временная метка, адреса и номера портов отправителя и получателя, тип протокола, длина и краткая информация о пакете.

Выбрав необходимый пакет из списка, мы можем просмотреть содержимое средней панели. В ней представлено дерево протоколов для пакета. Дерево отображает каждое поле и его значение для заголовков всех протоколов стека.

В программе Wireshark можно выбрать фильтрацию списка пакетов, например по IP-адресам, кликнув правую кнопку мыши, в контекстном меню нажать "Conversation filter->IP".

В результате получим окно, как на рис. 88, с отфильтрованными пакетами.

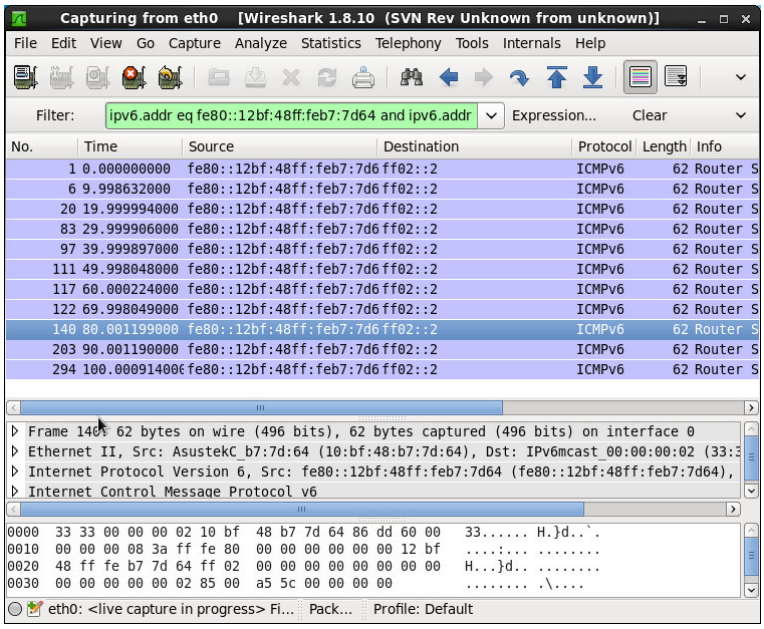


Рисунок 88 - Результат фильтрации по IP

Для того, чтобы найти пакет среди общего списка, нужно выбрать пункт меню "Edit->Find Packet..." (рис. 89). Выбрать предмет поиска: показать фильтр (Display filter), шестнадцатиричное значение (Hex value) или строка (String) и указать сам фильтр.

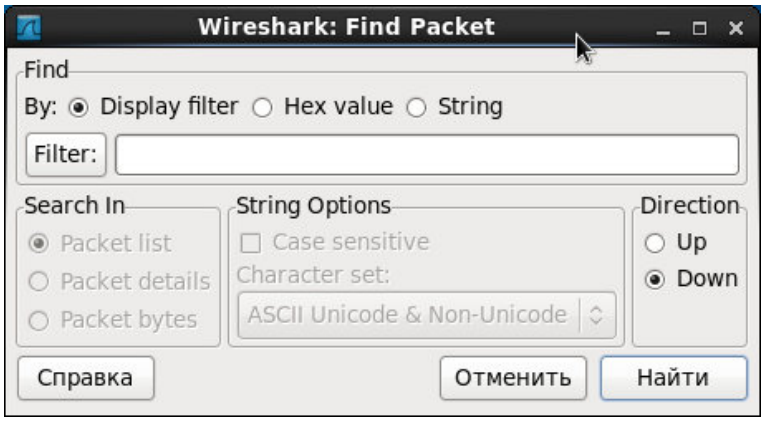


Рисунок 89 - Параметры поиска пакета

Wireshark предоставляет возможность сохранять файлы данных на жесткий диск. Для этого необходимо в главном меню программы выбрать "File->Export Objects" и вариант сохранения данных. Например, если выбрать сохранение объекта HTTP, то можно сохранить объекты, найденные в Интернете, выбрав в появившемся списке необходимый файл и нажав "Save As", сохранить на диск.

Программа обладает большим набором вывода статистических данных о захваченных пакетах сообщений. Так можно вывести общую таблицу иерархии протоколов при помощи пункта главного меню "Statistics>Protocol Hierarchy" (рис. 90).

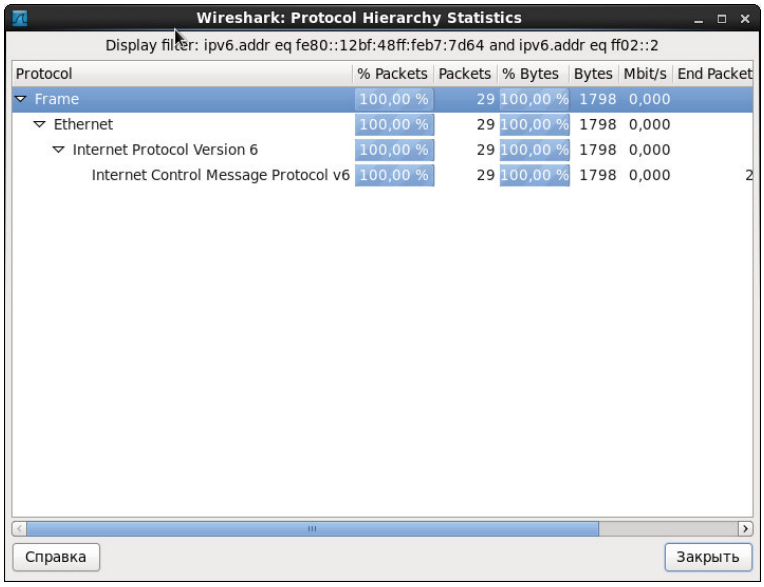


Рисунок 90 - Общая таблица иерархии протоколов

Для наглядного представления результатов выполнения захвата пакетов и сборки кадров в программе имеется возможность отображения данной информации в виде графика передачи пакетов в единицу времени. Для отображения данного графика необходимо воспользоваться пунктом главного меню "Statistics>IO Graphs" (рис. 91).

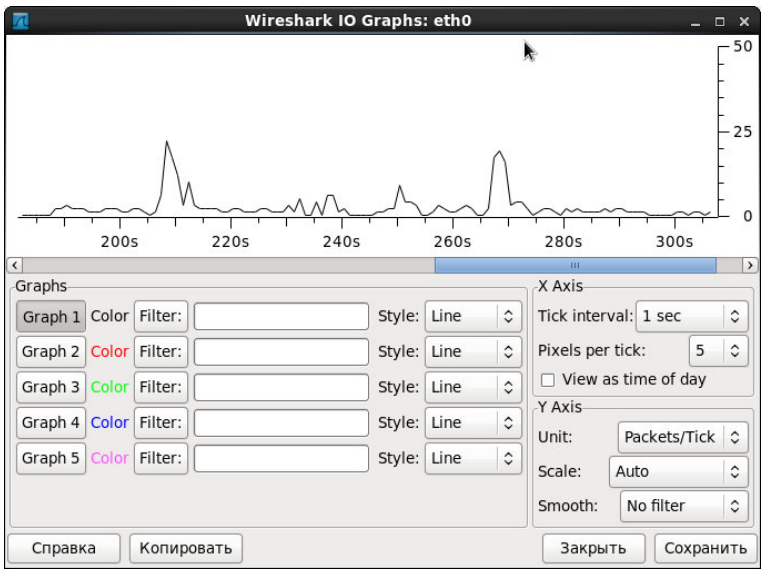


Рисунок 91 - График передачи пакетов в единицу времени

Более подробную информацию о возможностях программы Wireshark можно найти на ее официальном сайте.

3.17 Приложение "KDiskFree"

Приложение "KDiskFree" отображает список доступных файловых устройств, вместе с информацией о них: пиктограмма, отображающая тип устройства, устройство, тип файловой системы, размер, точка монтирования, свободное и занятое пространство, графически представленное использование диска. Приложение вызывается из пункта меню "Приложения"-> "Системные" ->"KDiskFree" (рис 92).

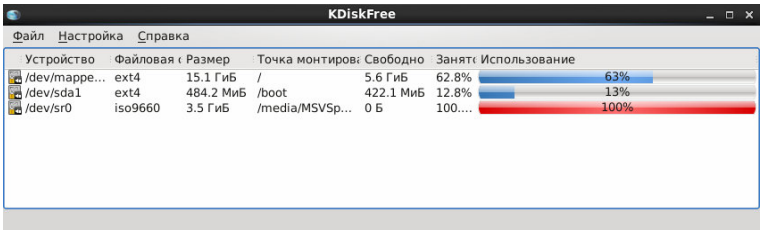


Рисунок 92 - Приложение "KDiskFree"

Для настройки "KDiskFree" выберите пункт меню "Настройка"->"Настроить KDiskFree...", в результате чего откроется окно (рис. 93), содержащее две вкладки "Параметры" и "Команды".

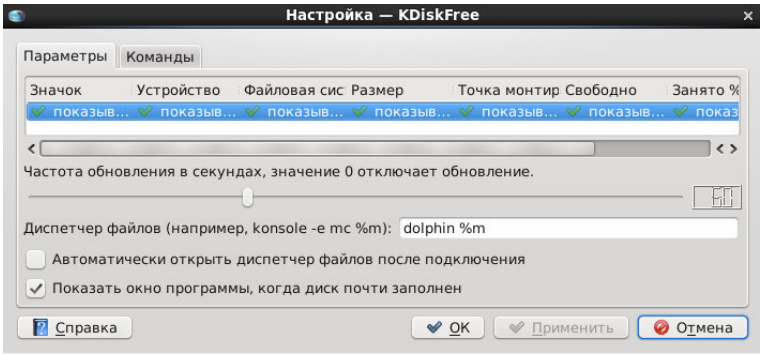


Рисунок 93 - Окно настройки приложения "KDiskFree"

На вкладке "Параметры" можно настроить отображение информации, нажимая на слова "показывать" или "скрыть". Смена частоты обновления контролируется перемещением ползунка. Так же существуют два флажка, один контролирует открытие диспетчера файлов после подключения, а другой - появление окна, когда устройство заполнено до критического уровня.

На вкладке "Команды" (рис. 94) можно указать команды подключения и отключения для выбранного устройства.

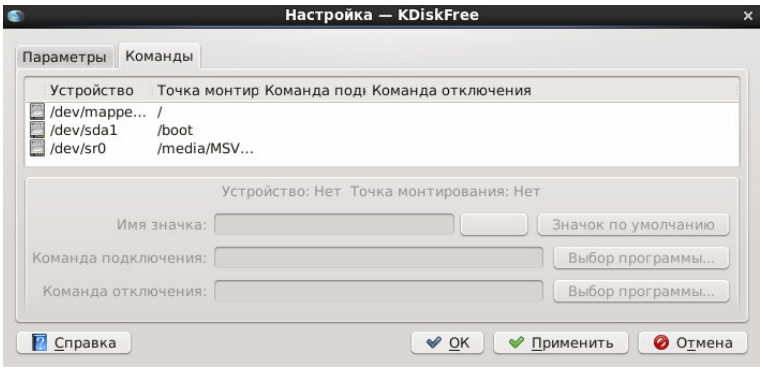


Рисунок 94 - Вкладка "Команды" приложения "KDiskFree"

3.18 Приложение "KSystemLog"

Мониторинг (просмотр, анализ) результатов регистрации событий аудита осуществляется с помощью приложения "KsystemLog", которое запускается из главного меню "Приложения–>Системные–>KsystemLog" (рис. 95).

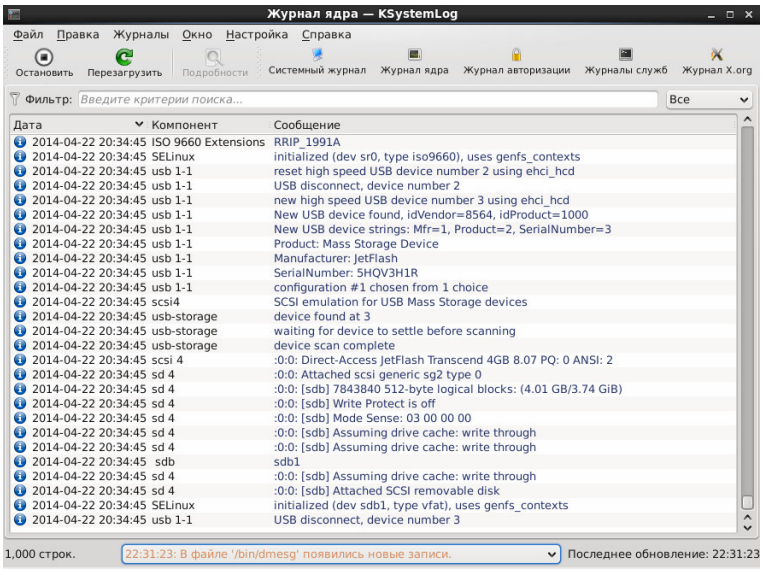


Рисунок 95 - Приложение "KsystemLog"

"KsystemLog" поддерживает вкладки, которые открываются нажатием Ctrl+T или пунктом меню «Окно»–>«Новая вкладка». Таким образом, можно просматривать несколько журналов одновременно в одном окне на разных вкладках.

Чтобы просмотреть подробности сообщения в журнале нужно выбрать пункт меню "Правка"->"Подробности", в результате чего откроется окно, например, как на рис. 96.

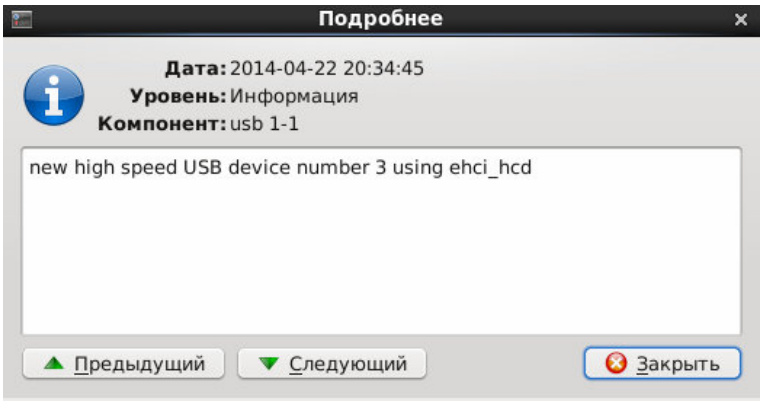


Рисунок 96 - Подробности о сообщении в журнале

Если журналы в вашей системе находятся не по стандартным путям, то настроить их можно воспользовавшись пунктом меню "Настройка"->"Настроить KsystemLog...", в результате чего откроется окно, как на рис. 97.

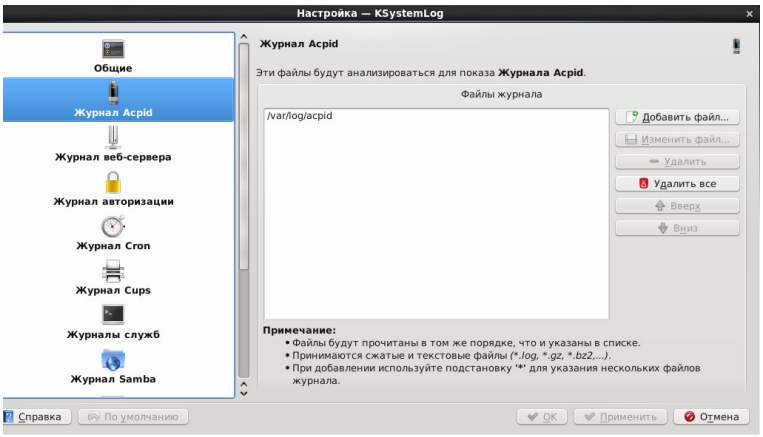


Рисунок 97 - Окно настройки "KsystemLog"

3.19 Приложение "Анализатор использования дисков"

Приложение "Анализатор использования дисков" представляет собой графическое средство анализа использования дисков и вызывается пунктом меню "Приложения"-> "Системные"-> "Анализатор использования дисков" (рис. 98). Анализатор использования дисков может изучать как полное дерево файловой системы, так и ее отдельные папки (локальные или удаленные). Кроме того, он может строить полную графическую карту для каждой выбранной папки.

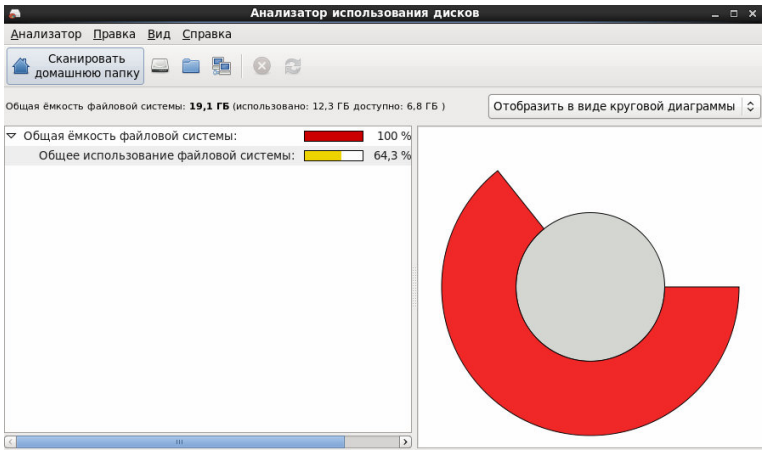


Рисунок 98 - Приложение "Анализатор использования дисков"

Чтобы запустить полное сканирование файловой системы, необходимо выбрать пункт меню "Анализатор"->"Сканировать файловую систему". После завершения сканирования будет построено полное дерево файловой системы, например, как на рис. 99. Анализатор использования дисков в дереве каталогов показывает объем занятого места на диске.

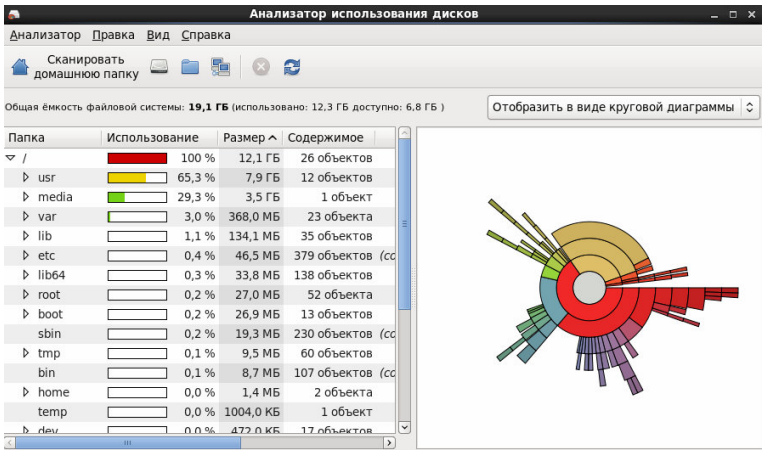


Рисунок 99 - Сканирование файловой системы

Чтобы выполнить сканирование отдельной папки, нужно выбрать пункт меню "Анализатор"->"Сканировать папку...".

Для сканирования удаленной папки, выбрать "Анализатор"->"Сканировать удаленную папку...", в результате чего появится окно "Соединиться с сервером" (рис. 100), в котором необходимо выбрать через какой протокол будет осуществляться подключение к серверу (SSH, FTP, SMB, HTTP и HTTPS).

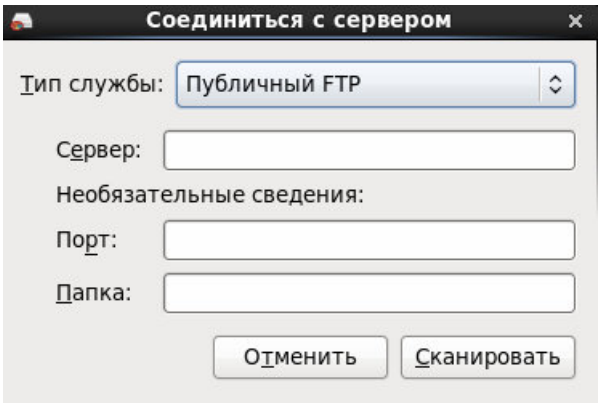


Рисунок 100 - Окно соединения с сервером

Чтобы изменить параметры анализатора использования дисков, необходимо выбрать пункт меню приложения "Правка"->"Параметры" (рис. 101).

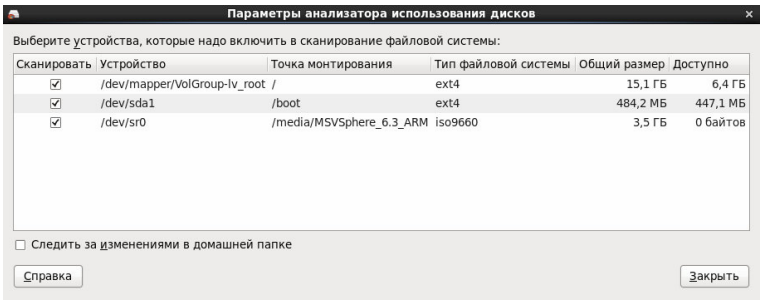


Рисунок 101 - Параметры анализатора использования дисков

В первой части окна параметров перечислены все найденные присоединенные устройства. Устройство будет сканироваться лишь в том случае, если напротив него стоит флажок.

Сканирование можно выполнять в виде древовидной карты (рис. 102) или круговой диаграммы (рис. 99). Карты основаны на концепции treemap, разработанной Беном Шнайдерманом, а круговая диаграмма - это графическое представление использования диска конкретной папкой.

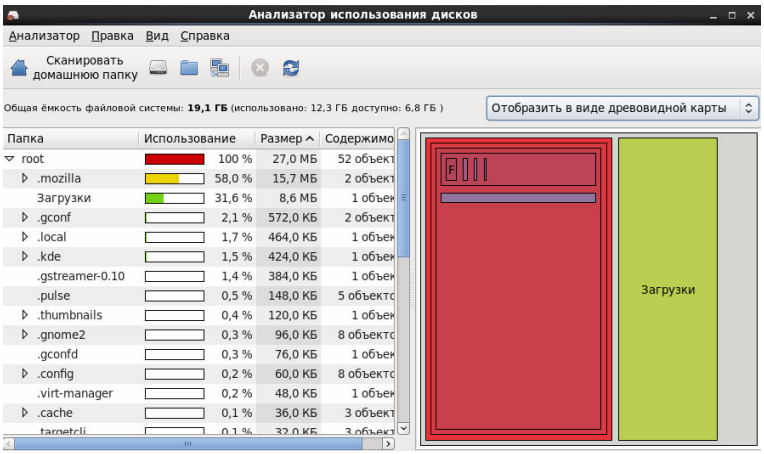


Рисунок 102 - Сканирование в виде древовидной карты

3.20 Приложение "Диагностика проблем SELinux"

Приложение "Диагностика проблем SELinux" ("SELinux Alert Browser") предназначено для диагностики проблем отказа в доступе SELinux. Вызывается из меню "Приложения-> Системные-> Диагностика проблем SELinux" (рис. 103).

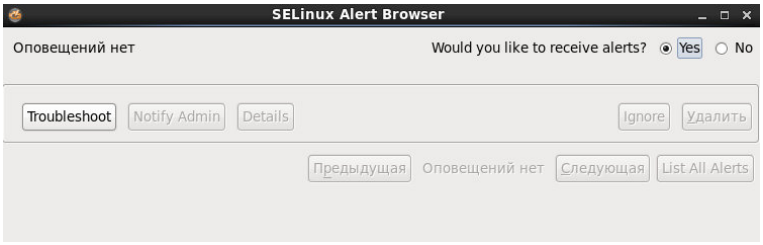


Рисунок 103 - Приложение "Диагностика проблем SELinux"

При возникновении SELinux ошибки появляется окно с информацией о ней (рис. 104).

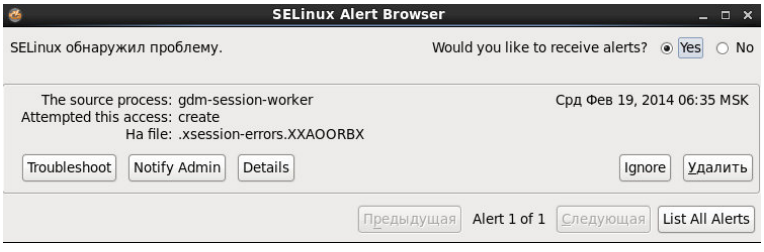


Рисунок 104 – Информация об ошибке

Для просмотра описания данной ошибки необходимо нажать на кнопку «Details» (детализация) (рис. 105), для устранения неполадок - кнопку «Troubleshoot» (устранение неполадок), для уведомления администратора - кнопку «Notify Admin» (уведомление администратора). Для просмотра списка всех ошибок используется кнопка «List All Alerts» (список всех ошибок) (рис. 106). Полученную ошибку можно проигнорировать - кнопка «Ignore» или удалить кнопкой «Удалить».

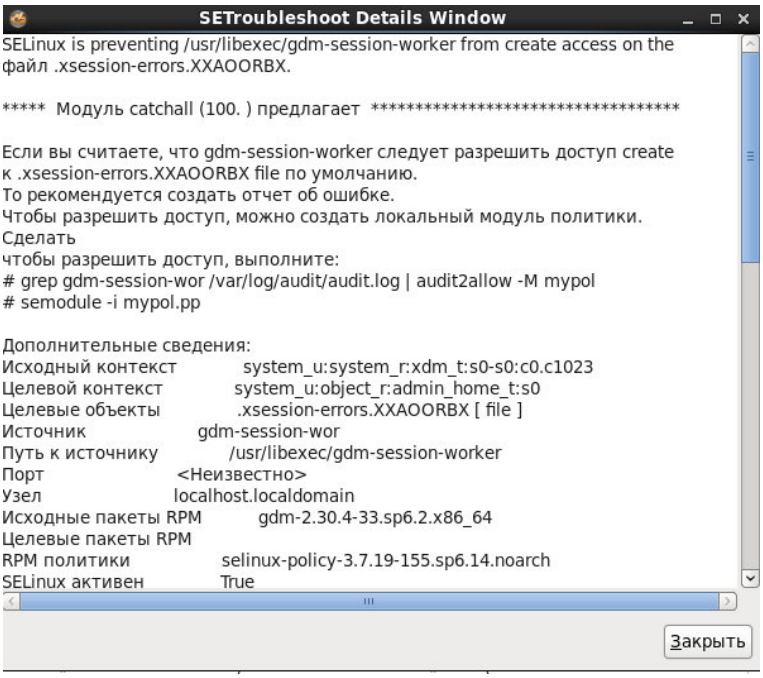


Рисунок 105 – Пример детализации ошибки

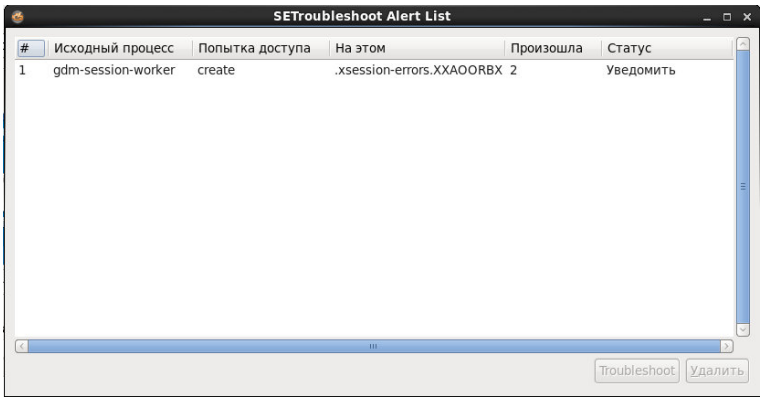


Рисунок 106 – Список ошибок

Изм.	Лист	№ докум	Подп	Дата

4 СТИРАНИЕ ИНФОРМАЦИИ

4.1 Основные сведения

Средства защиты информации в системе МСВСфера 6.3 АРМ предоставляют возможность уничтожения (стирания) данных и остаточной информации.

Вышеперечисленная возможность реализуются с помощью следующих программных средств:

- утилита dd;
- утилита shred;
- утилита scrub.

4.2 Утилиты dd и shred

При удалении файла посредством команды rm или с помощью файлового менеджера, содержимое файла не уничтожается, удаляется лишь его индекс, а пространство, которое занимал файл, помечается системой как свободное для записи.

Утилита shred случайными числами заполняет место, занятое файлом и даже восстановив удалённый файл, его невозможно будет прочитать.

Создадим файл 1.txt командой:

touch 1.txt

Заполним файл нулями с помощью утилиты dd, как показано на рис. 107.

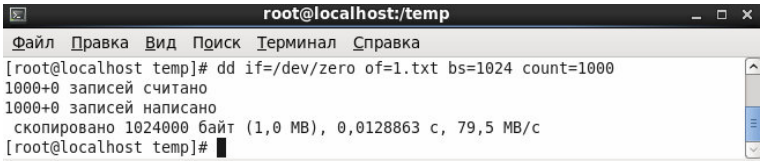


Рисунок 107 - Заполнение файла нулями с помощью утилиты dd

Представим файл как блочное устройство с помощью следующей команды:

losetup /dev/loop0 1.txt

Создадим файловую структуру на блочном устройстве, как на рис. 108.

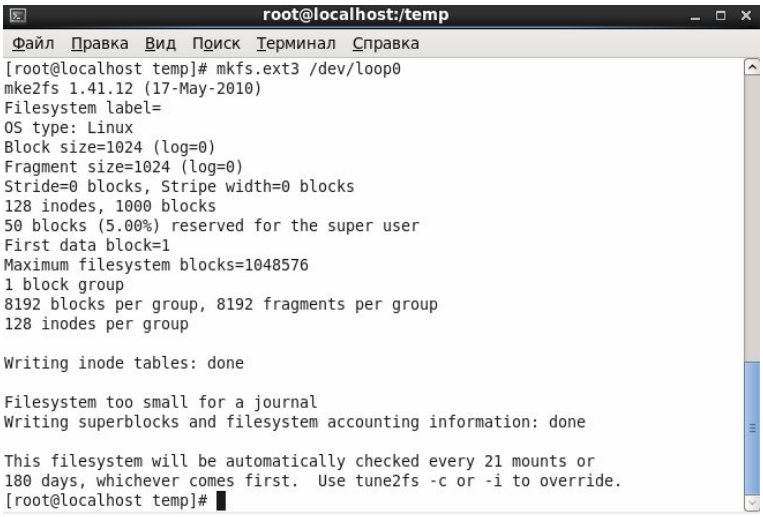


Рисунок 108 - Создание файловой структуры на блочном устройстве

Создадим директорию /mnt/newdisk с помощью команды:

mkdir /mnt/newdisk

Смонтируем диск следующей командой:

mount /dev/loop0 /mnt/newdisk

Перейдем в директорию /mnt/newdisk командой:

cd /mnt/newdisk

Создадим файл 2.txt на диске с определенной сигнатурой с помощью команды:

echo 1234567890987654321 > 2.txt

Выведем содержание файла в шестнадцатиричном виде, как на рис. 109.

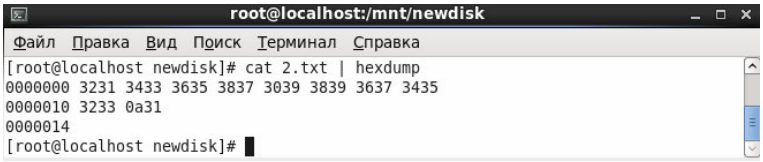


Рисунок 109 - Содержимое файла 2.txt

Выполним поиск на блочном устройстве 1.txt шестнадцатиричного представления, как на рис. 110.

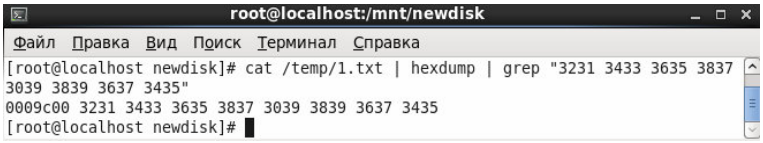


Рисунок 110 - Поиск шестнадцатиричного представления

Как видно из рис. 110, данные находятся по определенному смещению.

Удалим файл 2.txt командой "rm" и вновь выполним поиск (рис. 111).

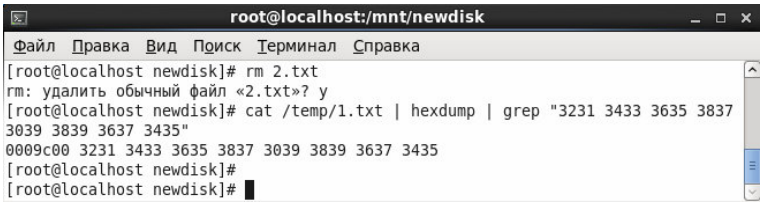


Рисунок 111 - Удаление файла и повторный поиск

Как видно из рис. 111 файл не был удален до конца и в последствии его можно найти.

Теперь удалим файл 2.txt командой shred, указав опции -u для удаления и -z для того, чтобы скрыть информацию, что файл был удален:

shred -u -z 2.txt

Повторно выполним поиск шестнадцатиричного представления (рис. 112).

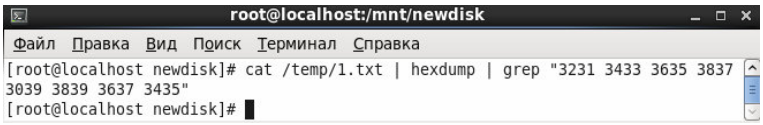


Рисунок 112 - Поиск шестнадцатиричного представления

В результате видим, что файла уже нет, что означает, что данные полностью удалены.

4.3 Утилита scrub

Когда требуется удалить файлы так, чтобы их восстановление было невозможно, можно обратиться к утилите scrub, которая имеет режим создания файла со случайным содержимым до полного заполнения диска. При этом свободное место затирается новым содержимым, что затрудняет восстановление стертых до этого файлов.

Создадим файл 1.txt командой:

touch 1.txt

Заполним файл нулями с помощью утилиты dd, как показано на рис. 113.

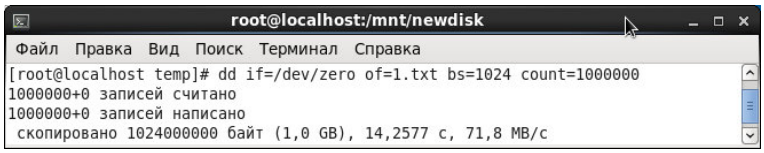


Рисунок 113 - Заполнение файла нулями с помощью утилиты dd

Представим файл как блочное устройство с помощью следующей команды:

losetup /dev/loop4 1.txt

Создадим файловую структуру на блочном устройстве, как на рис. 114.

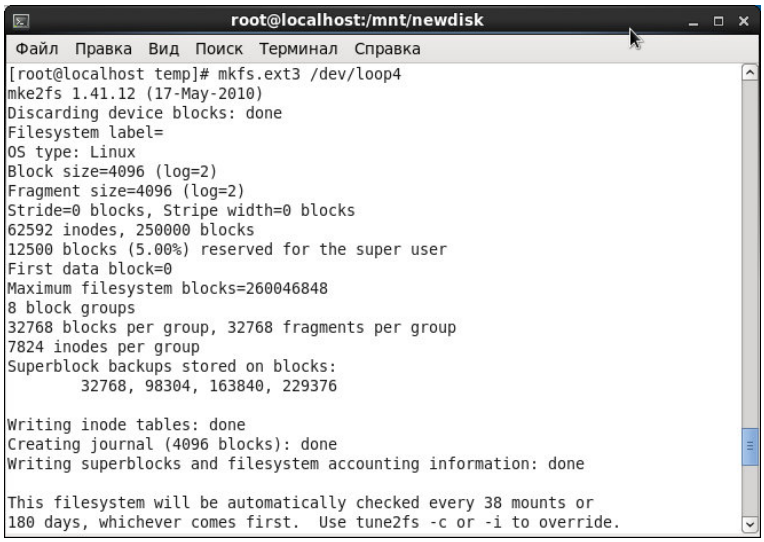


Рисунок 114 - Создание файловой структуры на блочном устройстве

Создадим директорию /mnt/newdisk с помощью команды:

mkdir /mnt/newdisk

Смонтируем диск следующей командой:

mount /dev/loop4 /mnt/newdisk

Перейдем в директорию /mnt/newdisk командой:

cd /mnt/newdisk

Создадим файл 2.txt на диске с определенной сигнатурой с помощью команды:

echo 1234567890987654321 > 2.txt

Выведем содержание файла в шестнадцатиричном виде, как на рис. 115.

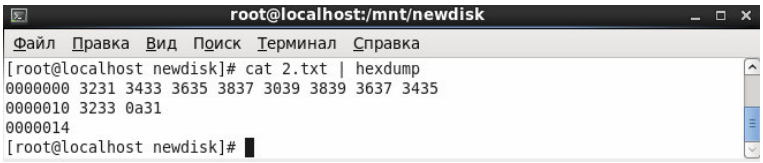


Рисунок 115 - Содержимое файла 2.txt

Выполним поиск на блочном устройстве 1.txt шестнадцатиричного представления, как на рис. 116.

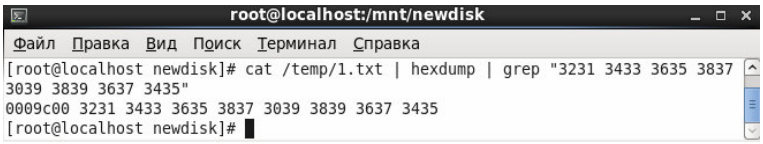


Рисунок 116 - Поиск шестнадцатиричного представления

Как видно из рис. 116, данные находятся по определенному смещению.

Удалим файл 2.txt командой rm и вновь выполним поиск (рис. 117).

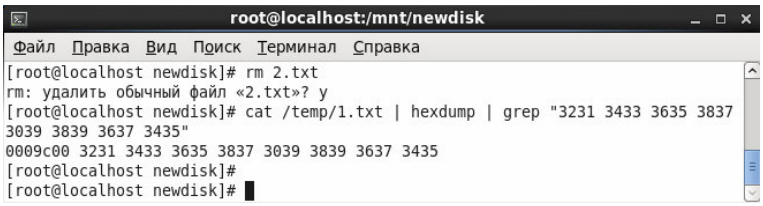


Рисунок 117 - Удаление файла и повторный поиск

Как видно из рис. 117 файл не был удален до конца и в последствии его можно найти.

Теперь воспользуемся командой scrub с опцией -X, которая создает файл со случайным содержимым до полного заполнения диска, в данном примере в папку scrubdir, при этом свободное место затирается новым содержимым (рис. 118).

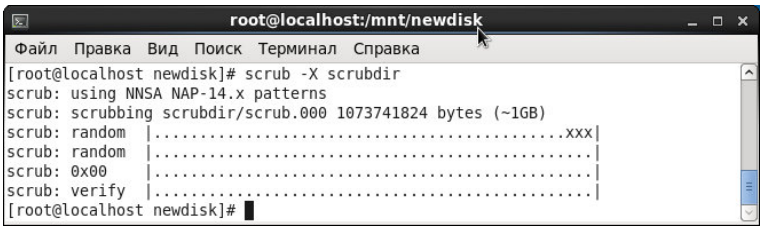


Рисунок 118 - Результат выполнения команды scrub

Повторно выполним поиск шестнадцатиричного представления (рис. 119).

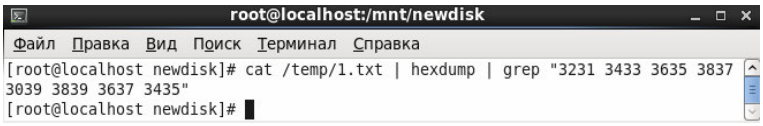


Рисунок 119 - Поиск шестнадцатиричного представления

В результате видим, что файла уже нет, что означает, что данные полностью удалены.

5 ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ БЕЗОПАСНОСТИ

В данном разделе приведены рекомендации по дополнительным настройкам системы с целью обеспечения ее безопасной эксплуатации.

5.1 Служба SNMP

SNMP - стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектуры TCP/UDP. Протокол обычно используется в системах сетевого управления для контроля подключенных к сети устройств на предмет условий, которые требуют внимания администратора. Если при настройке службы не было задано имя группы, будет использоваться значение по умолчанию. Это позволяет потенциальному нарушителю (атакующему) собрать дополнительную информацию о целевом хосте. Для исключения возможности использования этой уязвимости, нужно отключить данную службу.

Так же, используя недостатки в протоколе SNMP можно осуществить распределённую атаку отказа в обслуживании. Для этого атакующий отправляет большое количество IP пакетов с изменённым адресом на многочисленные устройства, которые отвечают на указанный адрес. Эта атака позволяет создавать огромный поток сетевых данных, нарушающий нормальную работу системы. Чтобы исключить возможность такой атаки, рекомендуется отключить службу.

Для отключения службы необходимо:

1. Выполнить команду "chkconfig snmpd off".
2. Выполнить команду "chkconfig snmptrapd off".
3. Перезагрузить систему.

Если нет возможности отключить службу, рекомендуется заменить "public" на другое имя в файле /etc/snmp/snmpd.conf, а также настроить фильтрацию UPD пакетов для порта 161.

5.2 Сертификаты SSL. Получение доверенного сертификата

В протоколе SSL используются сертификаты для проверки соединения. Они могут не пройти проверку в нескольких случаях:

- сертификат не имеет подписи известных публичных доверенных центров;
- сертификат может быть недействительным на момент проверки;
- данные в сертификате могут не совпадать с требуемыми.

В случае использования недоверенных сертификатов существенно упрощается проведение атаки посредника для перехвата передаваемых данных. Чтобы этого избежать, нужно получить и использовать корректный сертификат.

Иногда практикуется использование самозаверенных сертификатов - сертификатов, созданных самим пользователем. В этом случае издатель сертификата совпадает с владельцем сертификата, что также упрощает перехват передаваемых данных. Поэтому для исключения уязвимостей необходимо провести процедуру подписи сертификата доверенным центром.

Для получения доверенного сертификата нужно обращаться к поставщикам сертификатов, в центры сертификации. Рекомендуется также использовать алгоритм SHA-256 с длиной ключа не менее 2048 бит.

5.3 Сертификаты SLL. Длина криптографического ключа

Длина ключа, используемая криптографическим алгоритмом, определяет уровень безопасности, который может быть достигнут. Используйте ключи длиной более 2048 бит.

5.4 Протокол SSL. Старые версии

SSL - криптографический протокол, предназначенный для обеспечения безопасной связи. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для обеспечения целостности сообщений.

SSL постоянно развивается. Протоколы ранних версий SSL 2.0 и 3.0 являются небезопасными т.к. подвержены некоторым уязвимостям. Необходимо отключить небезопасные версии протокола для использования сервером HTTP.

Для этого необходимо:

1. В файле /etc/httpd/conf.d/ssl.conf ко всем строкам вида "SSLProtocol all" добавить: " -SSLv2 -SSLv3".

2. Перезагрузить систему.

5.5 Протокол SSL. Небезопасный шифр RC4

RC4 - потоковый шифр, реализованный на основе генератора псевдослучайных битов. Широко применяется в различных системах защиты информации в компьютерных сетях. Однако сейчас известно, что в нем имеется ряд существенных недостатков, позволяющих

получить передаваемые данные.

Для исключения этих уязвимостей необходимо отключить поддержку шифров RC4, а именно:

1. Убрать в файле /etc/httpd/conf.d/ssl.conf в строках, начинающихся с "SSLCipherSuite" вхождения "RC4".

2. Перезагрузить систему.

5.6 Протокол SSL. Разглашение информации

В протоколе SSL существует уязвимость, обусловленная особенностью шифрования данных в режиме CBC (сцепление блоков шифротекста) с векторами инициализации. Эксплуатация данной уязвимости позволяет злоумышленнику, действующему по принципу "человек посередине", получить доступ к HTTP-заголовкам в незашифрованном виде, используя атаку на HTTPS-сессии на основе поблочно подобранных границ (blockwise chosen-boundary attack) совместно с JavaScript-кодом, в котором используется HTML5 WebSocket API, Java URLConnection API или Silverlight WebClient API. Данная уязвимость известна под названием BEAST-атака.

Для исключения данной уязвимости необходимо:

1. В файле /etc/httpd/conf.d/ssl.conf нужно ко всем строкам вида: "SSLProtocol all" добавить " -TLSv1".

2. Перезагрузить систему.

5.7 Обработка пустых LDAP запросов

LDAP - протокол прикладного уровня для доступа к службе каталогов X.500, разработанный IETF как облегчённый вариант разработанного ITU-T протокола DAP. LDAP — относительно простой протокол, использующий TCP/IP и позволяющий производить операции аутентификации (bind), поиска (search) и сравнения (compare), а также операции добавления, изменения или удаления записей. Известно, что в запущенной службе LDAP разрешены пустые поисковые запросы, что позволяет получить информацию о структуре каталогов.

Чтобы избежать этого, необходимо:

1. Из файла /etc/openldap/slapd.conf удалить запись " defaultsearchbase".

2. В файл /etc/openldap/slapd.conf добавить "access to dn.base="" attrs=namingContexts by * none" .

3. Перезагрузить систему.

5.8 Сервер SSH. Защита от подбора имён и паролей учётных записей

В случае использования простых паролей методом перебора по словарю распространённых имён пользователей и паролей может быть получен доступ к их учетным записям. Чтобы исключить подобную возможность, необходимо задавать стойкие пароли.

Рекомендуется использовать нетривиальные пароли длиной более десяти символов, включающие в себя буквы в различных регистрах (aBcDeF), цифры, дополнительные символы (+-_). Следует избегать целых слов (password), повторяющихся комбинаций (123123123), а также осмысленных фраз.

5.9 Сервер SSH. Разрешены CBC шифры

На сервере SSH разрешено использование Cipher Block Chaining (CBC) шифров. В них нет известных уязвимостей, но иногда рекомендуется отключить их поддержку.

Для этого в файле /etc/ssh/sshd_conf нужно найти строку "Ciphers" и удалить оттуда все вхождения CBC шифров. Если такой строки нет, то нужно добавить в файл "Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,arcfour". Затем перезагрузить систему.

5.10 Сервер SSH. Разрешены слабые алгоритмы MD5 или 96-bit MAC

На сервере SSH разрешено использование MD5 или 96-bit MAC алгоритмов. В них нет известных уязвимостей, однако они считаются слабыми. Рекомендуется отключить их поддержку.

Для этого в файле /etc/ssh/sshd_conf нужно найти строку "MACs" и удалить из неё все вхождения MD5 и 96-bit алгоритмов. Если такой строки нет, то нужно добавить в файл строку "MACs hmac-sha1,umac-64@openssh.com,hmac-ripemd160". Затем перезагрузить систему.

5.11 Служба memcached

Служба memcached предназначена для кэширования данных других приложений в оперативной памяти. Неограниченный доступ позволяет злоумышленнику получить полный доступ к кэшируемым объектам (добавление, изменение, удаление), что может нарушить работу служб, использующих memcached.

Необходимо ограничить список адресов, с которых возможен доступ к сервису.

Для этого:

1. В файле /etc/memcached.conf заменить строку "-l <список адресов>" на "-l 127.0.0.1".

2. Перезапустить систему.

5.12 Сервер HTTP. Методы TRACE / TRACK

В HTTP сервере метод TRACE используется для отладочных целей и предоставляет большой объём информации о внутренней работе сервера. Поэтому при обычной работе его поддержка должна быть отключена.

Для этого:

1. В начало файла /etc/httpd/conf/httpd.conf добавить строку "TraceEnable off".
2. Перезагрузить систему.

5.13 Сервер HTTP. Доступ к каталогам для просмотра

Пользователи или злоумышленники могут использовать информацию, полученную путем просмотра структуры каталогов, для обнаружения незащищенных каталогов и для получения доступа к каталогам и файлам, которые не должны находиться в общем доступе. Структура каталогов может дать злоумышленнику представление о типе веб-сервера, операционной системы или другого программного обеспечения, запущенного в системе.

Рекомендуется запретить доступ к каталогу для просмотра, если в этом нет необходимости. Для этого в каталоге нужно создать файл ".htaccess", содержащий "deny from all" и перезапустить систему.

5.14 Блокировка модуля n_hdlc

В модуле n_hdlc ядра начальной версии операционной системы и версий с включенными первым и вторым наборами обновлений имеется ошибка, которая позволяет локальному пользователю с помощью специального эксплойта повысить свои привилегии или вызвать сбой типа «отказ в обслуживании». Для устранения этой ошибки необходимо установить соответствующее обновление безопасности или вручную заблокировать вышеупомянутый модуль, что можно сделать, войдя в консоль с полномочиями администратора root и запустив следующий скрипт:

```
#!/bin/bash
echo "install n_hdlc /bin/true">> /etc/modprobe.d/disable-n_hdlc.conf
result=$(awk /^n_hdlc/ /proc/modules)
```

```
echo "disable n_hdlc is OK !!!"
if [ -n "$result" ]; then
   echo "Module n_hdlc is running. Now the pc will reboot!!!"
   shutdown -r now
fi
```

Если во время работы скрипта обнаружится, что модуль n_hdlc загружен, то система будет автоматически перезагружена.

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					

Изм.	Лист	№ докум	Подп	Дата