

“Настройка CentOS. Основы работы с ОС Linux”

#Краткие теоретические сведения, которые полезно узнать перед началом работы

IP-телефония - телефонная связь (передача голоса) по сетям передачи данных, использующим протокол IP.

Asterisk - программный сервер телефонии (программная АТС) с открытым исходным кодом, поддерживающий работу со специализированным оборудованием для аналоговых/цифровых телефонных линий, а также программные и аппаратные IP-телефоны.

Linux - общее название ОС из семейства Unix, которых объединяет ядро, созданное Линусом Торвалдсом. На базе ядра Linux создано множество дистрибутивов различного назначения (для использования в производственной среде, домашнего использования, и т.д.), среди наиболее известных - Red Hat, CentOS, Fedora, Debian, Ubuntu, Kali, Arch. Android также базируется на Linux.

Виртуализация – технология создания виртуального представления вычислительных ресурсов абстрагировано от аппаратного обеспечения, на базе компьютера, сервера или серверного кластера (обобщенно говоря, *хоста*) для возможности одновременной работы нескольких ОС. Реальные ресурсы хоста (процессор, оперативная и дисковая память и т.д.) с помощью специализированного ПО (*гипервизора*) распределяются между *виртуальными машинами* (ВМ) - программными средами, имитирующими физический компьютер, на которые устанавливаются *гостевые* ОС.

Гипервизор – ПО, которое управляет выделением физических ресурсов хоста для ВМ, разделяет и изолирует эти ресурсы между ними, позволяя запускать несколько ОС одновременно, также гипервизор выполняет обработку запросов прерываний процессора и запросов на доступ к памяти от гостевых ОС. Для хостовой ОС ВМ представляет собой набор файлов - обычно это файл виртуального диска, файл конфигурации ВМ и некоторые другие файлы (файлы контрольных точек и тп).

Существует 2 основных типа гипервизоров, 1 - представляет собой специализированную ОС, устанавливаемую непосредственно на сервер в качестве хостовой, имеет прямой доступ ко всем аппаратным ресурсам. Является оптимальным вариантом для высоконагруженных сред виртуализации ввиду легковесности и оптимизированности такой ОС под конкретные задачи виртуализации, а главное - минимальной возможности возникновения ошибок ОС вследствие отсутствия ненужных компонентов, несущих сторонний функционал; 2 - ПО, устанавливаемое в обычной ОС (Windows, Linux, macOS), взаимодействующее с аппаратными ресурсами через хостовую ОС, что подходит для быстрого развертывания тестовых стендов и выполнения лабораторных работ.

Раздел 1. Создание ВМ в VMware Workstation Player 15

Скачайте с сервера данное руководство и образ CentOS (в папке soft) себе на компьютер и сохраните на диске D: или F:

1. Нажмите **Create a New Virtual Machine.**

2. Выберите пункт **I will install the operating system later.**

New Virtual Machine Wizard ✕

Welcome to the New Virtual Machine Wizard
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

☐ Installer disc:
No drives available

☐ Installer disc image file (iso):
D:\CentOS-8-x86_64-1905-dvd1.iso Browse...

☒ I will install the operating system later.
The virtual machine will be created with a blank hard disk.

Help < Back Next > Cancel

3. Выберите тип и версию гостевой ОС (если в вашей версии доступен на выбор **CentOS 8** или **Red Hat Enterprise Linux 8** - укажите его, если нет - **CentOS 7**).

New Virtual Machine Wizard ✕

Select a Guest Operating System
Which operating system will be installed on this virtual machine?

Guest operating system

☐ Microsoft Windows
☒ Linux
☐ Other

Version
CentOS 7 64-bit

Help < Back Next > Cancel

4. Укажите имя (рекомендуется отобразить в имени принадлежность ВМ к студенту) и папку сохранения для ВМ (рекомендуется сохранить на диск D: или F:)

New Virtual Machine Wizard ✕

Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name:

Location:

5. Укажите параметры диска для ВМ (объем 20 ГБ)

New Virtual Machine Wizard ✕

Specify Disk Capacity
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB):

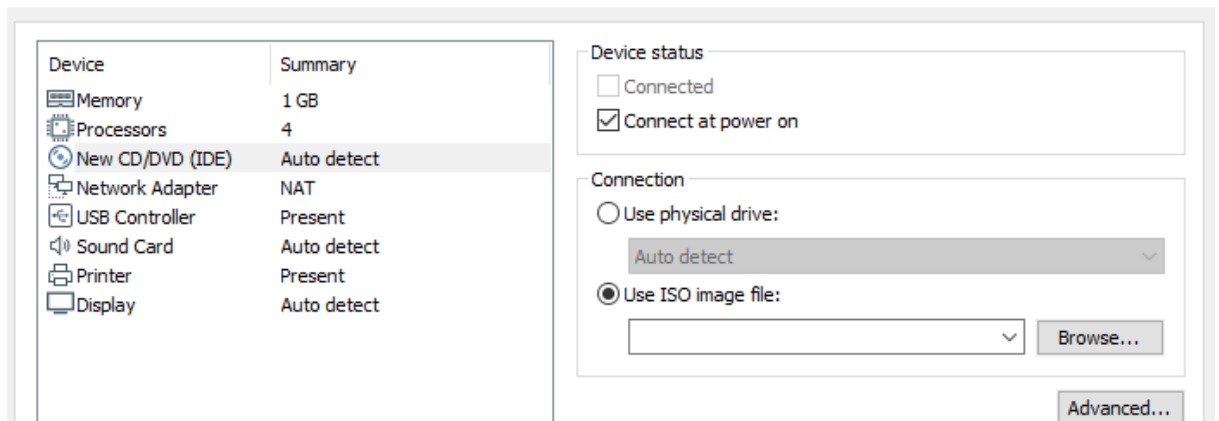
Recommended size for CentOS 7 64-bit: 20 GB

☐ Store virtual disk as a single file

☒ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

6. Нажмите **Customize Hardware...** Выделите для ВМ 1 ГБ оперативной памяти (Memory), 4 ядра процессора (Processors), в New CD/DVD выберите **Use ISO image file** и нажав Browse, укажите путь к сохраненному ранее образу CentOS:

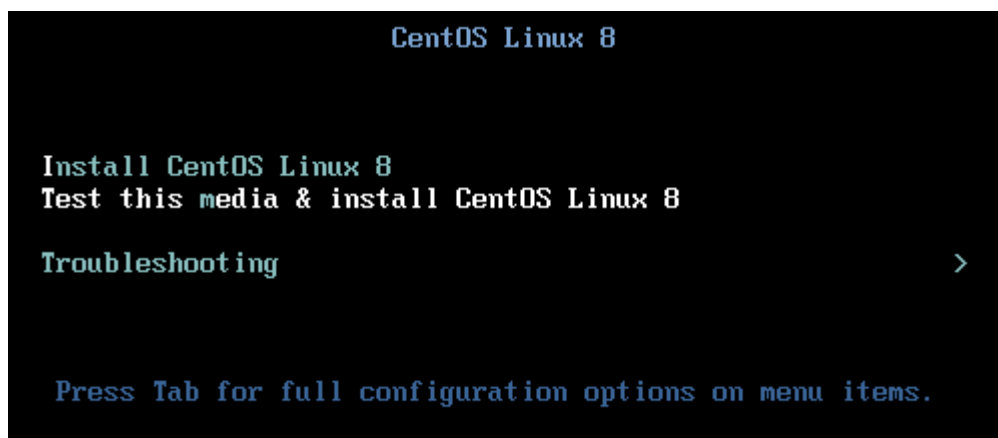


Выделенных ресурсов хватит для тестовой установки и эксплуатации CentOS без графического окружения с Asterisk, обслуживающим до 10 клиентов. Нажмите **Close** и потом **Finish**

7. Запустите ВМ (появится слева в VMware Player), нажав **Play virtual machine**. Переключение ввода внутрь ВМ производится щелчком ЛКМ по окну с запущенной ВМ, возврат в хостовую ОС - Ctrl+Alt.

Раздел 2. Установка CentOS 8

1. При появлении меню загрузки, как показано на рисунке, выберите пункт **Install CentOS...** чтобы начать установку CentOS 8.



2. Выберите язык системы (*настоятельно* рекомендуется оставить английский **English (United States)**) и нажмите **Continue**.



3. В появившемся окне параметров установки перейдите в **Time&Date**, выберите корректный часовой пояс, нажмите **Done**.

TIME & DATE

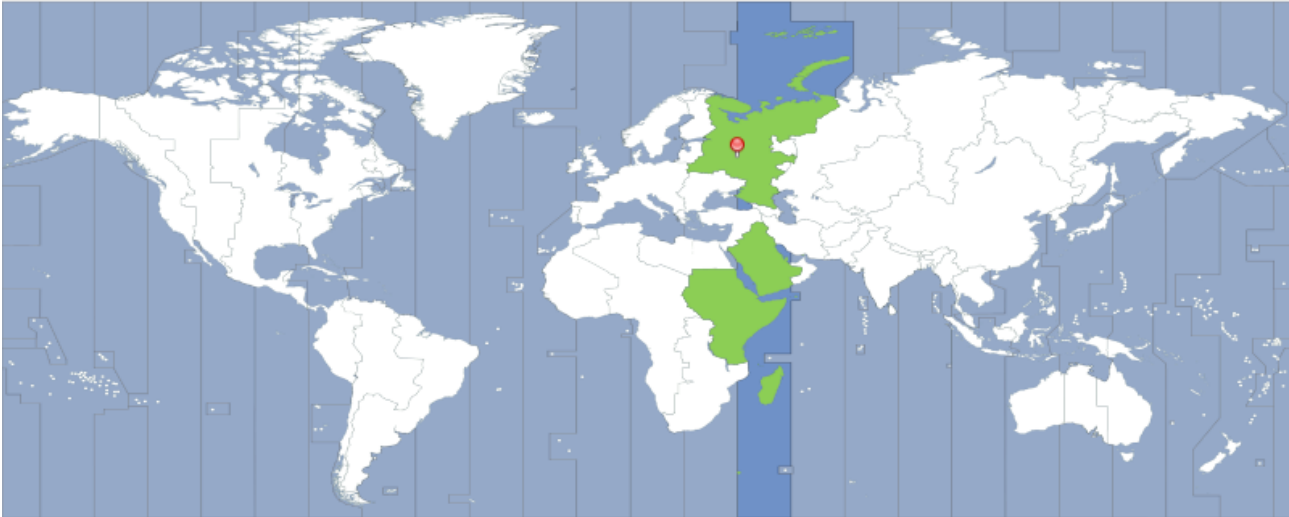
Done

CENTOS LINUX 8 INSTALLATION

us

Help!

Region: EuropeCity: MoscowNetwork TimeOFF



12:33

24-hour

AM/PM

08 / 31 / 2020

You need to set up networking first if you want to use NTP

4. Перейдите в **Software Selection** и выберите подходящее базовое окружение - **Minimal Install** (в целом, опция Minimal Install вполне подходит для большинства случаев развертывания, установка Asterisk - в их числе).

SOFTWARE SELECTION

Done

CENTOS LINUX 8 INSTALLATION

us

Help!

Base Environment

☐ **Server with GUI**
An integrated, easy-to-manage server with a graphical interface.

☐ **Server**
An integrated, easy-to-manage server.

☒ **Minimal Install**
Basic functionality.

☐ **Workstation**
Workstation is a user-friendly desktop system for laptops and PCs.

☐ **Custom Operating System**
Basic building block for a custom CentOS system.

☐ **Virtualization Host**
Minimal virtualization host.

Additional software for Selected Environment

☒ **Guest Agents**
Agents used when running under a hypervisor.

☐ **Standard**
The standard installation of CentOS Linux.

☐ **Legacy UNIX Compatibility**
Compatibility programs for migration from or working with legacy UNIX environments.

☐ **Container Management**
Tools for managing Linux containers

☐ **Development Tools**
A basic development environment.

☐ **.NET Core Development**
Tools to develop .NET applications

☐ **Graphical Administration Tools**
Graphical system administration tools for managing many aspects of a system.

☐ **Headless Management**
Tools for managing the system without an attached graphical console.

☐ **Network Servers**
These packages include network-based servers such as DHCP, Kerberos and NIS.

5. Откройте пункт **Installation Destination** и нажмите Done для автоматической разметки диска.

6. Перейдите в пункт **Network & Host name**. Включите доступные сетевые интерфейсы Ethernet (и проверьте, что им присваивается IP-адрес). В поле **Host Name** внизу задайте произвольно имя хоста (это имя будет установлено в ОС как имя системы) и нажмите Apply. Если текущее имя изменено, адрес успешно получен, нажмите **Done**.

NETWORK & HOST NAME

Done

CENTOS LINUX 8.0.1905 INSTALLATION

us

Help!

Ethernet (ens160)
VMware VMXNET3 Ethernet Controller

+ -

Ethernet (ens160)
Connected

Hardware Address 00:0C:29:B4:08:92

Speed 10000 Mb/s

IP Address 192.168.125.122/24

Default Route 192.168.125.2

DNS 192.168.125.2

ON

Configure...

Host Name: voip-vasya

Apply

Current host name: voip-vasya

7. Нажмите **Begin Installation** чтобы начать установку. В **Root Password** задайте пароль пользователю **root** (На данном этапе возможно задать простой короткий пароль путем двойного нажатия Done). Создайте своего пользователя (**User Creation**) с любым удобным именем (в поле Full name можно использовать ПРОПИСНЫЕ буквы и длинное имя, поле User name содержит логин, под которым авторизуется пользователь, он должен быть достаточно короткий и не должен содержать ПРОПИСНЫХ букв. Обязательно отметьте пункт **Make this user administrator** для добавления пользователя в соответствующую группу администраторов (wheel). На данном этапе также возможно аналогично задать простой короткий пароль.

ЗАПИШИТЕ ПАРОЛЬ И ИМЯ ПОЛЬЗОВАТЕЛЯ, ЧТОБЫ НЕ ЗАБЫТЬ ДО КОНЦА УСТАНОВКИ ОС!

CREATE USER

Done

CENTOS LINUX 8.0.1905 INSTALLATION

us

Help!

Full name the best Admin Vasya

User name vasya

Tip: Keep your user name shorter than 32 characters and do not use spaces.

☒ Make this user administrator

☒ Require a password to use this account

Password

Too short

Confirm password

Advanced...

8. По окончании установки нажмите **Reboot**. ВМ перезагрузится и загрузится с виртуального диска со свежееустановленной CentOS.

ОБРАТИТЕ ВНИМАНИЕ! Не сохраняйте состояние ВМ (Suspend Guest) по окончании работы с ней, завершайте работу из CentOS (`sudo shutdown now`) или VMware Player - Shut Down Guest.

Первоначальная настройка CentOS

В Linux подключенные диски отображаются иначе и имеют отличные от используемых в Windows идентификаторы. В зависимости от интерфейса, через который подключен жесткий диск, название может начинаться на:

- sd - устройство, подключенное через интерфейс SCSI (SAS);
- hd - устройство, подключенное через интерфейс ATA (SATA);

Третья буква в имени диска отображает его порядковый номер в алфавитном системе, цифра на 4 месте обозначает раздел.

Получить информацию о доступных дисках и разделах, их размере и свободном месте можно с помощью команды

```
df -h
```

Также подобную информацию можно получить командой

```
lsblk
```

1. Настройка удаленного доступа по протоколу SSH

Авторизуйтесь в окне ВМ под пользователем, которого Вы создали на этапе установки. (Данная работа (и последующие в курсе) предполагает, что Вы НЕ используете учетную запись root)

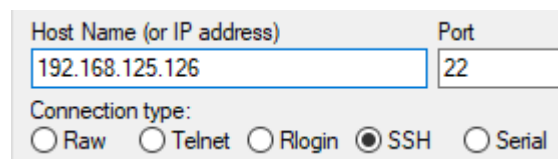
Узнайте IP адрес, который был получен CentOS от DHCP сервера VMware Player, для этого выполните команду

```
ip address
```

Первый сетевой адаптер в списке с именем lo, с адресом 127.0.0.1 (адрес указан после слова inet), также известным как адрес **localhost** - **loopback**-адаптер, используемый для обращения ОС к себе самой, трафик этого адаптера никогда не покидает ОС и не попадает в сеть, целая подсеть 127.0.0.0/8 выделена под loopback, и, соответственно, недоступна извне. Используемый для связи с “внешним миром” адрес следует искать в секции, соответствующей адаптеру с именем, начинающимся на eth или ens.

Для удаленного подключения к CentOS воспользуемся протоколом SSH (Secure SHell 2 версия), который предоставляет безопасный (защищенное криптоалгоритмами RSA или ECDSA соединение) доступ к командной оболочке. Этот протокол заменил в большинстве случаев небезопасный открытый протокол Telnet.

Запустите на хостовом ПК программу PuTTY, в поле Host Name введите полученный на предыдущем шаге IP адрес CentOS, выберите тип подключения SSH и нажмите Open.



Host Name (or IP address)	Port
192.168.125.126	22
Connection type:	
<input type="radio"/> Raw	<input type="radio"/> Telnet
<input type="radio"/> Rlogin	<input checked="" type="radio"/> SSH
<input type="radio"/> Serial	

Согласитесь на добавление незнакомого ключа сервера, после появления окна с приглашением login as: введите имя пользователя, нажмите Enter, введите пароль, нажмите Enter. Вы можете открыть несколько параллельных сессий от имени одного пользователя в новых окнах PuTTY, что может быть удобно, если потребуется одновременно изменять конфигурацию и отслеживать сообщения в интерфейсе какого-либо ПО.

Раздел 3. Изучение базовых команд Linux.

Основные теоретические сведения:

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

Теоретическая часть:

Среди всех элементов операционной системы Linux самым важным, является командная строка (Терминал). Оболочка во многом определяет богатые возможности и гибкость операционной системы Linux. С помощью командной строки можно выполнять действия, которые были бы немыслимы при работе с графическим пользовательским интерфейсом. Независимо от того, KDE или GNOME, оказывается, что многие действия гораздо быстрее и эффективнее выполнить, пользуясь только командной строкой. Освоение Linux стоит начинать с изучения средств командной оболочки.

Файлы и ничего кроме файлов

Все, с чем Вы встретитесь в операционной системе Linux, - это файлы. Очевидно, что текстовый документ - это файл. Изображения, аудиоданные в формате MP3 и видеофрагменты - это несомненно файлы. Каталоги - это тоже файлы, содержащие информацию о других файлах. Дисковые устройства - это большие файлы. Сетевые соединения тоже файлы. Даже исполняемый процесс - это файл. С точки зрения операционной системы Linux файл представляет собой поток битов или байтов. Система не интересуется тем, что означает каждый байт. Это забота конкретных программ, выполняющихся в операционной системе Linux. Для операционной системы Linux и документ, и сетевое соединение всего лишь файлы. Как обрабатывать текстовый документ, знает редактор, а сетевое приложение умеет работать с сетевым соединением.

В отличие от Windows и MacOS в операционной системе Linux имена файлов чувствительны к регистру символов. В частности, Вы можете встретить в одном каталоге все три файла которые приведены ниже в качестве примера:

Sit.txt
sIt.txt
SIT.txt

С точки зрения файловой операционной системы Linux - это различные имена файлов. Если вы попытаетесь создать файлы с этими же именами в Windows или MacOS, то вероятнее всего попытка увенчается провалом, и система предложит Вам выбрать другое имя для файла.

Чувствительность к регистру символов также означает, что при вводе команд они должны в точности совпадать с именами файлов, поддерживающих их. Так, например, удаляя файл с помощью команды `rm`, нельзя вводить `RM`, `Rm` или `rM`. Надо также следить за написанием имен, задаваемых в качестве параметров. Если вы захотите удалить файл «SIT.txt», а укажете имя `Sit.txt`, вы лишитесь совсем не того файла, с которым предполагали расстаться.

Список специальных символов которые не рекомендуется использовать в названиях файлов:

/	- Нельзя использовать ни при каких обстоятельствах
\	- Должен быть предварен таким же символом. Применять не рекомендуется

- - Нельзя использовать в начале имени файла или каталога
- [] - Каждый из этих символов должен быть предварен обратной косой чертой. Применять не рекомендуется
- { } - Каждый из этих символов должен быть предварен обратной косой чертой. Применять не рекомендуется
- * - Должен быть предварен обратной косой чертой. Применять не рекомендуется
- ? - Должен быть предварен обратной косой чертой. Применять не рекомендуется
- ' - Должен быть предварен обратной косой чертой. Применять не рекомендуется
- " - Должен быть предварен обратной косой чертой. Применять не рекомендуется

Групповые операции:

Предположим, что в одном из каталогов на вашем компьютере содержатся сто файлов с изображениями и два текстовых файла. Ваша задача удалить все файлы с изображениями за исключением двух текстовых файлов. Удалять файлы по одному - это утомительное занятие. В операционных системах Linux для автоматизации данного процесса можно применять символы групповых операций. Групповые операции задаются посредством звездочки (*), знака вопроса (?) и квадратных скобок ([]).

Пример использования групповых операций:

Групповая операция с применением » * « - отмечает любое (в том числе нулевое) количество любых символов.

```
rm sit1*.*    Удаляться файлы : sit1.txt, sit1.jpg, sit11.jpg,
sit123123.txt

rm sit*.jpg   Удаляться файлы : sit1.jpg, sit11.jpg

rm *txt       Удаляться файлы : sit1.txt, sit123123.txt

rm sit*       Удаляться файлы : sit1.txt, sit1.jpg, sit11.jpg,
sit123123.txt

rm *          Удалятся все файлы в каталоге
```

Групповая операция с применением » ? «. Символ » ? « - соответствует одному произвольному символу.

```
rm sit1?.jpg   Удалится файл : sit11.jpg, но не sit1.txt,
sit1.jpg, sit123123.txt

rm sit?.jpg    Удалится файл : sit1.jpg, но не sit1.txt,
sit11.jpg, sit123123.txt
```

<code>rm sit?.*</code> Удаляться файлы : sit1.txt, sit1.jpg, но не sit11.jpg, sit123123.txt

Групповая операция с применением » [] «. Квадратные скобки позволяют задавать один символ из набора или символ, принадлежащий определенному диапазону.

<code>rm sit[0-1].txt</code> Удалится файл : sit1.txt, но не sit1.jpg, sit11.jpg, sit123123.txt

<code>rm sit1[0-2].jpg</code> Удалится файл : sit11.jpg, но не sit1.txt, sit1.jpg, sit123123.txt
--

Консольные команды:

<pre>\$ pwd - определить текущий каталог. \$ cd [имя каталога] - осуществить переход в заданный каталог. \$ ls [имя каталога] - просмотреть список файлов и подкаталогов. \$ mkdir [имя каталога] - создать каталог с заданным именем. \$ cp <имя файла 1> <имя файла 2> - скопировать файл «имя файла 1» в файл «имя файла 2», например: cp first.txt copy1.txt. \$ mv <имя файла 1> <имя файла 2> - переименовать файл «имя файла 1» в файл «имя файла 2», например: mv first.txt orig.txt. \$ ln «имя файла» «имя ссылки» - создать жёсткую ссылку «имя ссылки» на файл «имя файла». Пример: ln orig.txt copy2.txt. \$ ln -s «имя файла» «имя ссылки» - создать символическую ссылку «имя ссылки» на файл «имя файла». Пример: ln -s orig.txt copy2.txt. \$ rm <имя файла> - удалить файл. \$ touch <имя файла> - создание файла. \$ man <название команды> - получение справочной документации о выбранной команде.</pre>

Задания к разделу 3 лабораторной работы

- Откройте терминал.
- Ознакомьтесь с возможностями команды pwd с помощью команды man:
- Определите текущий каталог, в котором вы находитесь командой pwd:
- Ознакомьтесь с возможностями команды cd с помощью команды man:
- Перейдите в корневой каталог командой cd
- Ознакомьтесь с возможностями команды ls с помощью команды man:
- Просмотрите содержимое корневого каталога командой ls:
- Сделайте копию экрана для использования в отчете по лабораторной работе .
- Вернитесь в домашний каталог, используя команду cd без параметров:
- Ознакомьтесь с возможностями команды mkdir с помощью команды man:
- Создайте каталог «test», используя команду mkdir:
- Перейдите в каталог «test», используя команду cd:
- Просмотрите содержимое каталога, используя команду ls:
- Создайте каталог «test2», используя команду mkdir:
- Ознакомьтесь с возможностями команды touch с помощью команды man:
- Создайте файл «text» в каталоге «test2» используя команду touch:
- Ознакомьтесь с возможностями команды mv с помощью команды man:
- Переименуйте файл «text» в «textSIT» используя команду mv
- Ознакомьтесь с возможностями команды cp с помощью команды man:

- Скопируйте файл «textSIT» в каталог «test2» под именем «copy.txt», используя команду `cp`:
- Ознакомьтесь с возможностями команды `ln` с помощью команды `man`:
- Создайте жесткую ссылку «link» на файл «copy.txt» используя команду `ln`:
- Создайте символическую ссылку «simlink» на файл «copy.txt» используя команду `ln`:
- Просмотрите результаты в текущем каталоге при помощи команды `ls` с аргументами `la`:
- Сделайте копию экрана для использования в отчете по лабораторной работе .
- Удалите созданные вами файлы и ссылки в лабораторной работе используя команду `rm`
- Сделайте копию экрана для использования в отчете по лабораторной работе

Раздел 4. Разграничение прав доступа

Цель: Изучение механизмов управления доступом к ресурсам, прав доступа.

Постижение понятия пользователя и группы. Приобретение практических навыков управления пользователями при помощи консольных утилит. Приобретение навыков работы с правами пользователей и правами на файлы, каталоги при помощи консольных утилит.

Теоретическая часть

У каждого объекта (файла) есть уникальное имя, по которому к нему можно обращаться, и конечный набор операций, которые процессы могут выполнять в отношении этого объекта. Файлу свойственны операции read, write и execute.

Совершенно очевидно, что нужен способ запрещения процессам доступа к тем объектам, к которым у них нет прав доступа. Более того, этот механизм должен также предоставлять возможность при необходимости ограничивать процессы поднабором разрешенных операций. Например, процессу А может быть дано право проводить чтение данных из файла F, но не разрешено вести запись в этот файл.

Права доступа означают разрешение на выполнение той или иной операции (чтение, запись, исполнение).

Когда пользователь входит в систему, его оболочка получает UID и GID (UID – идентификатор пользователя, GID - идентификатор группы), которые содержатся в его записи в файле паролей, и они наследуются всеми его дочерними процессами. Представляя любую комбинацию (UID, GID), можно составить полный список всех объектов (файлов, включая устройства ввода-вывода, которые представлены в виде специальных файлов и т.д.), к которым процесс может обратиться с указанием возможного типа доступа (чтение, запись, исполнение).

Два процесса с одинаковой комбинацией (UID, GID) будут иметь абсолютно одинаковый доступ к одинаковому набору объектов. Процессы с различающимися значениями (UID, GID) будут иметь доступ к разным наборам файлов, хотя, может быть, и со значительным перекрытием этих наборов.

SUID (Set User ID)

Атрибут исполняемого файла, позволяющий запустить его с правами владельца. В операционных системах Linux приложение запускается с правами пользователя, запустившего указанное приложение. Это обеспечивает дополнительную безопасность т.к. процесс с правами пользователя не сможет получить доступ на запись к важным системным файлам, например /etc/passwd, который принадлежит суперпользователю root. Если на исполняемый файл установлен бит suid, то при выполнении эта программа автоматически меняет «эффективный userID» на идентификатор того пользователя, который является владельцем этого файла. То есть, независимо от того - кто запускает эту программу, она при выполнении имеет права хозяина этого файла.

SGID (Set Group ID)

Аналогичен SUID, но относится к группе. При этом, если для каталога установлен бит SGID, то создаваемые в нем объекты будут получать группу владельца каталога, а не пользователя.

Практические примеры:

Узнать права на файл/директорию

```
sit@ubuntu:~$ ls -l /bin/ls
-rwxr-xr-x 1 root root 129280 Feb 18 2016 /bin/ls
```

Права доступа состоят из трех троек символов. Первая тройка представляет права владельца файла, вторая представляет права группы файла и третья права всех остальных пользователей.

В нашем случае это :

- «rwx» - Права владельца файла
- «r-x» - Права группы файла
- «r-x» - Права всех остальных на файл.

Символ «r» означает, что чтение (просмотр данных содержащихся в файле) разрешено, «w» означает запись (изменение, а также удаление данных) разрешено и «x» означает исполнение (запуск программы разрешен).

Таким образом, если в целом посмотреть на права мы увидим, что кому угодно разрешено читать содержимое и исполнять этот файл, но только владельцу (root) разрешено как либо модифицировать этот файл. Иными словами, нормальным пользователям разрешено копировать содержимое этого файла, то только root может изменять или удалять его.

Определение текущего пользователя и групп в которых он состоит

Перед тем, как изменять владельца или группу которой принадлежит файл, необходимо уметь определять текущего пользователя и группу к которой он принадлежит. Чтобы узнать под каким пользователем вы работаете, наберите whoami:

```
sit@ubuntu:~$ whoami
sit
```

Для определения в каких группах состоит пользователь sit, необходимо воспользоваться командой groups:

```
sit@ubuntu:~$ groups
sit adm cdrom sudo dip plugdev lxd lpadmin sambashare
```

Из этого примера видно, что пользователь sit состоит в группах sit, adm, cdrom, sudo, dip, plugdev, lxd, lpadmin, sambashare. Если вы хотите посмотреть, в каких группах состоит другой пользователь, то передайте его имя в качестве аргумента.

```
sit@ubuntu:~$ groups root
root : root
```

Изменение пользователя и группы владельца

Чтобы изменить владельца или группу файла (или другого объекта) используется команды chown или chgrp соответственно. Сначала нужно передать имя группы или владельца, а потом список файлов.

```
chown sit /home/sit/itmo.txt
chgrp sit /home/sit/itmo.txt
```

Можно также изменять пользователя и группу одновременно используя команду chown в другой форме:

```
chown sit:sit /home/sit/itmo.txt
```


Вы не можете использовать команду `chown` без прав суперпользователя, но `chgrp` может быть использована всеми, чтобы изменить группу-владельца файла на ту группу, к которой они принадлежат.

`chown` и `chgrp` используются для изменения владельца и группы объекта файловой системы, но кроме них существует и другая программа, называемая `chmod`, которая используется для изменения прав доступа на чтение, запись и исполнение, которые мы видим в выводе команды `ls -l`. Команда `chmod` использует два и более аргументов: метод, описывающий как именно необходимо изменить права доступа с последующим именем файла или списком файлов, к которым необходимо применить эти изменения:

```
chmod +x /home/sit/itmo.sh
```

В примере выше в качестве метода указано `+x`. Как можно догадаться, метод `+x` указывает `chmod`, что файл необходимо сделать исполняемым для пользователя, группы и для всех остальных. Если мы решим отнять все права на исполнение файла, то сделаем вот так:

```
chmod -x /home/sit/itmo.sh
```

Разделение между пользователем, группой и всеми остальными

Часто бывает удобно изменить только один или два набора прав доступа за раз. Чтобы сделать это, просто необходимо использовать специальный символ для обозначения набора прав доступа, который необходимо изменить, со знаком «+» или «-» перед ним. Символ «u» для пользователя, «g» для группы и «o» для остальных пользователей.

```
chmod go-w /home/sit/itmo.sh
```

Данный пример удаляет право на запись для группы и всех остальных пользователей, но оставляет права владельца нетронутыми.

Числовые режимы

Существует еще один достаточно распространенный способ указания прав: использование четырехзначных восьмеричных чисел. Этот синтаксис, называется числовым синтаксисом прав доступа, где каждая цифра представляет тройку разрешений. Например, в 0777, 777 устанавливают флаги для владельца, группы, и остальных пользователей. Ниже таблица показывающая как транслируются права доступа на числовые значения.

Режим	Число
Rwx	7
rw-	6
r-x	5
r--	4
-wx	3
-w-	2
--x	1
---	0

umask

Когда процесс создает новый файл, он указывает, какие права доступа нужно задать для данного файла. Зачастую запрашиваются права 0666 (чтение и запись всеми), что дает больше разрешений, чем необходимо в большинстве случаев. К счастью, каждый раз, когда в

Linux создается новый файл, система обращается к параметру, называемому `umask`. Система использует значение `umask` чтобы понизить изначально задаваемые разрешения на что-то более разумное и безопасное. Вы можете просмотреть текущие настройки `umask` набрав `umask` в командной строке:

```
sit@ubuntu:~$ umask
0002
```

В Linux-системах значением по умолчанию для `umask` является `0022`, что позволяет другим читать ваши новые файлы (если они могут до них добраться), но не изменять их. Чтобы автоматически обеспечивать больший уровень защищенности для создаваемых файлов, можно изменить настройки `umask`:

```
sit@ubuntu:~$ umask 0077
```

Такое значение `umask` приведет к тому, что группа и прочие не будут иметь совершенно никаких прав доступа для всех, вновь созданных файлов.

В отличие от «обычного» назначения прав доступа к файлу, `umask` задает какие права доступа должны быть отключены. Снова посмотрим на таблицу соответствия значений чисел и методов:

Режим	Число
<code>rwX</code>	7
<code>rw-</code>	6
<code>r-X</code>	5
<code>r--</code>	4
<code>-wX</code>	3
<code>-w-</code>	2
<code>--X</code>	1
<code>---</code>	0

Воспользовавшись этой таблицей мы видим, что последние три знака в `0077` обозначают —`rwXrwX`. `umask` показывает системе, какие права доступа отключить. Совместив первое и второе становится видно, что все права для группы и остальных пользователей будут отключены, в то время как права владельца останутся нетронутыми.

Изменение `suid` и `sgid`

Способ установки и удаления битов `suid` и `sgid` чрезвычайно прост. Чтобы задать бит `suid`:

```
chmod u+s /home/sit/itmo.sh
```

Чтобы задать бит `sgid`:

```
chmod g+s /home/sit/itmo/
```

Определение первого знака прав доступа

Он используется для задания битов `sticky`, `suid` и `sgid` совместно с правами доступа:

<code>suid</code>	<code>sgid</code>	<code>sticky</code>	режим
<code>on</code>	<code>on</code>	<code>on</code>	7
<code>on</code>	<code>on</code>	<code>off</code>	6
<code>on</code>	<code>off</code>	<code>on</code>	5
<code>on</code>	<code>off</code>	<code>off</code>	4
<code>off</code>	<code>on</code>	<code>on</code>	3
<code>off</code>	<code>on</code>	<code>off</code>	2
<code>off</code>	<code>off</code>	<code>on</code>	1

off	off	off	0
-----	-----	-----	---

Ниже приведен пример того, как использовать четырех значный режим для установки прав доступа на директорию.

```
sit@ubuntu:~$ chmod 4775 /home/sit/itmo
sit@ubuntu:~$ ls -l /home/sit/itmo
-rwsrwxr-x 1 sit sit 0 Sep  9 12:42 /home/sit/itmo
```

Консольные команды:

id	<печать идентификатора пользователя>
chgrp	<изменить группу файла>
chown	<изменить владельца и группу файлов>
chmod	<изменить права доступа к файлу>
usermod	<изменение параметров учетной записи пользователя>
useradd	<создание нового пользователя>
userdel	<удаление пользователя>
whoami	<определение текущего пользователя>
umask	<определение или установление маски прав доступа для вновь создаваемых файлов>
sudo su	<получение прав суперпользователя>
groups	<определение к каким группам принадлежит пользователь>

Задания к разделу лабораторной работы

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

- Создайте каталог из под пользователя «sit2»
- Установите права записи для группы пользователей на данный каталог
- Добавьте пользователя «sit» в группу «sit2» с помощью команды usermod
- Проверьте в какие группы входит пользователь «sit»
- Создайте несколько файлов в каталоге, который был создан пользователем «sit2» из под пользователя «sit».
- Ознакомьтесь как удалить пользователя вместе с содержимым его домашнего каталога из справочной документации
- Удалите пользователя «sit2» вместе с его домашним каталогом.

Раздел 5. Конфигурация пакетного менеджера yum

Стандартный способ управления ПО в Linux (установка, обновление, удаление) - через соответствующий дистрибутиву пакетный менеджер, который скачивает и устанавливает пакетные файлы из репозитория - хранилища данных, предназначенных для распространения пакетов ПО по сети. В deb-based дистрибутивах Linux (Debian, Ubuntu, Kali) используется пакетный менеджер apt, в rpm-based (RedHat, CentOS, Fedora) - yum, в Fedora, а также начиная с 8 версии в RedHat и CentOS, yum является алиасом (ссылкой на другую команду) для менеджера dnf, который используется в системе вместо yum. Далее по тексту работы как пакетный менеджер будут упоминаться традиционный для CentOS yum и приводиться команды и конфигурация для него, что вполне возможно благодаря наличию в CentOS 8 обратной совместимости (а вот в ранних версиях CentOS использовать команды для dnf не получится).

В случае доступа в Интернет через прокси-сервер необходимо сконфигурировать yum для работы через прокси ИЛИ настроить локальные репозитории. В данном курсе работ будет использоваться первый способ.

Изменение параметров работы системного ПО в подавляющем большинстве случаев в Linux производится редактированием соответствующих конфигурационных файлов в текстовом редакторе и применением изменений/перезапуском службы. По умолчанию в CentOS установлен текстовый редактор vi, первоначально используйте его для редактирования текстовых файлов конфигурации, после получения доступа к репозиториям (в случае отсутствия прямого доступа в Интернет), можно установить удобный Вам - mc, nano и тп.

Обратите внимание, что для возможности сохранения файлов (право записи на файл) в любых директориях, кроме домашней, могут потребоваться права суперпользователя, с которыми должен быть запущен текстовый редактор (`sudo vi ПУТЬ_К_ФАЙЛУ`).

Параметры прокси-сервера прописываются в конфигурационном файле yum /etc/yum.conf, его необходимо открыть в редакторе с правами суперпользователя для внесения изменений:

```
sudo vi /etc/yum.conf
```

Troubleshooting

```
[sudo] password for vasya:
vasya is not in the sudoers file. This incident will be reported.
[vasya@voip-vasya ~]$
```

**Если Вы получили такой вывод в терминале, значит Ваш пользователь при установке не был добавлен в группу администраторов (пользователей с привилегиями sudo). Следует под пользователем root добавить его в группу пользователей sudo (wheel) вручную командой `usermod -aG wheel username` (пример ниже).*

```
[vasya@voip-vasya ~]$ su
Password:
[root@voip-vasya vasya]# usermod -aG wheel vasya
[root@voip-vasya vasya]# exit
exit
```

**Команда `su` переключает сессию текущего пользователя на суперпользователя `root`, поэтому пароль необходимо вводить от учетной записи `root`.*

Для применения изменений требуется полностью выйти из системы с помощью команды `exit` и авторизоваться под Вашим пользователем заново.

Переведите `vi` в режим редактирования нажав `i`. Добавьте в конец секции `[main]`:

```
proxy=http://прокси:порт (http://proxy.miet.ru)
proxy_username=логин      (номер зачетной книжки)
proxy_password=пароль
```

**уточните у преподавателя, какие параметры использовать для прокси*

Выход из `vi` с сохранением изменений: нажать `Esc` ввести `:wq`

Выход из `vi` без сохранения: `Esc` `:q!`