1) Analyze the structure of the /etc/passwd and /etc/group file, what fields are present in it, what users exist on the system? Specify several pseudo-users, how to define them?

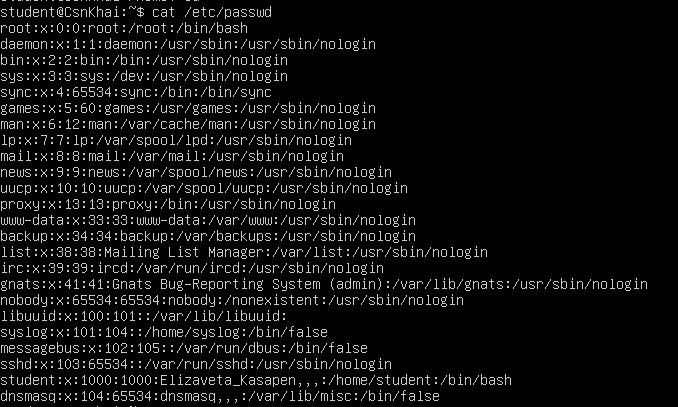
/etc/passwd

Файл /etc/passwd содержит список пользователей, которые известны системе. В процессе регистрации пользователя система обращается к этому файлу в поисках идентификатора пользователя и его домашнего каталога.

Каждая строка файла описывает одного пользователя и 7 полей, разделенных двоеточиями:

* Регистрационное имя. Регистрационные имена должны быть уникальными и состоять не более чем из 32 символов. Они могут содержать любые символы, кроме двоеточия и символа новой строки, не должны начинаться с цифры.
* Зашифрованный пароль или «заполнитель» пароля. В данном поле возможно присутствие символа «х», символа «\*» или набора случайных символов и чисел. В первом случае указывается, что пароль храниться в файле /etc/shadow. Во втором случае говорится, что данная учетная запись временно отключена. В последнем случае указывается непосредственный пароль пользователя в зашифрованном виде.
* Идентификатор пользователя - это 32-битное целое число, которое уникально идентифицирует пользователя в системе. По умолчанию, идентификаторы меньше 1000 зарезервированы для служебных учетных записей. Регулярные пользователи имеют идентификаторы, начиная с 1000.

* Идентификатор группы по умолчанию. Как и идентификатор пользователя, идентификатор группы (GID) является 32-битным целым числом. Идентификатор 0 зарезервирован для группы с именем root, идентификатор 1 - для группы bin, а 2 - для группы daemon. По умолчанию, в ОС Linux для каждого нового пользователя создается новая группа с таким же регистрационным именем и идентификатором.
* Поле персональных данных. В основном используется для хранения персональной информации о каждом пользователе. Оно не имеет четко определенного синтаксиса. Структура данного поля может быть произвольной, но команда finger интерпретирует разделенные запятыми элементы данного поля в следующем порядке: полное имя; номер офиса и здания; рабочий телефон; домашний телефон.
* Домашний каталог. Войдя в систему, пользователь попадает в свой домашний каталог. Если на момент регистрации этот каталог отсутствует, выводится сообщение о его отсутствии. По умолчанию, домашние каталоги пользователей создаются в каталоге /home. При добавлении в систему нового пользователя в его домашний каталог копируются все файлы из каталога /etc/skel, в котором содержаться персональные конфигурационные файлы командного интерпретатора и различных программ.
* Командный интерпретатор. В качестве регистрационной оболочки, как правило, задается интерпретатор команд, например, /bin/sh или /bin/csh. По умолчанию используется интерпретатор bash.

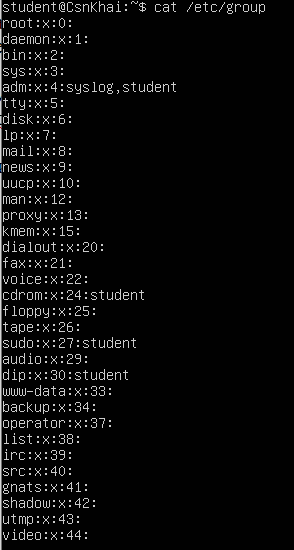


/etc/group

Файл /etc/group содержит имена групп, присутствующих в ОС Linux, и списки членов каждой группы.

Каждая запись файла /etc/group представляет одну группу и содержит четыре поля:

* Имя группы. По умолчанию при создании нового пользователя создается также его группа с таким же именем, как и регистрационное имя пользователя.
* Зашифрованный пароль или символ х, указывающий на использование файла /etc/gshadow;
* Идентификатор группы.
* Список членов, разделенный запятыми без пробелов.

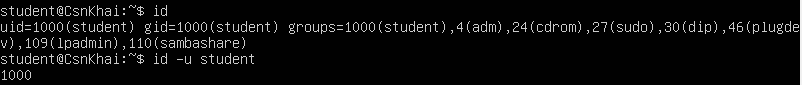


1. What are the uid ranges? What is UID? How to define it?

UID - это номер, назначенный каждому пользователю Linux.UID используется для идентификации пользователя в системе и для определения того, к каким системным ресурсам пользователь может получить доступ.

В большинстве дистрибутивов Linux UID 1-500 обычно зарезервирован для системныхпользователей. В Ubuntu и Fedora UID для новых пользователей начинаются с 1000.

Самый простой способ посмотреть идентификатор текущего пользователя - использовать команду*id*, она выводит не только сам UID, но и идентификатор группы пользователя, а также основные группы этого пользователя.



1. What is GID? How to define it?

GID - числовой идентификатор группы.

Чтобы администраторам было проще разделять полномочия между пользователями, в Linux системах существуют группы, поэтому для каждого файла в Linux системе определяется не только пользователь, но и группа. Группы нужны для того, чтобы предоставить одинаковые полномочия на файлы или какие-нибудь действия.



1. How to determine belonging of user to the specific group?

вывести группы для определенного пользователя



5) What are the commands for adding a user to the system? What are the basic

parameters required to create a user?

Команда *useradd* - это довольно простая команда, которая есть во всех дистрибутивах Linux. Она позволяет зарегистрировать нового пользователя или изменить информацию об уже имеющемся. Во время создания можно даже создать домашний каталог пользователя и скопировать в него системные файлы. Синтаксис команды:

*$ useradd опции имя\_пользователя*

Основные опции команды, с помощью которых можно настраивать нового пользователя:

*-b* - базовый каталог для размещения домашнего каталога пользователя, по умолчанию /home;

*-c* - комментарий к учетной записи;

*-d* - домашний каталог, в котором будут размещаться файлы пользователя;

*-e* - дата, когда учетная запись пользователя будет заблокирована, в формате ГГГГ-ММ-ДД;

*-f* - заблокировать учетную запись сразу после создания;

*-g*- основная группа пользователя;

*-G* - список дополнительных групп;

*-k*- каталог с шаблонами конфигурационных файлов;

*-l* - не сохранять информацию о входах пользователя в lastlog и faillog;

*-m* - создавать домашний каталог пользователя, если он не существует;

*-M*- не создавать домашнюю папку;

*-N*- не создавать группу с именем пользователя;

*-o*- разрешить создание пользователя linux с неуникальным идентификатором UID;

*-p*- задать пароль пользователя;

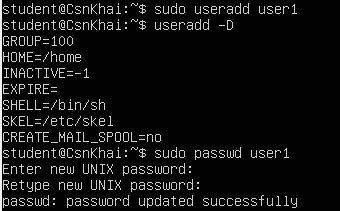
*-r*- создать системного пользователя, не имеет оболочки входа, без домашней директории и с идентификатором до SYS\_UID\_MAX;

*-s* - командная оболочка для пользователя;

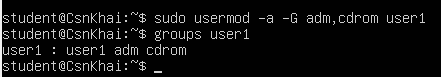
*-u* - идентификатор для пользователя;

*-D* - отобразить параметры, которые используются по умолчанию для создания пользователя. Если вместе с этой опцией задать еще какой-либо параметр, то его значение по умолчанию будет переопределено.

Добавила пользователя, просмотрела параметры по умолчанию, установила пароль для него.



Добавила пользователя в некоторые группы



1. How do I change the name (account name) of an existing user?





1. What is skell\_dir? What is its structure?

*/etc/skel* директория содержит файлы и директории, которые автоматически копируются в домашнюю директорию нового пользователя, когда его создают с помощью команды *useradd.*

Это каталог, который выглядит следующим образом:



*/ etc / skel* позволяет системному администратору создать домашний каталог по умолчанию для всех новых пользователей на компьютере или в сети и, таким образом, убедиться, что все пользователи начинают с одинаковыми настройками или средой.

1. How to remove a user from the system (including his mailbox)?

Для того, чтобы удалить пользователя существует утилита *userdel*. Пример использования:

*sudo userdel name*

*userdel* имеет всего два основных ключа:

*-f* - принудительно удалить пользователя, даже если он сейчас работает в системе;

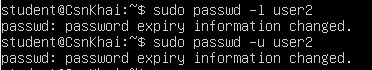
*-r* - удалить домашний каталог пользователя.





1. What commands and keys should be used to lock and unlock a user account?

Используется команда *passwd* к лючом *-l* для блокировки и *-u* для разблокировки учетной записи пользователя.



10) How to remove a user's password and provide him with a password-free login for subsequent password change?

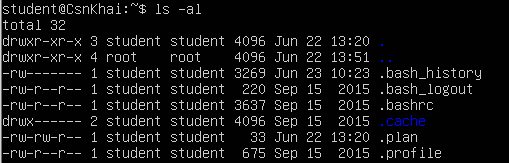
Полностью убрать пароль: *passwd -d*

Сделать пароль устаревшим (пользователь должен сменить пароль при след. входе в систему) можно с помощью *passwd* с ключом *-е*:



11) Display the extended format of information about the directory, tell about

the information columns displayed on the terminal.



*1-й столбец:* Символьное обозначение прав доступа к файлам Linux для разных групп пользователей

*2-й стобец* : Количество ссылок на файл

*3-й столбец:* Имя пользователя (владельца)

*4-й столбец:* Группа пользователя  
*5-й столбец:* Размер файла  
*6-й столбец:* Дата последнего изменения файла

*7-й столбец:* Имя файла

12) What access rights exist and for whom (i. e., describe the main roles)?

Briefly describe the acronym for access rights.

* Первый символ обозначает тип объекта: «-» означает обычный файл, «d» означает папку.
* Три следующих символа rwx означают права доступа владельца файла.
* Далее следует триада rwx означают права доступа группы.
* Последние 3 символа rwx означают права доступа остальных.

Прочерк (-) на месте одного из этих символов указывает на то, что соответствующее разрешение недоступно для соответствующего класса.

Порядок классов является одинаковым во всех дистрибутивах Linux.

Например, триада вида “r--” означает, что файл доступен "только для чтения".

*Символ r*- это сокращение от слова Read (Чтение).

Для обычного файла это разрешение на чтение, позволяет пользователю просматривать содержимое файла.

Для каталога разрешение на чтение позволяет пользователю просматривать имена файлов в каталоге.

*Символ w* - это сокращение от слова Write (Запись)/

Для файла это разрешение на запись, позволяет пользователю изменять и удалять файл.

Для каталога разрешение на запись позволяет пользователю удалить каталог, изменять его содержимое (создавать, удалять и переименовывать файлы в нем), а также изменять содержимое файлов, которые пользователь может прочитать.

*Символ x* - это сокращение от слова Execute (Выполнять)

Для файла это разрешение на исполнение, позволяет пользователю выполнять файл (пользователь также должен иметь разрешение на чтение). Таким образом, права на выполнение должны быть установлены для исполняемых программ и скриптов до того, как пользователь запустит их.

Для получения подробной информации о файлах, находящихся в каталоге нужно иметь доступ на исполнение папки.

*Пример*

*-rwxr--r--*

Файл доступен владельцу для чтения, записи и выполнения, а членам группы и прочим пользователям только для чтения.

13) What is the sequence of defining the relationship between the file and the

user?

Смотреть вопрос 12)

14) What commands are used to change the owner of a file (directory), as well

as the mode of access to the file? Give examples, demonstrate on the terminal.

Права пользователя могут быть изменены только владельцем файла или пользователем с правами администратора системы. Для изменения прав используются команды ***chown***, ***chgrp*** и ***chmod***.

Аргументы команды ***chmod***:

***chmod [ u | g | o | a ] [+ | - | = ] [r | w | x ] name1 [name2 ...]***

Выделяют 3 группы, которые могут иметь права доступа к файлам Linux:  
owner (u) – владелец файла;  
group (g) – группа владельца файла;  
others (o) – все остальные;  
all (a ) – все вышеперечисленные группы вместе.  
 3 вида прав доступа для каждой группы:  
право на чтение ( r);  
право на запись (w);  
право на исполнение (x).  
 3 вида операций:  
добавить (+);  
убрать (-);  
присвоить (=).

Также права доступа к файлам Linux можно изменять явным указанием нужных разрешений при каждом изменении. Для этого используется символьное или цифровое обозначение нужных прав, где *каждому виду прав доступа сопоставлены цифры 4, 2, 1 для r, w, x соответственно*, а итоговые права доступа к файлам определяются их суммой.

*Пример*

chmod rw-r--r-- или chmod 644 – команда разрешает владельцу чтение и запись файла, а пользователям из группы владельца и всем остальным, только чтение.

Синтаксис команды *chown*

*chown [опции] пользователь[:группа] файл...*

//создала новый файл



//изменила владельца





//изменила права доступа с помощью 8-ричного представления





//изменила права доступа (разрешила группе запись)





15) What is an example of octal representation of access rights? Describe the

umask command.

Восьмеричное представление было рассмотрено в предыдущем вопросе.

При создании файла или директории, среда операционной системы присваивает им определенные права доступа по умолчанию, и *umask* - это пользовательская маска (user mask), которая используется для определения конечных прав доступа.

Текущее значение umask:



Для файла это = 644 (т.е. rw-r--r--)

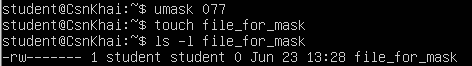
Для директории = 755 (т.е. rwxr-xr-x)

*Как посчитать*

В операционной системе Linux базовые права для директории равны 0777 (rwxrwxrwx), а для файла 0666 (rw-rw-rw).

Как посчитать (определить) права файла для маски 002 (пользователь root):  
Права по умолчанию: 666  
Вычитаемое значение umask: 002 (-)  
Итоговые права: 664

//поменяла umask, создала файл, в котором теперь по умолчанию rw-------



16) Give definitions of sticky bits and mechanism of identifier substitution. Give

an example of files and directories with these attributes.

Существуют специальные биты, такие как *SUID, SGID*и*Sticky-бит*. *SUID, SGID* влияют на запуск файла, а *Sticky* влияет на определение владельца объектов в каталоге.

*SUID* (Set User ID - бит смены идентификатора пользователя) , *SGID*(Set Group ID - бит смены идентификатора группы). Когда пользователь или процесс запускает исполняемый файл с установленным одним из этих битов, файлу временно назначаются права его (файла) владельца или группы (в зависимости от того, какой бит задан).

*Sticky bit* используется в основном для каталогов, чтобы защитить в них файлы. Из такого каталога пользователь может удалить только те файлы, владельцем которых он является. Примером может служить каталог /tmp, в который запись открыта для всех пользователей, но нежелательно удаление чужих файлов. Sticky-бит каталога, в отличие от sticky-бита файла, остается в каталоге до тех пор, пока владелец каталога или суперпользователь не удалит каталог явно или не применит к нему chmod.

*Добавление стикли-бита:*

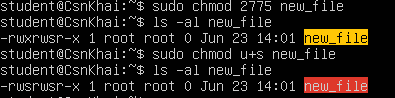
*// для папки*







// для файла подмена и для группы, и для пользователя



1. What file attributes should be present in the command script?

Чтобы сделать файл исполняемым:

*chmod +x ./myscript (атрибут х)*