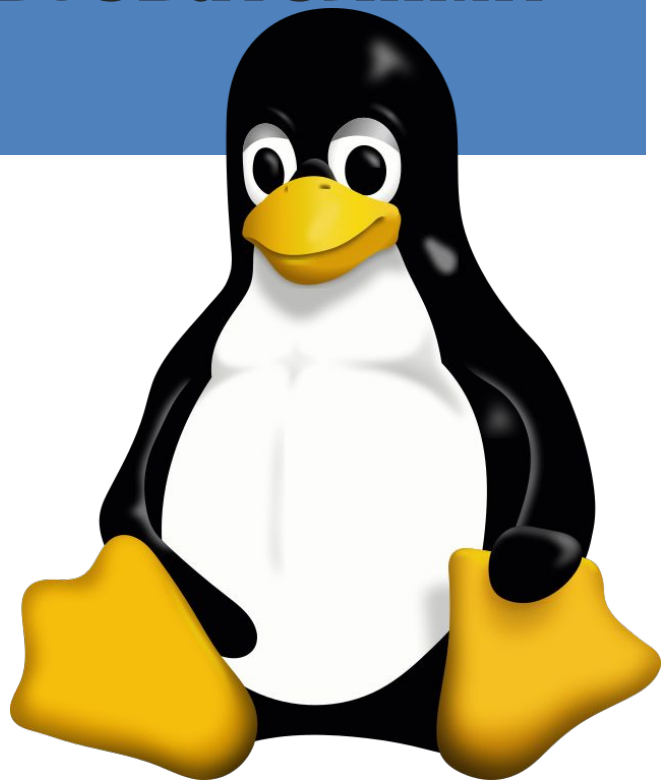
Тема: Управление пользователями и правами



План занятия

1. Основные определения
2. Работа с пользователями
3. Работа с группами
4. Конфигурационные файлы

Основные определения

Основные определения

Пользователь - это абстракция наделенная определенными правами в операционной системе.

Под каждого пользователя, создается свой каталог, пользователю назначается командная оболочка (командный интерпретатор, используемый в операционных системах семейства UNIX). Например: */bin/bash*, */bin/zsh*, */bin/sh* и другие.

Каждому пользователю назначается идентификационный номер (User ID). Сокращенно номер обозначается как **UID**, является уникальным идентификатором пользователя. Операционная система отслеживает пользователя именно по UID, а не по их имени.

Также, каждому пользователю назначается пароль для входа в систему.
Каждый пользователь принадлежит минимум к одной или нескольким группам.

Помимо пользователей, существуют **группы**. Так же как и пользователь, группа обладает правам доступа к тем или иным каталогам, файлам, периферии. Для каждого файла определён не только пользователь, но и группа. Группы группируют пользователей для предоставления одинаковых полномочий на какие-либо действия и упростить назначения прав.

Каждой группе назначается идентификационный номер (group ID). Сокращённо **GID**, является уникальный идентификатором группы. Принадлежность пользователя к группе устанавливается администратором.

Источник: ссылка

Основные правила управления доступом

Объекты (например, файлы и процессы) имеют владельцев. Владельцы обладают обширным (но необязательно неограниченным) контролем над своими объектами.

- Вы являетесь владельцами новых объектов, **создаваемых вами**.
- Пользователь **root** с особыми правами, известный как **суперпользователь**, может действовать как **владелец любого объекта в системе**.
- Только суперпользователь может выполнять административные операции особого значения.
- Владельцем файла всегда является один пользователь, тогда как в группу владельцев могут входить несколько пользователей.

По традиции информация о группах хранится в файле **/etc/group**.

Источник: ссылка

Хранение информации о пользователях

Вся информация о пользователях хранится в файле **/etc/passwd**

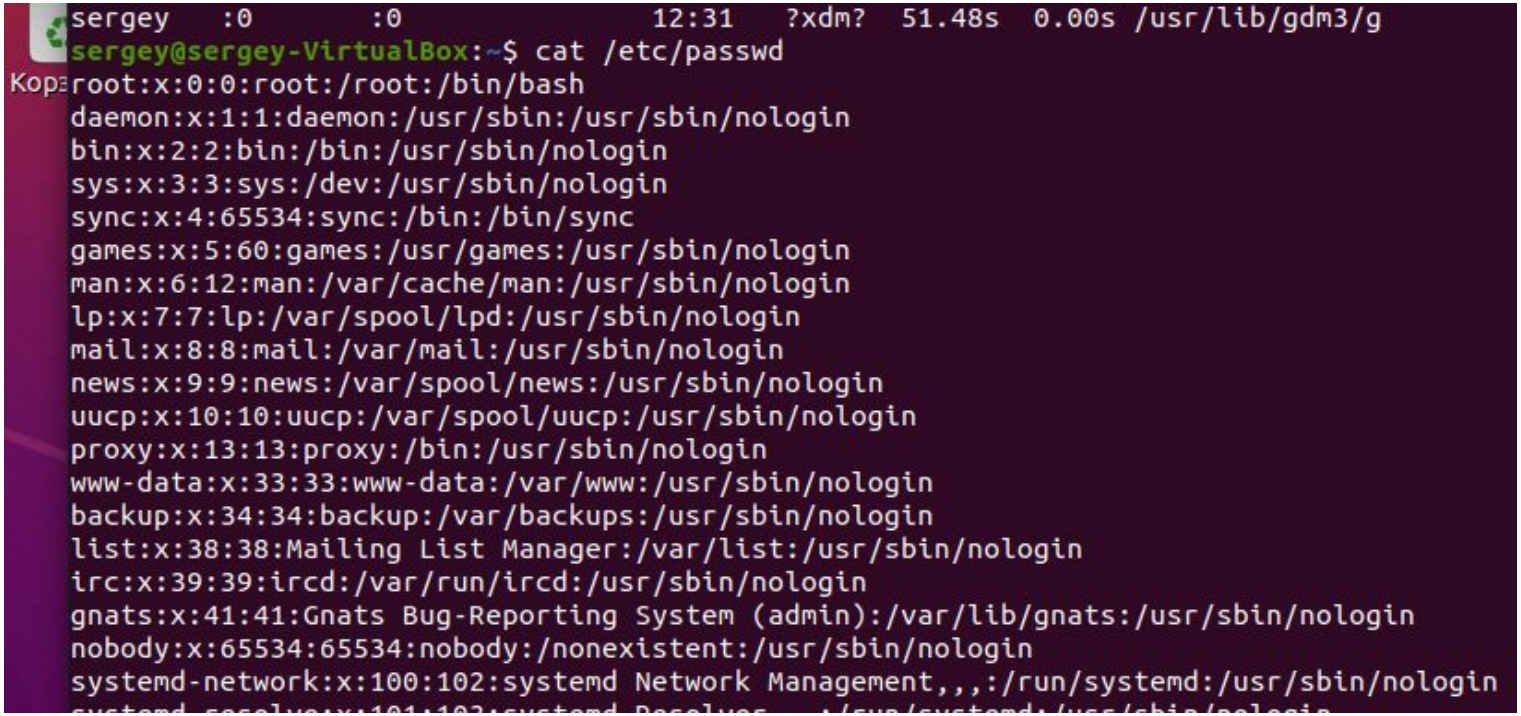
Каждый аккаунт занимает одну строку, в формате

account:password:UID:GID:GECOS:directory:shell

- **account** — имя пользователя.
- **password** — зашифрованный пароль пользователя.
- **UID** — идентификационный номер пользователя.
- **GID** — идентификационный номер основной группы пользователя.
- **GECOS** — необязательное поле, используемое для указания дополнительной информации о пользователе (например, полное имя пользователя).
- **directory** — домашний каталог ($HOME) пользователя.
- **shell** — командный интерпретатор пользователя (обычно /bin/sh).

Источник: ссылка

Хранение информации о пользователях



Запись /usr/sbin/nologin говорит о том, что данный пользователь не может входить в систему. Такие пользователи нужны для запуска программ, имеющих ограниченные права, и им, естественно, не нужно входить в систему.

Источник: ссылка

Работы с пользователями

Получение информации о пользователях

w – вывод информации (имя пользователя, рабочий терминал, время входа в систему, информацию о потребленных ресурсах CPU и имя запущенной программы) о всех вошедших в систему пользователях.

who – вывод информации (имя пользователя, рабочий терминал, время входа в систему) о всех вошедших в систему пользователях.

who am i или whoami или id – вывод вашего имени пользователя.

users – вывод имен пользователей, работающих в системе.

id <имя_пользователя> – вывод о идентификаторах пользователя: его uid, имя_пользователя, gid и имя первичной группы и список групп в которых состоит пользователь

groups <имя_пользователя> – вывод списка групп в которых состоит пользователь.

Источник: ссылка

Добавление пользователя useradd

Добавление пользователя осуществляется при помощи команды **useradd**.

- sudo useradd ivanovv

useradd — не интерактивная утилита;
adduser — интерактивная утилита;

Ключи:
-b *Базовый каталог*. Это каталог, в котором будет создана домашняя папка пользователя. По умолчанию */home*.

-c Комментарий. В нем вы можете напечатать любой текст.

-d Название домашнего каталога. По умолчанию название совпадает с именем создаваемого пользователя.

-e *Дата, после которой пользователь будет отключен*. Задается в формате ГГГГ-ММ-ДД. По умолчанию отключено.

-f *Количество дней, которые должны пройти после устаревания пароля до блокировки пользователя*, если пароль не будет изменен (период неактивности). Если значение равно 0, то запись блокируется сразу после устаревания пароля, при -1 - не блокируется. По умолчанию -1.
-g *Первичная группа пользователя*. Можно указывать как GID, так и имя группы. Если параметр не задан будет создана новая группа название которой совпадает с именем пользователя.

Источник: ссылка

Добавление пользователя useradd

-G Список вторичных групп в которых будет находится создаваемый пользователь

-k *Каталог шаблонов. Файлы и папки из этого каталога будут помещены в домашнюю папку пользователя. По умолчанию /etc/skel*.

-m Ключ, указывающий, что необходимо создать домашнюю папку. По умолчанию домашняя папка не создается.

-p *Зашифрованный пароль пользователя*. По умолчанию пароль не задается, но учетная пользователь будет заблокирован до установки пароля.

-s Оболочка, используемая пользователем. По умолчанию */bin/sh*.

-u Вручную задать UID пользователю.

Если при создании пользователя не указываются дополнительные ключи, то берутся настройки по умолчанию. Посмотреть настройки по умолчанию можно с помощью команды useradd -D.

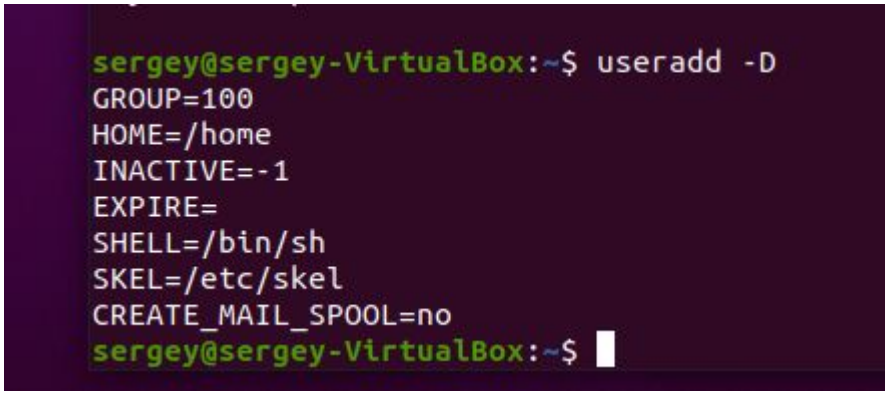
Если вас не устраивают такие настройки, вы можете поменять их выполнив sudo useradd -D -s /bin/bash, где -s это ключ из таблицы выше.

Источник: ссылка

Добавление пользователя useradd

Для предоставления дефолтных настроек при добавлении пользователя, введите:

useradd –D



Также обратите внимание на параметр:

GROUP=100. В Debian пользовательские группы начинаются с 1000, а в RHEL с 500, поэтому в современных системах этот параметр игнорируется. Все параметры, кроме **SKEL**, могут быть изменены, но практический смысл это имеет только для **HOME** и **SHELL**.

Источник: ссылка

Добавление пользователя

Например, мы обслуживаем веб-сервер и хотим создавать домашние директории в каталоге веб-сервера, в этом случае можно выполнить:

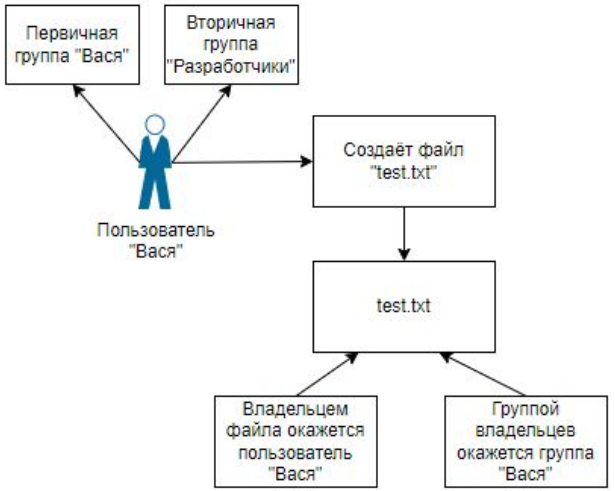
useradd -D -b /var/www/home

А для изменения командной оболочки:

useradd -D -s /bin/bash

Чтобы добавить нового пользователя введите:

useradd -m ivanovii



Ключ **-m** предписывает создать домашний каталог пользователя. Это самый простой вариант использования, но при использовании дополнительных ключей мы можем сразу задать или переопределить многие параметры пользователя.

Источник: ссылка

Добавление пользователя

Например:

useradd -m -b /var/www/ivanovii -g webadmins -G www-data -k /etc/myskel -s /sbin/nologin ivanovii

Этой командой мы создадим пользователя **ivanovii**, которому назначим домашнюю директорию в **/var/www/ivanovii**, для которой будет использован шаблон из **/etc/myskel**, включим его в основную группу **webadmins** и дополнительную **www-data**.

Также запретим ему интерактивный вход в систему, назначив оболочкой **/sbin/nologin**.

- Созданная учетная запись будет заблокирована до тех пор, пока мы не установим для нее пароль, это можно сделать следующей командой:
- passwd ivanovii

которая установит пароль к учетной записи ivanovii. Для блокировки пароля используйте:

- passwd -l ivanovii

Источник: ссылка

Изменение пользователей usermod

Изменение параметров пользователя происходит с помощью утилиты **usermod**.

Пример использования:

sudo usermod -c "Эта команда поменяет комментарий пользователю" ivanovii

Изменить пароль пользователю можно при помощи утилиты **passwd**.

sudo passwd ivanovii

Утилита passwd может использоваться и обычным пользователем для смены пароля.

Основные ключи passwd:

-d Удалить пароль пользователю. После этого пароль будет пустым, и пользователь сможет входить в систему без предъявления пароля.

-e Сделать пароль устаревшим. Это заставит пользователя изменить пароль при следующем входе в систему.

-i Заблокировать учетную запись пользователя по прошествии указанного количества дней после устаревания пароля.

-n Минимальное количество дней между сменами пароля.

-x Максимальное количество дней, после которого необходимо обязательно сменить пароль.

-L Заблокировать учетную запись пользователя.

-U Разблокировать учетную запись пользователя.

Источник: ссылка

Изменение пользователей

Опция	Назначение опций команды passwd
-s	Показывает атрибуты пароля для регистрационного_имени пользователя. Любой пользователь может задавать данную опцию.
-l	Блокирует запись пароля для регистрационного_имени.
-d	Удаляет пароль для регистрационного_имени, так что у пользователя с этим регистрационным_именем пароль не запрашивается.
-f	Заставляет пользователя изменить пароль при следующей регистрации в системе, делая пароль для регистрационного_имени устаревшим.
-x max	Задает для пользователя с указанным регистрационным_именем количество дней, в течение которых пароль будет действителен.
-n min	Задает минимальное количество дней между изменениями пароля для пользователя с указанным регистрационным именем. Всегда используйте эту опцию с опцией -x, если только max не установлен в -1 (устаревание отключено). В этом случае, min устанавливать не нужно.
-w warn	Задает, за сколько дней (относительно max) пользователя с данным регистрационным_именем будут предупреждать о предстоящем устаревании пароля.
-s -a	Показывает атрибуты паролей для всех пользователей.

Источник: ссылка

/etc/default/passwd

Стандартные значения атрибутов

Присваивая значения набору параметров в файле **/etc/default/passwd**, администратор может управлять устареванием и длиной паролей. Можно задать следующие параметры:

MINWEEKS Минимальное количество недель перед тем, как пароль можно будет изменить. Сразу после установки системы этот параметр имеет значение 0.

MAXWEEKS Максимальное количество недель, в течение которых пароль можно не изменять. Сразу после установки системы этот параметр имеет значение 24.

WARNWEEKS Количество недель перед устареванием пароля, когда необходимо предупреждать пользователя. Сразу после установки системы этот параметр имеет значение 1.

PASSLENGTH Минимальное количество символов в пароле. Сразу после установки системы этот параметр имеет значение 6. Обратите внимание, что аргументы опций команды **passwd** (**min**, **max** и **warn**), а также соответствующие поля файла **/etc/shadow** задают параметры устаревания в днях; тогда как соответствующие поля файла **/etc/default/passwd** (**MINWEEKS**, **MAXWEEKS** и **WARNWEEKS**) - в неделях.

Источник: ссылка

Изменение пользователей

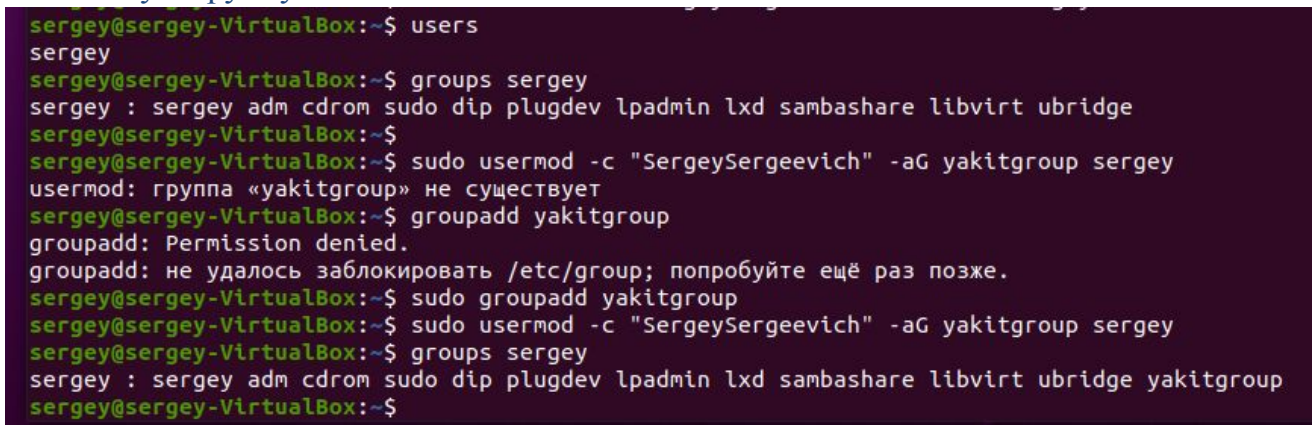
Например:

usermod -c «Sergey Sergeevich" -aG sudo sergey

-a добавляет к текущим группам пользователя дополнительные. Без этой опции группы заменяются на новые, а с этой опцией к старым группам добавляются новые;

-G указывает, что работать будем с дополнительными группами а не с первичной.

- Данная команда создаст новый комментарий к учетной записи и добавит пользователя **sergey** в дополнительную группу **sudo**.



Установка пустого пароля пользователя

Суперпользователь с помощью утилит командной строки **passwd** и **usermod** или путем редактирования файла */etc/shadow* может удалить пароль пользователя, дав возможность входить в систему без указания пароля.

sudo passwd -d ivanovii или sudo usermod -p "" ivanovii

После этого имеет смысл принудить пользователя установить себе новый пароль при следующем входе в систему.

sudo passwd -e ivanovii

Источник: ссылка

Удаление пользователя userdel

Для того, чтобы удалить пользователя воспользуйтесь утилитой **userdel**.

sudo userdel **ivanovii**

Пример использования:

-f Принудительно удалить пользователя, даже если он сейчас работает в системе.

-r Удалить домашний каталог пользователя.

Источник: ссылка

Работа с группами

Управление группами

Создание группы

Программа **groupadd** создаёт новую группу согласно указанным значениям командной строки и системным значениям по умолчанию.

sudo groupadd yakitgroup

- **groupadd** — не выводит ничего при создании группы;
- **addgroup** — выводит создаваемый **gid** при создании группы.

Основные ключи:

- -g Установить собственный GID.
- -p Пароль группы.
- -r Создать системную группу.

Источник: ссылка

Управление группами

Файл /etc/group. Просмотр настроек групп.

- Этот файл соотносит числовые идентификаторы групп с символьными именами. Каждая строка файла **/etc/group** содержит четыре поля.

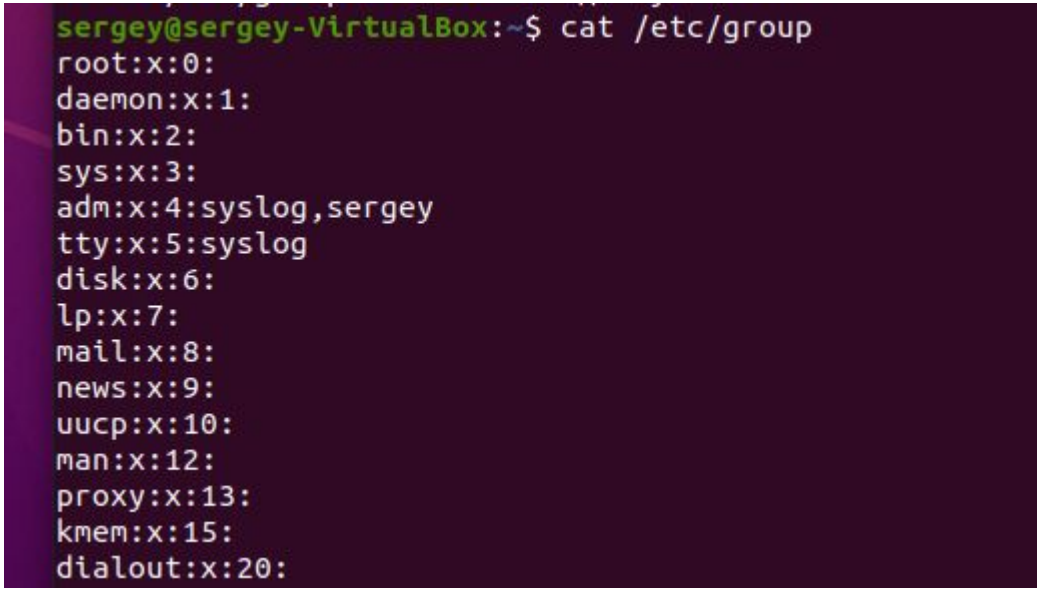
Поле	Назначение
Имя группы	Содержит (уникальное) символьное имя группы.
Пароль группы	Группы могут иметь пароли, хотя использование паролей групп - явление редкое. В примере данное поле пустое - это значит, что пароль отсутствует.
Идентификатор группы	Содержит числовой идентификатор группы.
Список пользователей	Содержит список регистрационных имен пользователей данной группы. Имена в этом списке разделяются запятыми. Пользователи могут принадлежать к нескольким группам и, при необходимости, переключаться между ними с помощью команды newgrp.

Источник: ссылка

Управление группами

Файл /etc/group. Просмотр настроек групп.

- Этот файл соотносит числовые идентификаторы групп с символьными именами. Каждая строка файла **/etc/group** содержит четыре поля.



Источник: ссылка

Управление группами

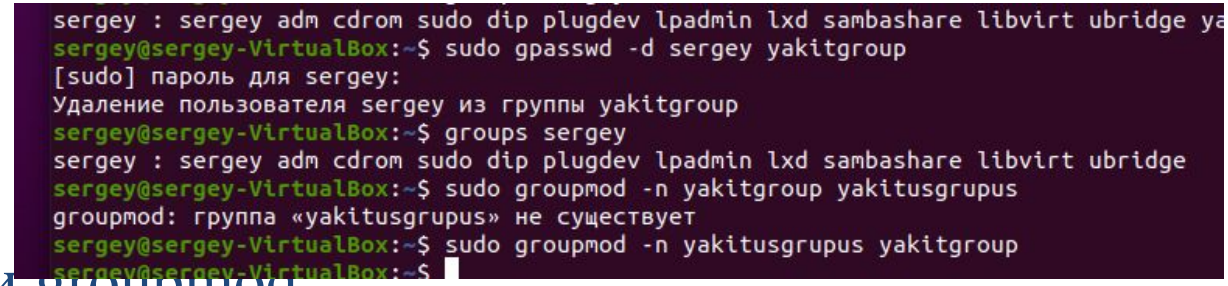
Изменение группы

Сменить название группы, ее GID или пароль можно при помощи **groupmod**.

sudo groupmod –n [новоеимя] [староеимя]

sudo groupmod -n newtestgroup testgroup

Имя группы изменено с testgroup на newtestgroup



Опции groupmod:

- -g Установить другой GID.
- -n Новое имя группы.
- -p Изменить пароль группы

Источник: ссылка

Управление группами

Удаление группы

Утилита **groupdel** не имеет никаких дополнительных параметров.

- sudo groupdel testgroup

Для того, чтобы проверить членство пользователя в группах используйте команду:

- groups ivan

где **ivan** - имя пользователя.

Чтобы быстро удалить пользователя из всех дополнительных групп используйте:

- usermod -G "" ivan

Источник: ссылка

Управление группами

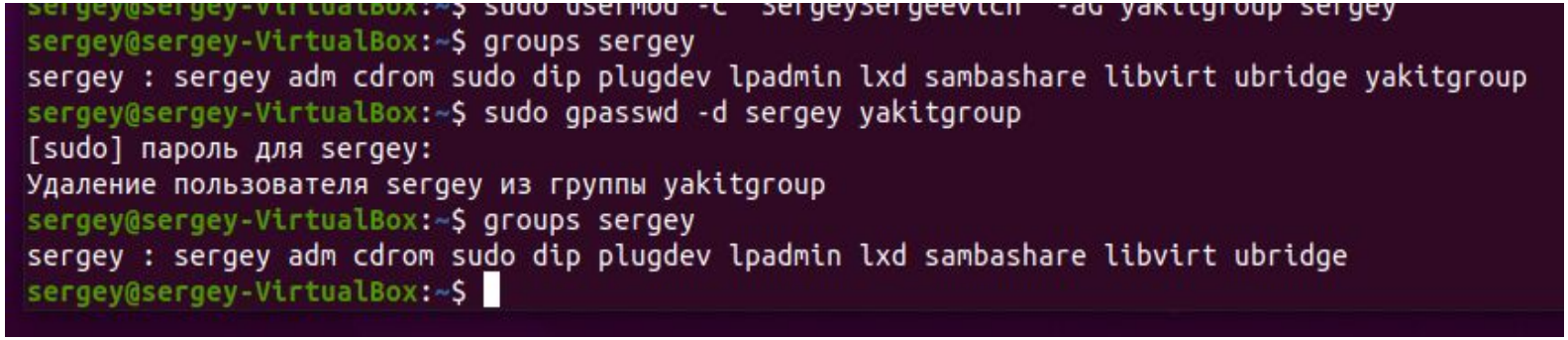
Управление пользователями группы

Для управления пользователями группы используется утилита **gpasswd**. Чтобы занести пользователя в группу:

- gpasswd -a [user] [group]

Вывод пользователя из группы:

- gpasswd -d [user] [group]



Источник: ссылка

Управление доступом

У каждого объекта в Linux есть свой идентификатор, а так же права доступа, применяемые к данному идентификатору. Идентификатор есть у пользователя - *UID*, у группы - *GID*, у файла - *inode*.

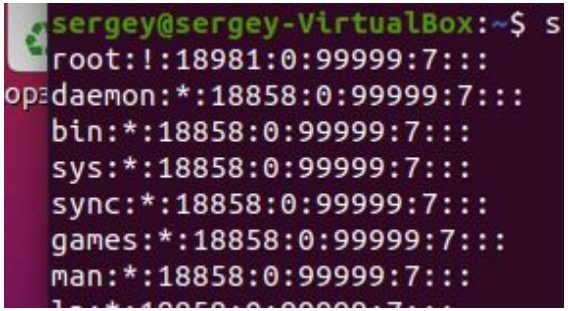
Собственно **inode** является, как идентификатором файла/каталога, так и сущностью, которая содержит в себе информацию о файле/каталоге. Например такую, как: принадлежность к владельцу/группе, тип файла и права доступа к файлу.

Источник: ссылка

Файл /etc/shadow

Этот файл используется в системах с теневым хранением паролей, где они вынесены из доступного всем пользователям на чтение файла /etc/passwd для повышения безопасности системы. Здесь (помимо собственно зашифрованных паролей) хранятся дополнительные ограничения, связанные с регистрационным именем и паролем пользователя. Доступ к этому файлу на чтение имеет только пользователь root, а работают с ним команды passwd и login.

Номер поля	Назначение
1	Имя пользователя.
2	Зашифрованный по особому алгоритму (обычно, DES или MD5) пароль.
3	Количество дней между 01.01.1970 (началом эры UNIX) и днем последнего изменения пароля.
4	Минимальное количество дней между изменениями пароля.
5	Срок действия пароля пользователя.
6	За сколько дней система будет начинать предупреждать пользователя о необходимости изменения пароля.
7	Сколько дней пользователь может не работать в системе, прежде чем его регистрационное имя будет заблокировано.
8	Дата, после которой имя пользователя нельзя будет использовать в системе.



Источник: ссылка

Системные регистрационные имена

- Каждая версия ОС UNIX резервирует несколько специальных регистрационных имен для предопределенных системных целей. Так, в UNIX SVR4 системными считаются регистрационные имена, соответствующие идентификаторам от 0 до 100.

Регистрационное имя	Назначение
root	Регистрационное имя суперпользователя, администратора системы, соответствующее идентификатору 0. Единственное имя, обязательно имеющееся в любой UNIX-системе. Пользователь root не связан никакими ограничениями по доступу. Для выполнения большинства программ администрирования используется регистрационное имя root, обеспечивающее гарантированный доступ к необходимым ресурсам.
daemon	Владелец процессов, реализующих пользовательские службы.
sys	Владелец выполняемых пользовательских системных команд UNIX (часто соответствует идентификатору 0).
bin	Владелец стандартных пользовательских утилит UNIX (часто соответствует идентификатору 0).
adm	Псевдопользователь, владеющий файлами системы журнализации.
cron	Псевдопользователь, владеющий соответствующими файлами, от имени которого выполняются процессы подсистемы запуска программ по расписанию.
news	Псевдопользователь, от имени которого выполняются процессы системы телеконференций (дискуссионных групп или групп новостей).
nobody	Псевдопользователь, используемый при работе сетевой файловой системы NFS.
uucp	Псевдопользователь подсистемы UUCP, позволяющий передавать почтовые сообщения и файлы между UNIX-хостами.
lp, lpd	Псевдопользователь, от имени которого выполняются процессы системы печати, владеющий соответствующими файлами.

Источник: ссылка

Итоги

- Научились смотреть информацию о пользователе командой **id**. А также поняли что такое **uid** и **gid**.
- Узнали как создавать пользователей командами **useradd** и **adduser**.
- Узнали как удалять пользователей командами **userdel** и **deluser**.
- Научились менять пароль пользователю командой **passwd**.
- Создавали группы командами **groupadd** и **addgroup** и удаляли группы командами **groupdel** и **delgroup**.
- Научились различать первичную и дополнительную группы.
- Научились добавлять пользователей в группы командами **usermod** и **adduser**, удалять пользователей из группы командой **deluser**, а также менять пользователю первичную группу командой **usermod**.
- Узнали про конфигфайлы **/etc/passwd**, **/etc/group**, **/etc/shadow**.