

Пользователи.
Группы.
Права доступа.

SKILLFACTORY



Содержание

- ☒ Пользователи и группы — понятие бюджета
- ☐ Права доступа — чтение, запись, выполнение
- ☐ Команды — управление пользователями и правами

Бюджет пользователя

Учетная запись пользователя

Необходимая для системы информация о пользователе, хранящаяся в специальных файлах

Информация об учетных записях пользователей

/etc/passwd

Аутентификация

Процедура проверки пользователя по реквизитам

Защищенная информация о пользователях

/etc/shadow

Авторизация

Выдача прав доступа пользователю

Бюджет пользователя

`/etc/passwd`

`vagrant:x:1001:1001:vagrant,,,:/home/vagrant:/bin/sh`

- имя пользователя
- x(в `/etc/shadow`)
- UID – числовой идентификатор пользователя
- GID – числовой идентификатор группы
- полное имя пользователя
- путь к домашнему каталогу
- путь к оболочке входа

`/etc/shadow`

`vagrant:6.n.:17736:0:99999:7:::`

- имя пользователя
- соленый хеш пароля
- последнее изменение пароля
- минимальный возраст пароля
- максимальный возраст пароля
- период предупреждения
- период бездействия
- срок годности
- зарезервированное поле

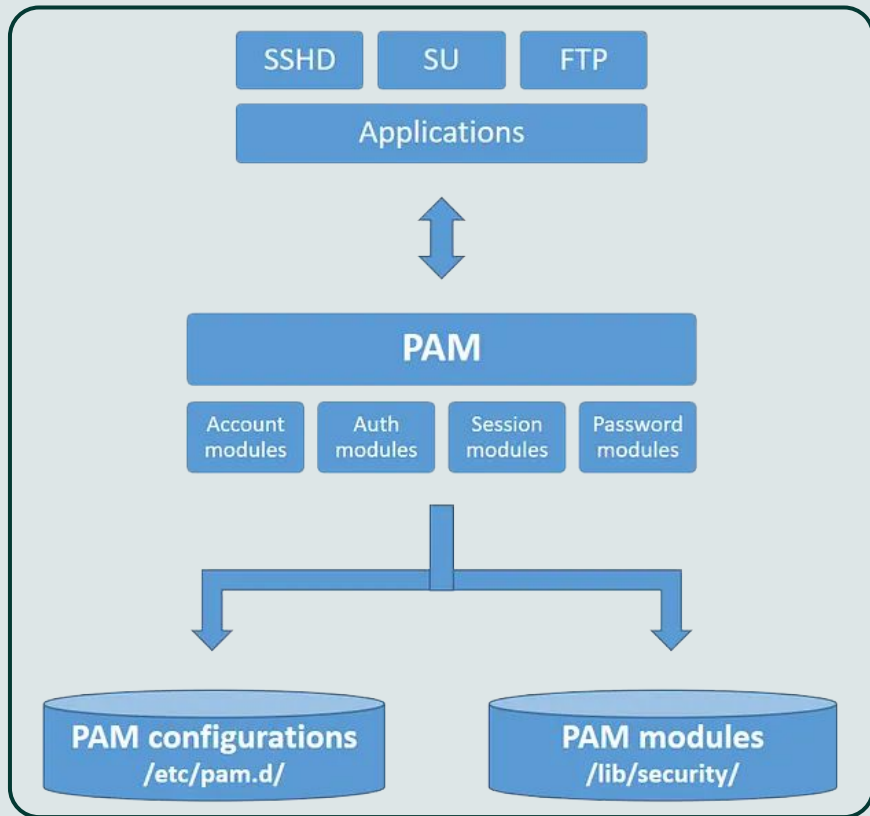
PAM

Подгружаемые Модули Аутентификации

Осуществляет процесс
аутентификации пользователя

Тип модуля:

- **auth**: проверка пользователя и выдача привилегий;
- **account**: контроль распределения ресурсов, бюджета пользователя;
- **session**: действия перед выдачей доступа
- **password**: проверка секрета на подлинность



Группы

Совокупность пользователей

Основная цель – **определение набора привилегий**, которые могут быть совместно использованы пользователя внутри группы

Первичная группа (группа входа в систему) – назначается файлам, создаваемым пользователем

Вторичная группа – предоставление дополнительных привилегий

Информация о группах в которые входят пользователи

/etc/group

Защищенная информация о группах

/etc/gshadow

Группы

/etc/group

vagrant:x:1000

- имя группы
- x(в /etc/gshadow)
- GID – числовой идентификатор группы
- имя пользователей, включенных в несколько групп

/etc/gshadow

vagrant:\$6\$.n.:17736:0:99999:7:::

- имя пользователя
- соленый хеш пароля
- последнее изменение пароля
- минимальный возраст пароля
- максимальный возраст пароля
- период предупреждения
- период бездействия
- срок годности
- зарезервированное поле

Содержание

- ☒ Пользователи и группы — понятие бюджета
- ☒ Права доступа — чтение, запись, выполнение
- ☐ Команды — управление пользователями и правами

Примеры записи прав доступа в **двоичной** форме:

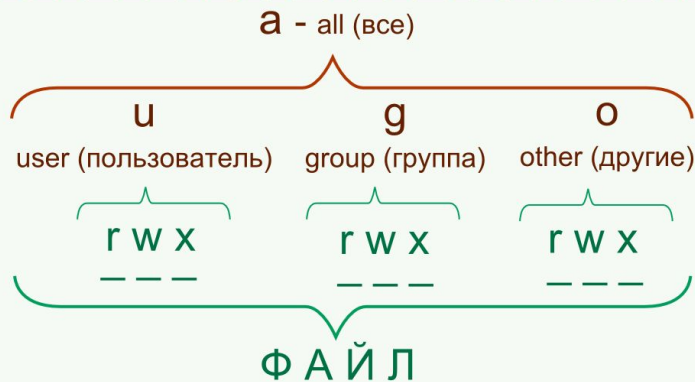
110 110 110 (все могут читать и изменять)
111 000 000 (полный доступ имеет владелец файла)
110 100 100 (все могут читать, владелец также изменять)
111 101 101 (все могут читать и исполнять, владелец также изменять)

Перевод представления прав доступа к **восьмеричной** форме:

гwx- представление	Двоичное число	Восьмеричное число	Значение
- - -	0 0 0	0	Все запрещено
- - x	0 0 1	1	
- w -	0 1 0	2	
- w x	0 1 1	3	
r - -	1 0 0	4	Только чтение
r - x	1 0 1	5	Чтение и исполнение
r w -	1 1 0	6	Чтение и запись
r w x	1 1 1	7	Все разрешено

Примеры записи прав доступа в **восьмеричной** форме:

666 (все могут читать и изменять)
700 (полный доступ имеет владелец файла)
644 (все могут читать, владелец также изменять)
755 (все могут читать и исполнять, владелец также изменять)



r - read (чтение) **W** - write (запись) **X** - execution (исполнение)

Примеры:

r w - r w - r w - (все могут читать и изменять)
r w x - - - - - (полный доступ имеет владелец файла)
r w - r - - r - - (все могут читать, владелец также изменять)
r w x r - x r - x (все могут читать и исполнять, владелец также изменять)

Содержание

- Пользователи и группы — понятие бюджета
- Права доступа — чтение, запись, выполнение
- Команды — управление пользователями и правами

Команды - пользователи

- **useradd** – создание пользователя с явным указанием параметров бюджета
- **adduser** – пошаговое создание пользователя с параметрами из файла `/etc/adduser.conf`
- **userdel** – удаление регистрационное имя пользователя из системы
- **deluser** – удаление пользователей исходя из информации из файла `/etc/deluser.conf`
- **passwd** – изменения пароля пользователя
- **chfn** – изменение реального имени пользователя и информации о нем
- **usermod** – изменение бюджета пользователя
- **finger** – информация о пользователях в системе
- **change** – изменение параметров пароля пользователя

Команды - группы

- **groupadd** – создать группу
- **addgroup** - создание группы с параметрами из файла /etc/adduser.conf
- **groupdel** – удаление группы
- **delgroup** - удаление группы с параметрами из файла /etc/deluser.conf
- **groupmems** – управление членами первичной группы пользователя
- **gpasswd** – изменение параметров группы
- **groupmod** – изменение параметров группы

Команды - права

→ **chmod** – изменяет права доступа к файлам:

- ♦ u,g,o,a – установка прав для пользователя, группы, остальных и всех соответственно
- ♦ +,-,= - добавить, удалить, установить права соответственно
- ♦ r,w,x,u,g,o – право чтения, записи, выполнения, как у владельца, как у группы, как у остальных.

Альтернатива: 744(rwxr--r--)

→ **chown** – смена владельца файла:

- ♦ format: user:group
- ♦ R – изменение владельца вложенных файлов и каталогов

→ **umask** – задание маски доступа по умолчанию:

- ♦ -p : вывести текущую маску в восьмеричном виде
- ♦ -S : вывести текущую маску в буквенном виде

Ссылки

- Ubuntu manuals:
https://manpages.ubuntu.com/manpages/kinetic/en/man8/group_mems.8.html
- PAM
https://www.opennet.ru/base/dev/pam_linux.txt.html
- Права доступа:
<https://www.opennet.ru/docs/RUS/linuxadmin/lesson04.html>