**Лабораторная работа 2. Работа с файлами и каталогами. Управление пользователями**

**Цель**: Познакомиться с принципами аутентификации, форматами файлов для хранения учетных записей и изучить команды для управления учетными записями.

**Теория:**

Linux — многопользовательская система, учётная запись — это информация о пользователе а системная политика представляет собой правила работы в системе.

При создании нового пользователя следует соблюдать правила при выборе имени пользователю. Имя может содержать символы латинского алфавита, цифры, \_, $,[a-z\_][a-z0-9\_]\*[$]. Нельзя использовать пробел, : @,#, т.д. и специальные символы (табуляция, конец строки).

Учётная запись пользователя – это необходимая для операционной системы информация о пользователе, хранящаяся в специальных файлах. Информация используется Linux для аутентификации пользователя и назначения ему прав доступа.

Аутентификация – системная процедура, позволяющая операционной системе определить, какой именно пользователь осуществляет вход. Вся информация о пользователе обычно хранится в файлах /etc/passwd и /etc/group. В файле /etc/passwd содержится информация о пользователях. Запись для каждого пользователя занимает одну строку.

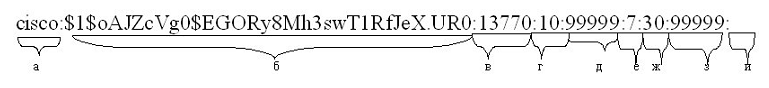


Рисунок 1 - Запись информации о пользователе в файл/etc/passwd

На рисунке 1 показана структура записи о пользователя, в которую входит следующая информация:

* а – имя пользователя;
* б – шифрованный пароль – применяются алгоритмы хеширования, как правило MD5 или символ '!', в случаях, когда интерактивный вход пользователя в систему запрещен;
* в – число дней с последнего изменения пароля, начиная с 1 января 1970 года;
* г – число дней, перед тем как пароль может быть изменен;
* д – число дней, после которых пароль должен быть изменен;
* е – число дней, за сколько пользователя начнут предупреждать, что пароль устаревает;
* ж – число дней, после устаревания пароля для блокировки учетной записи;
* з –дней, отсчитывая с 1 января 1970 года, когда учетная запись будет заблокирована;
* и – зарезервированное поле;

При добавлении нового пользователя происходит новая запись в /etc/passwd и /etc/shadow, создаётся домашний каталог. Каталог /etc/skel содержит файлы, которые копируются в создаваемый домашний каталог пользователя.

Добавляя нового пользователя чаще всего используются опции команды useradd такие как:

* s — файл оболочки по умолчанию;
* d — путь к домашнему каталогу;
* m — необходимо создавать домашний каталог;
* M — не создавать домашний каталог;
* k — путь к альтернативному каталогу скелета;
* u — назначить UID;
* g — назначить GID (первичную группу);
* G — список групп пользователя;
* e — дата блокировки учетной записи;
* f — срок после устаревания пароля до блокировки учетной записи.

Если пользователь не имеет право входить в сеанс, то ему в качестве оболочки нужно указать:

* /bin/false — команда, всегда возвращающая код ошибки;
* /dev/null — специальный файл-поглотитель;
* /sbin/nologin — возвращает код ошибки и сообщение о невозможности входа в сеанс.

Управление паролями в Linux - часть системной политики. Управляя паролями требуется определить категорий пользователей, которые могут сами выбирать пароль, правила выбора паролей и требования к их уровню сложности, сроки устаревания паролей, длительность периода запрета на изменение пароля. Это является типичными правилами при управлении паролями.

Опции при управлении паролями:

* -l — блокировка;
* -u — разблокирование;
* -S — текущее состояние пароля;
* -d — удаление пароля;
* -n — период запрета смены пароля;
* -x — максимальный срок использования пароля;
* -w — период предупреждений;
* -i — период после устаревания пароля до блокировки.

Группы пользователей очень удобный механизм администрирования пользователей в ОС Linux. Информация о группах пользователей хранится в файле /etc/group. Запись для каждой группы пользователей так же занимает одну строку как и в /etc/passwd. Строка в /etc/group имеет следующую структуру: <имя группы>:<пароль группы>:<GID группы>:<список пользователей>.

В файлах профиля пользователя устанавливаются переменные окружения. PATH- путь поиска исполняемых файлов, USER- имя пользователя, HOME- путь к домашнему каталогу. Так же в профиле пользователя хранятся настройки пользователя, файл сценария оболочки, который выполняется автоматически при входе в сеанс и umask. Umask - это права на доступ к файлам и каталогам по умолчанию.

Файл ~/.bashrc — это ресурс оболочки (для пользователя), выполняется только при запуске оболочки из командной строки (в отличие от файлов профиля), содержит дополнительные настройки оболочки /etc/bashrc — общесистемный файл ресурсов оболочки (удобно задавать псевдонимы для команд).

При входе в сеанс bash исполняются:

1. /etc/profile;

2. ~/.bash\_profile;

3. ~/.bashrc;

4. /etc/bashrc.

Если выполняется запуск оболочки из командной строки выполняются 3) и 4).

Отчёты об активности пользователей хранятся в файлах как и прочая информация в ОС Linux. В файле /var/run/utmp хранится список пользователей, находящихся в сеансе, в файле /var/log/wtmp хранится информация об открытых и законченных сеансах пользователей, файл /var/log/lastlog хранит информацию о последних входах в сеанс.

Опции команды who:

* -b — время последней загрузки системы;
* -H — печать заголовка;
* -login — информация о системных процессах, контролирующих вход в сеанс;
* -q — имена всех пользователей в системе и их количество;
* -u — подробная информация о сеансах;
* -a — полная информация о статусе процессов, контролирующих вход в сеанс.

Опции команды lastlog:

* -b — входы в сеанс, ранее указанного количества дней;
* -t — входы в сеанс, за указанный период;
* -u — входы в сеанс пользователя.

Таблица 1 - Команды для администрирования пользователей и учетных пользователей

|  |  |
| --- | --- |
| Описание | Команда |
| регистрация нового пользователя | useradd <username> |
| получить информацию о пользователе | id <username> |
| выдать настройки команды по умолчанию | useradd –D |
| изменение учетной записи | usermod <options> <username> |
| удаление учетной записи | userdel <username> |
| управление паролями | passwd <options> <username> |
| создание группы | groupadd <groupname> |
| удаление группы | groupdel <groupname> |
| назначение администратора группы | gpasswd –A <username> <groupname> |
| добавление пользователя к группе, удаление пользователя из группы (администратором группы) | gpasswd –a <username> <groupname>, gpasswd –d <username> <groupname> |
| задать пароль на вход в группу для не членов группы | gpasswd <password> |
| изменить текущую группу | newgrp <groupname> |
| выполнить файл профиля | source <profile\_file> |
| список пользователей, находящихся в сеансе | who |
| информация об открытых и законченных сеансах | last |
| информация о последних входах в сеанс | lastlog |

**Практическая часть:**

1. Ознакомиться с содержимым файлов:

* /etc/passwd;
* /etc/shadow;
* /etc/group.

2. Создать следующие группы:

* Workers;
* Teachers;
* Students.

3. Создать пользователей user\_[номер варианта]\_ N, где N =1, 2, .., 5, uid учетной записи должен быть равен 1000+N. Пользователей с N, равным 1 и 2, добавить в группу workers вручную внеся изменения в конфигурационный файл. После добавления пользователей осуществить проверку файла /etc/group на ошибки. Пользователей с N, равным 3, 4 и 5, добавить в группу students при помощи команд администрирования. Проверьте результат, выполнив действия п.1.

4. Создать пользователя teacher\_[номер варианта]. В комментарии к учетной записи должны быть Ваше имя и фамилия. uid учетной записи должен быть равен 3000. Пользователя добавить в группу teachers.

5. Для всех пользователей задайте пароли, используя команду passwd.

6. Создать директорию labs в корневом каталоге. В нем создать каталоги library и tests.

7. Создать файлы book\_[фамилия студента]\_N и поместить их в library.

8. Создать текстовый файл test\_[имя студента], и поместить в tests. Файлы должны содержать скрипт на создание пользователя user[номер варианта] и задание ему пароля pass[номер варианта]. Сделайте эти файлы исполняемыми для пользователей группы students.

9. В директории labs создать файл list, который должен содержать список файлов директории /etc.

10. Дать право на изменение файла только пользователю teacher\_[номер варианта], а на чтение пользователям группы workers.

11. Настроить права доступа к каталогу library и tests, таким образом, чтобы пользователи группы teachers могли изменять и создавать там файлы, а пользователи группы students имели доступ на чтение.

12. Просмотрите файл /etc/shadow (с правами root). У всех ли пользователей содержимое второго поля выглядит приблизительно одинаково? Какие символы могут содержаться в шифрованной строке пароля в /etc/shadow?

13. Зарегистрируйте пользователя test1, для которого запрещен вход в сеанс, имеющего домашний каталог /home/nouser и являющегося членом групп user и mail. Пользователь должен иметь UID равный 2000.

14. Создайте учетную запись для пользователя test2 с настройками по умолчанию. Проверьте, создался ли домашний каталог пользователя, наполнен ли он файлами и какому пользователю он принадлежит.

15. Измените имя пользователя test2 на test3.

16. Удалите пользователя test3.

17. Помимо файла /etc/default/useradd имеется еще один конфигурационный файл, влияющий на поведение команды useradd. Найдите его и изучите его содержание. Какая настройка позволяет изменять минимальный UID для новых пользователей?

18. Зарегистрируйте пользователя test4 с настройками по умолчанию и установите для него пароль. Изучите содержимое соответствующей записи в /etc/shadow.

19. Установите дату устаревания пароля для пользователя на 31 декабря текущего года. Проверьте, что изменилось в /etc/shadow.

20. Удалите пароль пользователя и проверьте изменения в /etc/shadow.

21. Заблокируйте учётную запись test4.

22. Создайте группу пользователей xusers с GID, равным 1010.

23. Зарегистрируйте себя в качестве участника группы xusers. Проверьте результат выполненного действия.

24. Измените имя группы на yusers.

25. Сделайте так, чтобы при запуске оболочки из командной строки выдавалось приветствие.

26. Определите, когда последний раз была загружена система.

27. Кто входил в сеанс за последние 2 недели?