Лабораторная работа №2

Администрирование пользователей в ОС Red Hat Enterprise Linux 4.

Цель работы: получить навыки управления пользователями, группами, паролями, изучить особенности файловых прав данной ОС, механизмы получения особых привилегий и установки дисковых квот.

Данная лабораторная работа будет проводиться на сервере, работающем под управлением ОС RHEL 4, установленной в ходе лабораторной работы №1.

Краткие теоретические сведенья:

1.Механизм учетных записей.

В ОС RedHat Linux существует три типа пользователей: пользователь root, обычные пользователи и системные пользователи. Каждый пользователь имеет в системе учетную запись. Информация об учетных записях хранится в текстовом файле /etc/passwd. Зашифрованные пароли обычно хранятся /etc/shadow.

Системный пользователь – это не человек, а процесс, выполняющийся на компьютере. В отличии от обычных пользователей системные пользователи не имеют начальных каталогов и паролей, поэтому в систему нельзя войти под именем системного пользователя.

2.Идентификаторы пользователей и групп.

Компьютер – это машина, работающая с числами. Он идентифицирует пользователей по номерам, известным, как идентификатор пользователя (UID) и идентификатор группы (GID).

Пользователь root имеет неограниченные права в системе, его UID, GID равны 0.

Идентификаторы в диапазоне от 1 до 499 и 65534 зарезервированы для системных пользователей. Идентификаторы для людей начинаются с 500.

3.Права доступа

Права доступа бывают трех видов: чтение (read), запись (write), выполнение (execute), а также каждый вид прав имеет цифровой аналог 4, 2, 1 соответственно. При наличии нескольких видов прав одновременно цифры суммируются.

Команды изменения прав группы, пользователя или доступа к файлу или каталогу:

- chgrp – изменение принадлежности файла или каталога к определенной группе
- chown – изменяет владельца файла или каталога
- chmod – изменяет режим доступа к файлу или каталогу. Если при помощи команды chmod g+s [имя каталога].

Узнать текущие атрибуты/права доступа Вы можете при помощи команды ls –la.

4.Группы пользователей

Список групп содержится в файле /etc/group.

Ниже представлены наиболее часто используемые инструменты командной строки для управления группами:

- groupadd - создание новой группы;
- groupdel – удаление существующей группы;
- groupmod – модификация параметров группы (ключи: -g, -n)
- gpasswd – создание пароля группы (ключ: -A -создание администратора группы);
- useradd -G – использование команды с данным аргументом позволяет добавить пользователя к определенной группе при создании учетной записи;
- usermod -G – добавление пользователя к группе;
- grpck – проверка файла /etc/group на ошибки.

Система Red Hat Enterprise Linux предоставляет администратору и графический интерфейс system-config-users, но опытные администраторы предпочитают использовать консоль.

5.Управление пользователями

Первым делом необходимо создать учетную запись пользователя с предоставлением UID, создать начальный каталог, поместить туда стандартный набор файлов. Во-вторых, пользователя следует отнести к определенным группам и определить, какой объем дискового пространства он может использовать.

В Red Hat имеется несколько инструментов командной строки для управления пользователями, такие как useradd, userdel, passwd, usermod. При создании пользователя в каталоге /etc/skel содержится набор файлов, который помещается в начальный каталог пользователя.

- useradd – создание нового пользователя;
- userdel - используется для удаления учетной записи пользователя, при этом будет удален и начальный каталог пользователя;
- passwd - задает пароль пользователя (ключ: -l – заблокировать учетную запись пользователя);
- usermod - команда изменяет атрибуты пользователя (ключи: -s, -u).
- useradd user –p password –u 1000.

6.Механизмы получения особых привилегий

Бывают случаи, когда обычным пользователям требуется запускать команды с правами других пользователей. При помощи команды su существует возможность заменить пользователя на любого другого пользователя системы. Используя команду sudo возможно обычному пользователю выполнять команды, доступные лишь суперпользователю. Список авторизованных пользователей содержится в файле /ets/sudoers.

7.Дисковые квоты

В больших системах, в которых работает много пользователей, обязательно возникает необходимость контролировать дисковое пространство, которое занимают пользователи. Для управления дисковыми квотами должен быть проинсталлирован программный пакет quota.

Ход работы:

В ходе работы необходимо изучить теоретические сведенья, связанные с администрированием пользователей, а также проделать практические задания и ответить на контрольные вопросы, описанные ниже.

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*.

Если у Вас возникли вопросы по поводу использования тех или иных ключей воспользуйтесь командой man для получения справки: man [имя команды].

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

Контрольные вопросы:

1. Почему в конфигурационных файлах пароли не хранятся в явном виде?
2. Почему не рекомендуется выполнять повседневные операции, используя учетную запись root?
3. В чем отличие механизмов получения особых привилегий su и sudo?
4. При выполнении команды ls –la получаем результат:
-rw-r-x-r-- 1 den factory 4464 30 May 2008 text.txt. Что это значит?
5. Как задать права на каталог и все объекты в нем содержащиеся?