Лабораторная работа № 1
Создание базовой конфигурации

Цель работы: Изучить типы учетных записей пользователей, ознакомиться с основными принципами управления учетными записями. Изучить основы разграничение доступа пользователей.

Операционные системы: Debian 8

Теоретический материал

Пользователь – это человек, пользующийся ресурсами и возможностями, которые ему предоставляет тот или иной сервис. Пользователь не обязан знать все аспекты функционирования этих сервисов, все, что ему необходимо знать – это как пользоваться ими.

В Linux каждый пользователь имеет свой уникальный числовой идентификатор, по которому он идентифицируется в системе. Этому идентификатору для более удобной работы соответствует имя пользователя. Например, для привилегированного пользователя root зарезервирован нулевой идентификатор.

Все имена пользователей Linux и соответствующие им идентификаторы хранятся в специальном файле passwd. Этот файл располагается в каталоге etc, который, в свою очередь, находится в корневом каталоге системы /. Файл имеет обычную текстовую форму.

Пример строки файла:

root:x:0:0:root:/root:/bin/bash

Структура строки:

login : password : UID : GID : GECOS : home : shell

Каждая запись в файле разделена двоеточиями на 7 частей:

1. Регистрационное имя или логин. Это поле содержит регистрационное имя пользователя. Для операционной системы не важно, какое имя имеет пользователь, система ориентируется на идентификатор, а имя играет, пожалуй, только информационное значение для человека, работающего в системе.

2. Поле пароля. Это поле в ранних версиях Linux содержало зашифрованный пароль, а теперь, когда была введена технология теневых паролей, в этом поле просто ставится *x*. Практического применения это поле не имеет.
3. Идентификатор пользователя (UID). В системе Linux каждый пользователь имеет уникальный идентификационный номер, который однозначно определяет его в системе.
4. Идентификатор группы, к которой принадлежит этот пользователь (GID).
5. Информационное поле GECOS. Поле GECOS хранит вспомогательную информацию о пользователе (номер телефона, адрес, полное имя и так далее). Оно не имеет чётко определённого синтаксиса.
6. Полный путь к домашнему каталогу пользователя. В ОС Linux для каждого пользователя создается его домашний каталог, в котором он может хранить свои документы. Обычно эти каталоги располагаются в директории /home корневого каталога и по умолчанию имеют имена владельцев.
7. Путь к командной оболочке. Последнее поле содержит полный путь к рабочей оболочке пользователя (по умолчанию такой оболочкой является bash). Эта оболочка запускается, когда пользователь проходит процедуру аутентификации.

Этот файл, как правило, не редактируется вручную, хотя это вполне допустимо. Обычно для редактирования файла пользователей используют специальные комманды: useradd, usermod и userdel.

1. Useradd – Позволяет добавить нового пользователя в систему.
2. Usermod – Позволяет изменять такие параметры, домашний католог, группа, идентификатор пользователя и так далее.
3. Userdel – Позволяет удалить пользователя.

Каждый пользователь в системе имеет свой собственный пароль. Наличие пароля – необходимая составляющая политики безопасности пользователей Linux. Пароли хранятся в отдельном файле /etc/shadow.

Пример строки файла /etc/shadow:

root:1gka0eOIt$3RXPSZVX9AMLVZ65gXmQA1:13766:0:::::

Файл shadow, по аналогии с файлом passwd, разделен на несколько частей двоеточиями (поля 3 - 8 являются необязательными) :

1. Имя пользователя. Это поле просто дублируется из файла passwd.
2. Хэш пароля. Пароль в Linux никогда не хранится в открытом виде.
3. Содержит число дней, прошедших с полуночи 01.01.1970 до дня последнего изменения пароля.
4. Содержит минимальное число дней действия пароля со дня его последнего изменения.
5. Содержит максимальное число дней действия пароля.
6. Содержит число дней до даты, когда система начнет выдавать предупреждения о необходимости смены пароля.
7. Содержит число дней со времени обязательной смены пароля до блокировки учетной записи.
8. Содержит день блокировки учетной записи.

Файл паролей имеет права только на чтение и только для суперпользователя (права доступа будут описаны ниже). Его содержимое является недоступным для рядовых пользователей, таким образом, исключается возможность раскрытия зашифрованного пароля.

Изменения пароля в Linux происходит с использованием специальной программы passwd. В качестве параметра в командной строке она получает имя пользователя и при запуске требует ввода пароля для этого пользователя.

Для более удобного управления доступом к ресурсам в Linux все пользователи объединяются в группы. В данном случае **группа** – это множество пользователей, объединенных по каким-либо критериям.

Пример строки файла /etc/group:

bin:x:1:root,bin,daemon

Каждая запись файла /etc/group разделена двоеточиями на 4 части:

1. Символьное имя группы.
2. Пароль группы – устаревшее поле, не используется.
3. Уникальный идентификатор группы, или GID.
4. Список имен участников, разделенных запятыми.

Всем файлам, созданным пользователем после регистрации в системе, будет автоматически присвоен этот номер группы.

Права пользователя.

Концепция файловой политики безопасности Linux строится на том, что любой файл системы имеет 3 категории владельцев: собственно владельца файла или, проще говоря, его создателя, какую-либо группу пользователей, в которую чаще всего входит владелец файла, и всех остальных. Таким образом, привилегированный пользователь или владелец файла, поскольку только он имеют возможность изменять права доступа, может построить политику файловой безопасности, определяя права отдельно для владельца файла, для группы пользователей и для всех остальных пользователей системы.

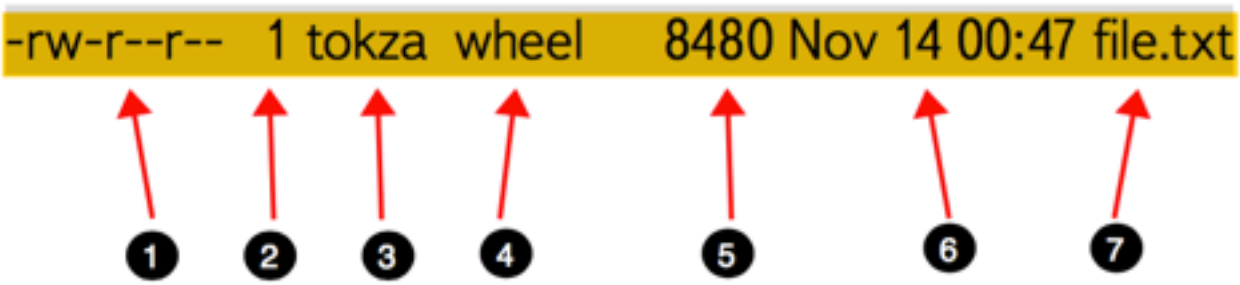
Права доступа к файлу или каталогу описываются тремя восьмеричными цифрами, самая левая из которых – права доступа владельца, средняя – права группы, правая – права доступа для всех остальных. Каждая из этих восьмеричных цифр представляет собой битовую маску из 3-х бит. Эти биты отвечают за право на чтение, запись и исполнение файла или каталога. Если бит установлен в 1 – операция разрешена, если в 0 – запрещена.

Для файлов и каталогов значения прав доступа немного отличаются:

восьмеричная	**символьная**	**права на файл**	**права на директорию**
0	---	нет	нет
1	--x	выполнение	чтение файлов и их свойств
2	-w-	запись	нет
3	-wx	запись и выполнение	всё, кроме чтения списка файлов

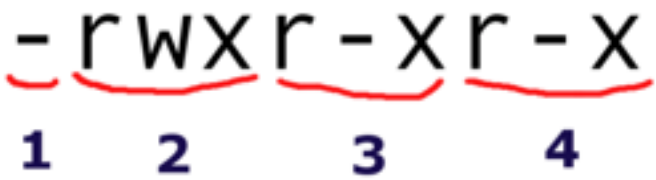
4	r--	чтение	чтение имён файлов
5	r-x	чтение и выполнение	доступ на чтение
6	rw-	чтение и запись	чтение имён файлов
7	rwx	все права	все права

Какие права доступа определены для каждого файла, можно узнать, просмотрев атрибуты файла, набрав в терминале команду ls с ключом –l:



1. Права доступа (владельца, группы, остальных).
2. Количество жестких ссылок.
3. Владелец файла.
4. Группа владельца файла.
5. Размер файла, в байтах.
6. Дата последний модификации файла.
7. Имя файла.

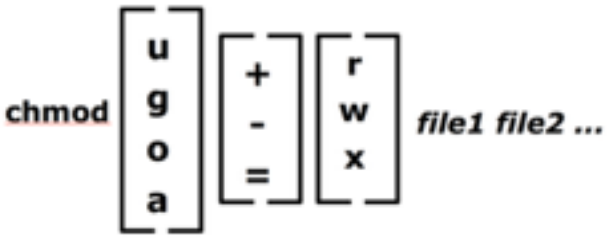
Биты доступа:



1. Тип файла [- (file), d (dir), l (link), c (char dev), b (block dev), s (socket), p (FIFO)].
2. Права пользователя - владельца файла.

3. Права группы – владельца файла.
4. Права остальных пользователей.

Изменение прав доступа к файлу осуществляется при помощи стандартной системной команды chmod. Права доступа при вызове команды могут задаваться как битовой маской в десятичном представлении, так и при помощи символов.



u – user

g – group

o – other

a - all

+ –добавить

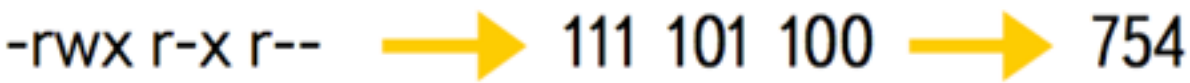
- – убрать

= – установить

Установка битов доступа:

1 — бит доступа установлен

0 — бит доступа не установлен



Пример: # chmod 754 somefile

Основы работы с командной строкой: http://help.ubuntu.ru/wiki/командная_строка Основные команды необходимые для выполнения работы: addgroup, adduser, chmod, chown, passwd. Дополнительную информацию о командах можно прочитать в man руководстве, для этого написать в терминале

man passwd. Скачать дистрибутив Debian можно по ссылке: http://cdimage.debian.org/debian-cd/8.4.0/amd64/iso-dvd/, для выполнения лабораторной работы достаточно DVD №1.

Задание

1. Создать две группы students, teachers. Создать 4-х пользователей (администратор (root- создается при установке системы), teacher, student1, student2). Пользователей студент1 и студент2 объединить в группу. Пользователей администратор и преподаватель объединить в группу.
2. Создать папку (dir1) с текстовыми файлами file1 и file2. Создать папку (dir2) с текстовыми файлами file3 и file4.
   Разграничить права доступа на эти файлы так:
   - /dir1/file1 - Доступ студентам только на чтение, остальным все разрешено.
   - /dir1/file2 - Полные права student1, остальным все запрещено.
   - /dir2 - Полный доступ группе преподавателей. Студентам запрещено просматривать содержание директории и писать в нее.
   - /dir2/file3 - Полный доступ группе преподавателей. Студентам доступ по прямой ссылке /dir2/file3.
   - /dir2/file4 - Доступ только группе преподавателей.
3. В политике безопасности (с помощью команды passwd) задать следующие пункты:
   - Максимальный срок действия - 30 дней.
   - Минимальный срок действия - 10 дней.
   - Предупреждение о скорой смене пароля - 5 дней.
   - Срок блокировки учетной записи с момента истечения пароля 15 дней.

Отчет необходимо оформить по шаблону с сайта «ЛЭТИ»(титульник, цель работы, ход выполнения работы, вывод) и сопроводить скриншотами с этапами выполнения задания, все задания выполняются с использованием терминала!

Отчеты присылать на почту ZOC.leti@yandex.ru . В теме письма должно содержаться имя, фамилия, группа, номер лабораторной работы и слово «Linux».