Пользователи, доступы chmod

1 Базовые концепции пользователей и групп

Определение 1.1. *Пользователь (User) — учетная запись в системе.*

Каждый пользователь имеет:

- **UID (User ID)**: Уникальный числовой идентификатор
- **GID (Group ID)**: Идентификатор основной группы
- **Домашний каталог (Home Directory)**: Личная папка пользователя (обычно $/home/username$)
- **Логинская оболочка (Login Shell)**: Командная оболочка, запускаемая при входе (например, $/bin/bash$)

Определение 1.2. *Группа (Group) — коллекция пользователей. Используется для удобного управления правами доступа к ресурсам для нескольких пользователей сразу.*

- **GID (Group ID)**: Уникальный числовой идентификатор группы

Типы пользователей:

- **Суперпользователь (root)**: Имеет UID 0 и неограниченные права
- **Системные пользователи**: Создаются для работы служб и демонов (например, **www-data** для веб-сервера)
- **Обычные пользователи**: Создаются для людей, работающих с системой

2 Файлы конфигурации пользователей и групп

/etc/passwd

- Содержит информацию о пользователях
- Формат строки: $username : x : UID : GID : UserInfo : HomeDirectory : LoginShell$
- Пример: $mj : x : 1000 : 1000 : MichaelJang : /home/mj : /bin/bash$

/etc/group

- Содержит информацию о группах
- Формат строки: $groupName : x : GID : groupMembers$
- Пример: $wheel : x : 10 : alex$

/etc/shadow

- Содержит зашифрованные пароли и информацию об их сроке действия
- Доступен только для чтения пользователем root

3 Основы прав доступа к файлам и директориям

Замечание 3.1. *Права доступа определяют, кто и что может делать с файлом или директорией*

Категории пользователей:

- `u` (user/owner) — владелец файла
- `g` (group) — группа-владелец
- `o` (others) — все остальные пользователи системы

Типы прав:

- `r` (read) — право на чтение
- `w` (write) – право на запись (и удаление для директорий)
- `x` (execute) — право на выполнение (для файлов) или вход в директорию (для папок)

4 Команда `ls -l`: Анализ прав доступа

Замечание 4.1. *Чтобы посмотреть права, используется команда `ls -l`.*

Листинг 1: Пример вывода

```
-rwxr-xr--. 1 root root 175376 Sep 21 10:45 /sbin/fdisk
```

Разбор строки прав `-rwxr-xr-`:

- Первый символ: Тип объекта (`-` — файл, `d` — директория, `l` — ссылка).
- **Следующие 9 символов: Права доступа, разбиты на три блока по три символа:**
  - `rwx` — права для Владельца (u)
  - `r-x` — права для Группы (g)
  - `r-` — права для Остальных (o)

5 Команда `chmod`: Изменение прав доступа

Замечание 5.1. *`chmod` (Change Mode) используется для изменения прав.*

5.1 Синтаксис №1: Символьный метод: `chmod` [<кто><оператор><права>] <файл>

- Кто: `u` (владелец), `g` (группа), `o` (остальные), `a` (все)
- Оператор: `+` (добавить), `-` (забрать), `=` (установить точно)
- Права: `r`, `w`, `x`

5.2 Примеры

Листинг 2: Дать владельцу право на выполнение

```
chmod u+x script.sh
```

Листинг 3: Забрать у группы право на запись

```
chmod g-w file.txt
```

Листинг 4: Забрать все права у "остальных"

```
chmod o= file.txt
```

Листинг 5: Дать всем право на чтение

```
chmod a+r file.txt
```

Листинг 6: Рекурсивно дать группе право на запись в папку и её содержимое

```
chmod -R g+w /myfolder/
```

5.3 Синтаксис №2: Цифровой (восьмеричный) метод: `chmod` <число> <файл>

Каждый блок прав кодируется цифрой:

- r (read) = 4
- w (write) = 2
- x (execute) = 1

Замечание 5.2. *Цифра для блока — это сумма нужных прав.*

Замечание 5.3. *Три цифры в команде означают:* ***Владелец | Группа | Остальные****.*

Примеры расчета:

- `rwx` = 4 + 2 + 1 = 7 (полные права)
- `rw-` = 4 + 2 + 0 = 6 (чтение и запись)
- `r-x` = 4 + 0 + 1 = 5 (чтение и выполнение)
- `r--` = 4 + 0 + 0 = 4 (только чтение)
- `---` = 0 + 0 + 0 = 0 (нет прав)

5.4 Примеры команд:

Листинг 7: Владелец: `rwx`=7, Группа: `r-x`=5, Остальные: `r--`=4

```
chmod 754 script.sh
```

Листинг 8: Владелец: `rw-`=6, Группа: `r--`=4, Остальные: `---`=0

```
chmod 640 config.txt
```

Листинг 9: Стандартные права для исполняемых директорий

```
chmod 755 mydir/
```

6 Специальные биты прав доступа

6.1 Установка специальных битов:

- **Символьный метод:** `chmod u+s file`, `chmod g+s dir`, `chmod o+t dir`
- **Цифровой метод:** Добавляется четвертая цифра в начало (SUID=4, SGID=2, Sticky=1):
  - `chmod 4755 file` (SUID установлен)
  - `chmod 2770 /shared_dir/` (SGID установлен)
  - `chmod 1777 /tmp/` (Sticky Bit установлен)

Таблица 1: Специальные права доступа в Unix-системах

Специальное право	На файле	На директории
SUID (Set User ID)	Процесс выполняется с правами владельца файла, а не запустившего его пользователя	Не имеет эффекта
SGID (Set Group ID)	Процесс выполняется с правами группы файла	Файлы, создаваемые в директории, наследуют её группу-владельца
Sticky Bit	Не имеет эффекта	Файлы в директории могут быть удалены только их владельцами (даже если у других есть w на директорию). Пример: /tmp

7 Смена владельца и группы

7.1 chown (Change Owner): Меняет владельца и/или группу файла.

Листинг 10: Сменить владельца

```
chown username file.txt
```

Листинг 11: Сменить группу

```
chown :groupname file.txt
```

Листинг 12: Сменить и владельца, и группу

```
chown username:groupname file.txt
```

Листинг 13: Сменить рекурсивно

```
chown -R username:groupname dir/
```

7.2 chgrp (Change Group): Меняет только группу файла.

```
chgrp groupname file.txt
```

8 Типичные сценарии для разработчика

Таблица 2: Типичные сценарии для разработчика

Сценарий	Команда (симв.)	Команда (цифр.)	Пояснение
Сделать скрипт исполняемым	chmod +x deploy.sh	chmod 755 deploy.sh	Владелец - все права, остальные - чтение и выполнение
Закрыть конфиг от посторонних	chmod o-rwx config.yml	chmod 600 config.yml	Только владелец может читать и писать
Общая папка для команды	chmod g+rw shared_dir/	chmod 770 shared_dir/	Владелец и группа - полные права, остальные - нет
Права для статики веб-сервера	chmod a+r style.css	chmod 644 style.css	Все могут читать, владелец - менять