13-1. 사용자 계정 관련 파일

사용자 계정 관련 파일

- 리눅스는 기본적으로 여러 명이 시스템을 사용하는 다중 사용자 시스템이므로 사용자를 구별하고 사용자에게 적절한 자원을 할당해주는 방법이 필요하다.

/etc/passwd 파일

- 사용자 계정 정보가 저장된 기본 파일이다.
- 한 행에 사용자 한 명에 대한 정보가 기록되며, 콜론(:)으로 구분되는 7개의 항목으로 구성되어 있다.

파일의 구조

로그인 ID : x : UID : GID : 설명 : 홈 디렉터리 : 로그인 셸

- 로그인 ID
  - 사용자 계정의 이름 = 사용자 ID, 사용자 이름, 로그인 이름
  - 32자를 넘을 수 없으나 유닉스와 같은 다른 운영체제와의 연동을 위해 8자로 제한하는 게 좋다.
  - 로그인 ID는 중복되는 이름을 사용해서는 안된다.
- x
  - 초기 유닉스 시스템에서 사용자 암호를 저장하던 항목이다.
  - 현재는 /etc/shadow 파일에 별도로 보관하고 있다.
- UID
  - 사용자 ID 번호로 시스템이 사용자를 구별하기 위해 사용하는 번호이다.
  - 일반적으로 0~999번(운영체제에 따라서는 499)과 65534번은 시스템 사용자를 위한 UID로 예약되어 있다.
  - 일반 사용자는 UID 1000번(때로는 500번)부터 할당된다.
  - 기본적으로 등록되는 시스템 사용자 ID
    - 0(root): root 사용자 계정
    - 1(bin): 명령어 관리를 위한 계정
    - 2(daemon): 시스템 데몬 계정
    - 4(lp): 프린트 서비스와 관련된 계정
    - 65534(nfsnobody): 사용자의 UID로 NFS와 관련된 계정
  - 로그인 ID가 다르더라도 UID가 같으면 시스템은 같은 사용자로 판단한다.
- GID
  - 그룹 ID를 나타낸다.
  - 리눅스에서 사용자는 무조건 하나 이상의 그룹에 소속된다.
  - 사용자의 기본 그룹은 사용자를 등록할 때 정해지며, 특별히 소속 그룹을 지정하지 않으면 자동적으로 로그인 ID와 동일한 그룹으로 등록된다.

    - 시스템에 등록된 그룹에 대한 정보는 /etc/group 파일에 저장되어 있다.
- 설명
    - 사용자의 실명이나 부서명, 연락처 등 사용자에 대한 일반적인 정보가 기록되는 부분이다.
- 홈 디렉터리
    - 사용자 계정에 할당된 홈 디렉터리의 절대 경로를 기록한다.
- 로그인 쉘
    - 사용자의 로그인 쉘을 지정한다.
    - 로그인 쉘: 사용자가 로그인할 때 기본적으로 동작하는 쉘이다.

/etc/shadow 파일

- 보안 때문에 사용자 암호에 관한 정보를 별도로 관리하는 파일이다.
- root 사용자만 읽고 쓸 수 있으며, shadow 그룹은 읽기만 가능하다.
- 9개의 항목으로 구성되어 있으며, 콜론으로 구분되어 있다.

파일의 구조

로그인 ID: 암호 : 최종 변경일 : MIN : MAX : WARNING : INACTIVE : EXPIRE : Flag

- 로그인 ID
- 암호
    - 실제 비밀번호가 암호화되어 저장된다.
    - 비밀번호는 일방향 암호여서 원 암호가 어떤 문자였는지 복호화할 수 없다.
    - 이 항목에 아무 값도 없으면 암호가 지정되지 않은 계정임을 뜻한다.
- 최종 변경일
    - 암호가 마지막으로 변경된 날짜를 지정한다.
    - 이 날짜는 유닉스의 전통을 따라 1970년 1월 1일을 기준으로 날수를 기록한다.
- MIN
    - **Password Aging**: MIN, MAX, WARNING, INACTIVE, EXPIRE 항목
        - 패스워드와 관련된 사용기간
    - 암호를 변경한 후 사용해야 하는 최소기간이다. (기본값 0)
- MAX
    - 암호를 사용할 수 있는 최대 기간이다. (기본값 99999)
- WARNING
    - 암호가 만료되기 전에 경고를 시작하는 날수이다. (기본값 7)
- INACTIVE
    - 암호 만료 후에도 이 항목에 지정한 날수 동안은 로그인이 가능하도록 한다.
- EXPIRE
    - 사용자 계정이 만료되는 날이다.
    - 최종 변경일처럼 1970년 1월 1일을 기준으로 한 날수로 표시된다.
- Flag
    - 향후 사용할 목적으로 비워둔 항목이다.
- **암호 부분이 !로 시작하는 것은 계정이 잠겨 있음을 의미한다.**

/etc/login.defs 파일

- 사용자 계정의 설정과 관련된 기본값을 정의한 파일

항목	기본 값	의미
MAIL_DIR	/var/spool/mail	기본 메일 디렉터리
PASS_MAX_DAYS	99999	패스워드 에이징
PASS_MIN_DAYS	0	
PASS_WARN_AGE	7	
UID_MIN, UID_MAX	1000~60000	사용자 계정의 UID 범위
SYS_UID_MIN, SYS_UID_MAX	100~999	시스템 계정의 UID 범위
GID_MIN, GID_MAX	1000~600000	사용자 계정의 GID 범위
SYS_GID_MIN, SYS_GID_MAX	100~999	시스템 계정의 GID 범위
UMASK	022	umask 값 설정
USERGROUPS_ENAB	yes	사용자 계정 삭제 시 그룹 삭제 여부
ENCRYPT_METHOD	SHA512	암호화 기법

/etc/group 파일

- 그룹에 관한 정보가 저장된 파일
- 사용자는 기본적으로 하나 이상의 그룹에 속해 있다.
- /etc/passwd 파일의 GID 항목에 지정된 그룹이 기본그룹이며, 사용자가 속한 2차 그룹은 /etc/group 파일에 지정된다.

파일의 구조

그룹 이름 : x : GID : 그룹 멤버

- 그룹 이름
- x
    - 그룹의 암호를 저장하는 곳
    - 예전 유닉스에서는 비어 있거나 * 표시가 되어 있었다.
    - 리눅스에서는 암호화된 그룹 암호를 저장하거나 /etc/gshadow 파일에 그룹 암호를 저장한다.
    - 그룹 암호는 newgrp 명령을 사용하여 자신이 속하지 않은 그룹으로 전환할 때 필요하다.
- GID
- 그룹 멤버
    - 그룹에 속한 멤버들의 사용자 계정 이름이며 쉼표(,)로 사용자를 구분한다.
    - 사용자의 2차 그룹을 나타낸다.

/etc/gshadow 파일

- 그룹 암호가 저장된 파일

파일의 구조

그룹 이름 : 그룹 암호 : 관리자 : 그룹 멤버

- 그룹 이름
- 그룹 암호
- 관리자
    - 그룹의 암호나 멤버를 바꿀 수 있는 사용자 계정
    - 여러 개일 경우 쉼표(,)로 구분한다.
- 그룹 멤버
    - 그룹에 속한 멤버들의 사용자 계정 이름이며 쉼표(,)로 사용자를 구분한다.