

# 목차

00. 개요

01. 사용자 계정 관련 파일

# 01 사용자 계정 관련 파일

## ■ 사용자 관리

- 리눅스는 다중 사용자 시스템이므로 사용자를 구별하고 사용자에게 적절한 자원을 할당해주는 방법이 필요
- 사용자 계정은 사용자가 시스템에 접근할 수 있는 유일한 방법
- 시스템 관리자의 입장에서 사용자의 접근 권한을 통제할 수 있는 중요한 수단

## ■ /etc/passwd 파일

- 사용자 계정 정보가 저장된 기본 파일
- 한 행에 사용자 한 명에 대한 정보가 기록되며, 쌍점(:)으로 구분되는 일곱 개의 항목으로 구성

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

1	2	3	4	5	6	7
---	---	---	---	---	---	---

/etc/passwd 파일의 사용자 계정 정보 구성

- 로그인 ID: 사용자 계정의 이름, 32자를 넘을 수 없으나 8자로 제한하는 것이 좋다
- x : 초기 유닉스 시스템에서 사용자 암호를 저장하던 항목, 요즘은 /etc/shadow 파일에 별도로 보관
- UID: 사용자 ID 번호로 시스템이 사용자를 구별하기 위해 사용하는 번호
  - 0~999번과 65534번은 시스템 사용자를 위한 UID로 예약(0: root, 1: daemon, 2: bin, 7: lp 등)
  - 일반 사용자들은 UID 1000번부터 할당
  - 로그인 ID가 다르더라도 UID가 같으면 리눅스 시스템은 같은 사용자로 판단, 따라서 UID가 중복되지 않았는지 주의해야함

# 01 사용자 계정 관련 파일

## ■ /etc/passwd 파일

- § GID : 그룹 ID, 시스템에 등록된 그룹에 대한 정보는 /etc/group 파일에 저장
- § 설명 : 사용자의 실명이나 부서명, 연락처 등 사용자에게 대한 일반적인 정보가 기록
- § 홈 디렉터리 : 사용자 계정에 할당된 홈 디렉터리의 절대 경로를 기록
- § 로그인 셸 : 사용자의 로그인 셸을 지정, 우분투에서는 배시 셸(/bin/bash)을 기본 셸로 사용

## ■ /etc/passwd 파일의 예

```
user1@myubuntu:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
( 생략 )
colord:x:114:122:colord colour management daemon,,,:/var/lib/colord:/bin/false
saned:x:115:123:::/home/saned:/bin/false
user1:x:1000:1000:user1,,,:/home/user1:/bin/bash
sshd:x:116:65534::/var/run/sshd:/usr/sbin/nologin
postfix:x:117:125::/var/spool/postfix:/bin/false
user1@myubuntu:~$
```

# 01 사용자 계정 관련 파일

## ■ /etc/shadow 파일

- 사용자 암호에 관한 정보를 별도로 관리하는 파일
- root 계정으로만 내용을 볼 수 있음

```
user1@myubuntu:~$ ls -l /etc/passwd /etc/shadow
-rw-r--r-- 1 root root 1813 2월 24 14:19 /etc/passwd
-rw-r----- 1 root shadow 1126 3월 18 00:28 /etc/shadow
user1@myubuntu:~$
```

## ■ /etc/shadow 파일의 구조

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

1	2	3	4	5	6	7	8	9
---	---	---	---	---	---	---	---	---

/etc/shadow 파일의 정보 구성

- 로그인 ID : 사용자 계정 이름
- 암호(패스워드) : 실제 비밀번호가 암호화되어 저장
- 최종 변경일 : 암호가 마지막으로 변경된 날짜를 지정, 1970년 1월 1일을 기준으로 날짜를 기록
- MIN : MIN은 암호를 변경한 후 사용해야 하는 최소 기간
- MAX : 암호를 사용할 수 있는 최대 기간
- WARNING : 암호가 만료되기 전에 경고를 시작하는 날짜
- INACTIVE : 암호가 만료된 후에도 이 항목에 지정한 날짜 동안은 로그인이 가능
- EXPIRE : 사용자 계정이 만료되는 날 ⑨ Flag : 향후 사용할 목적으로 비워둔 항목

# 01 사용자 계정 관련 파일

## ■ /etc/shadow 파일 예

```
user1@myubuntu:~$ sudo cat /etc/shadow
[sudo] password for user1:
root:!:16121:0:99999:7:::
daemon*:15994:0:99999:7:::
bin*:15994:0:99999:7:::
sys*:15994:0:99999:7:::
sync*:15994:0:99999:7:::
(생략)
colord*:15994:0:99999:7:::
saned*:15994:0:99999:7:::
user1:$6$Em8l2vYY$HjxlxB26yEfstxX0Mh9ttgtv3PArb7J90Rj0mSH/76kjfcZDGYTTqgG0NRDL
VHJfwd84qPGlmq3VMh/a1UEPK/:16146:0:99999:7:::
sshd*:16121:0:99999:7:::
postfix*:16125:0:99999:7:::
user1@myubuntu:~$
```

# 01 사용자 계정 관련 파일

## ■ /etc/login.defs 파일

- 사용자 계정의 설정과 관련된 기본 값을 정의

```
user1@myubuntu:~$ cat /etc/login.defs
(생략)
#
# Password aging controls:
#
#      PASS_MAX_DAYS   Maximum number of days a password may be used.
#      PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#      PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
(생략)
GID_MIN          1000
GID_MAX          60000
# System accounts
#SYS_GID_MIN      100
#SYS_GID_MAX      999
(생략)
DEFAULT_HOME     yes
# CLOSE_SESSIONS
# LOGIN_STRING
# NO_PASSWORD_CONSOLE
# QMAIL_DIR
user1@myubuntu:~$
```

# 01 사용자 계정 관련 파일

---

- /etc/login.defs 파일에서 정의하는 기본 값