

5. 패스워드 관리 정책

1) 패스워드 정책

- 대/소문자, 숫자, 특수문자를 혼용하여 8개 글자 이상의 패스워드를 사용
- 동일 문자를 연속 4회 이상 사용 금지
- 패스워드 히스토리를 관리하여 2~3개 이상의 동일 패스워드 사용금지
- 패스워드 변경주기를 설정(패스워드 유효기간을 90일 이하로 설정)
- 사전에 나오는 쉬운 단어나 이름은 패스워드로 사용하지 못하도록 설정
- 기본 설정된 패스워드는 사용하지 못하도록 설정
- 초기 부여된 패스워드는 사용자 최초 접속 시 변경하도록 설정

2) 패스워드 정책 설정 파일 /etc/security/pwquality.conf

difok = N	기존 패스워드와 비교. 기본값 10(50%)
minlen = 8	최소 패스워드 길이 설정
dcredit = -1	최소 필요한 숫자 수
ucredit = -1	최소 필요한 대문자 수
lcredit = -1	최소 필요한 소문자 수
ocredit = -1	최소 필요한 특수문자 수
maxrepeat = 3	최대 연속된 동일한 반복 수 (예 aaa,111 형태를 사용 못함)
maxclassrepeat = 3	최대 연속 문자 반복 수 [최소 3 이상 권장] (예 abc,123 형태를 사용 못함)
usercheck = 1	패스워드에 유저 ID가 포함되어 있는지 점검 [1 권장/0 체크 안 함] (예 ID:gildong PASS:gildong123 형태를 사용 못함)
retry = 3	패스워드 입력 실패 시 재시도 횟수

3) 패스워드 기본값 설정 파일 /etc/login.defs

- 사용자 추가할 때 참고하는 메일 디렉터리
- 패스워드 관련 설정(최대 사용기한, 최소 사용기한, 최소 길이, 만기 이전 경고 주는 날짜)
- UID의 최소값 및 최대값
- GID의 최소값 및 최대값
- 홈 디렉터리 생성 여부
- 기본 umask 값
- 패스워드에 적용되는 암호화 알고리즘 등이 정의되어 있는 파일

4) 패스워드 관련 명령어 passwd

- 패스워드를 부여하거나 변경
- 사용자명을 입력하지 않으면 현재 사용자의 패스워드로 변경
- 계정을 사용하지 못하게 하거나 패스워드 만기일 및 유효기간을 설정

[사용법] # **passwd** [option] [사용자명]

-n	패스워드 변경 후 최소 사용 기간
-x	패스워드 변경 후 최대 사용 기간
-w	패스워드 만기일 이전에 사용자에게 경고 메시지를 전달할 날짜 지정
-e	최초 로그인 시에 강제로 패스워드를 변경하도록 설정
-d	passwd 입력 없이 로그인 가능 (shadow 파일의 패스워드 필드 값 제거)
-l	해당 사용자의 상태를 locking으로 변경
-S	해당 사용자의 현재 패스워드 설정 조회