권한 및 그룹 설정

- 리눅스 시스템의 모든 파일과 디렉터리에는 접근권한(permission)과 소유권(ownership)이 부여된다.

- ‘ls -l’ 실행결과’ 문서 디렉터리의 정보를 바탕으로 해석

|  |  |
| --- | --- |
| drwxr-xr-x 1 82102 197610 0 1월 29 02:58 Documents/ | |
| **속성 값** | **의미** |
| **drwxr-xr-x** | 파일 허가권(파일 유형과 접근 권한으로 구성) |
| **1** | 물리적 파일 연결 개수 |
| **82102** | 파일 소유자 명(user ownership) |
| **197610** | 파일 소유 그룹 명(group ownership) |
| **0** | 파일(디렉터리)의 크기 (byte 단위) |
| **1월 29 02:28** | 파일이 마지막으로 변경된 시간 |
| **Documents/** | 파일(디렉터리) 명 |

**1. 소유권과 관련 명령어**

* 소유권은 임의의 파일 또는 디렉터리에 대해 사용자와 그룹들의 소유 권한을 나타낸 것이다.
* 그룹은 사용자들의 시스템 운영 특성에 따라 묶어 놓은 것으로, 같은 그룹에 속한 사용자들은 파일 또는 디렉터리에 대해 동일한 소유권과 작업 권한을 가진다.
* 명령어 chown: 파일과 디렉터리의 사용자 소유권과 그룹 소유권을 변경한다.
  + 형식: chown [옵션] 소유자[:그룹명] 파일명
  + 옵션: -R : 하위 디렉터리를 포함하여 디렉터리 내부의 모든 파일의 소유권 변경
* 명령어 chgrp: change group의 줄인 명령어로 파일이나 디렉터리의 그룹 소유권을 변경한다. 명령어 chown은 사용자와 그룹의 소유권 둘 다를 바꿀 수 있었지만 chgrp는 그룹의 소유권만 변경 가능
  + 형식: chgrp [옵션] 그룹명 파일명
  + 옵션: -R : 하위 디렉터리를 포함하여 디렉터리 내부의 모든 파일의 그룹 소유권 변경

**2. 허가권 관련 명령어**

* 명령어 ‘ls -l’으로 파일의 유형과 허가권을 알 수 있다. (- rw-rw-r--: 파일유형(-)과 파일의 접근 권한(-rw-rw-r--)을 나타냄)
* 파일 허가권의 첫번째 자리는 파일 유형을 기호로 정의한다.
* 파일은 일반 파일, 디렉터리 파일, 특수 파일로 나뉜다.
* 명령어 ‘la -l /dev’를 실행하면 파일 유형이 ‘b’나 ‘c’인 파일들을 볼 수 있다. (특수 파일)

|  |  |  |
| --- | --- | --- |
| **기호** | | **파일 유형** |
| **-** | | 일반 파일 |
| **d** | | 디렉터리 파일 |
| **특 수 파 일** | **b** | 블록 단위로 읽고 쓰는 블록 장치 특수 파일  블록장치: 하드디스크, 플로피디스크, CD/DVD 등의 저장장치 |
| **c** | 문자 단위로 읽고 쓰는 문자 장치 특수 파일  문자장치: 마우스, 키보드, 프린터의 입출력 장치 |
| **l** | 기호적 링크로 바로가기 아이콘 역할 수행 |
| **p** | 파이프 |
| **s** | 소켓 |

* 파일 허가권의 두 번째 자리에서 열 번째 자리는 파일 접근 권한을 정의한다.
* 리눅스는 사용자 별로 파일 권한을 부여한다.
* 파일 사용자는 파일 소유자(owner), 그룹 소속자(group), 그리고 기타 사용자(others 또는 public)로 구분한다.
* 파일 권한은 읽기(read) , 쓰기(write), 실행(execute)이 있다.
* 읽기, 쓰기 또는 실행의 접근 제한 표시는 하이픈(-)으로 나타낸다.
* 사용자별 권한은 기호 모드(symbolic mode) 또는 8진수 숫자 모드(numeric mode)로 표시한다.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **사용자 권한** | | | **그룹 권한** | | | **기타 사용자 권한** | | |
| **기호 모드** | r | w | x | r | w | x | r | w | x |
| **8진수 숫자모드** | 4 | 2 | 1 | 4 | 2 | 1 | 4 | 2 | 1 |

* 예를 들어 ‘- -rw-rw-r--’ 는 숫자 권한으로 ‘664’이다. 즉, 파일 소유자와 그룹 사용자들은 읽고 쓰기가 가능하며 기타 사용자는 읽기만 가능하다. 셋 다 실행권한은 없다.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **사용자 권한** | | | **그룹 권한** | | | **기타 사용자 권한** | | |
| **기호 모드** | r | w | - | r | w | - | r | - | - |
| **8진수 숫자모드** | 4 | 2 | 0 | 4 | 2 | 0 | 4 | 0 | 0 |
| 6 | | | 6 | | | 4 | | |

* 권한은 파일 유형에 따라 다르게 정의된다.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **일반 파일** | **디렉터리 파일** | **특수 파일** |
| **읽기(r)** | 파일 내용 읽기 | 디렉터리 내 파일 목록 읽기 | read()로 파일 읽기 |
| **쓰기(w)** | 파일 수정/삭제 | 디렉터리 내 파일 생성/삭제 | write()로 파일 내용 변경 |
| **실행(x)** | 파일 실행 | Cd 명령을 이용해 디렉터리 이동 | 권한 의미 없음 |

* 명령어 chmod: 파일이나 디렉터리의 접근 허가권을 변경하는 명령어이다.
  + 형식: chmod [옵션] 파일명
  + 옵션: -R : 하위 디렉터리에 포함되어 있는 모든 디렉터리 및 파일의 권한 변경
* 권한 변경은 ‘숫자모드’ 또는 ‘기호모드’가 있다.
* ‘숫자 모드’’를 이용한 권한 변경

Ex) chmod 666 TST.txt => TST파일의 권한을 -rw-rw-rw- 로 변경한다

|  |  |  |
| --- | --- | --- |
| **기호** | **숫자(2진수)** | **숫자(8진수)** |
| rwx | 111 | 7 |
| rw- | 110 | 6 |
| r-x | 101 | 5 |
| r-- | 100 | 4 |
| -wx | 011 | 3 |
| -w- | 010 | 2 |
| --x | 001 | 1 |
| --- | 000 | 0 |

* ‘기호 모드’를 이용한 권한 변경

Ex) chmod -R o+w Young => Young에 속한 모든 파일, 디렉터리들에 대해 기타 사용자에게 쓰기 권한을 부여한다.

|  |  |  |  |
| --- | --- | --- | --- |
| **기호 모드** | | **의미** | **적용 예시** |
| 사용자 | u | 소유자 | chmod u+w  : 소유자에게 쓰기 권한 부여  chmod u-x  : 소유자의 실행권한 제거  chmod o=rx  : 기타 사용자에게 읽기 실행 권한을 지정 |
| g | 그룹 |
| o | 기타 사용자 |
| a | 모든 사용자(u+g+o) |
| 연산자 | + | 허가권 부여 |
| - | 허가권 제거 |
| = | 특정 사용자에게 허가권 지정 |
| 권한 | r | 읽기 |
| w | 쓰기 |
| x | 실행 |

* 명령어 umask: 새로 생성되는 파일이나 디렉터리의 기본 허가권 값을 지정한다.
  + 파일의 기본 권한은 666, 디렉터리의 기본 권한은 777이다. 명령어 umask는 디폴트 권한 값을 변경한다.

ex) umask 0002 를 하게되면 파일의 권한은(666-2 = 664 = -rw-rw-r--) 디렉터리의 권한은(777-2 = 775 = drwxrwxr-x)를 가지게 된다.

* + 형식: umask [옵션][값], 옵션: -S : umask 값을 문자로 나타내 준다.

**3. 특수 권한**

* SetUID와 SetGID
  + 프로세스가 실행되는 동안 해당 프로세스의 root권한을 임시로 가져오는 기능이다.
  + 프로세스가 사용자보다 높은 수준의 접근을 요구할 때 파일 접근 제한 때문에 원활한 기능을 제공할 수 없기 때문에 이러한 문제점을 해결하기 위한 방법이다.
  + SetUID의 경우 **사용자가 사용할 때만** 소유자 권한으로 파일을 실행시키고, SetGID의 경우 **사용자가 사용할 때만** 그룹 권한으로 파일을 실행한다
    - SetUID는 프로그램을 실행하는 동안 프로세스는 파일의 소유자와 같은 권한으로 실행된다.
    - SetGID는 프로그램을 실행하는 동안 프로세스는 파일의 그룹과 같은 권한으로 실행된다.
    - SetGID 권한이 명시된 디렉터리에 생성되는 모든 하위 디렉터리나 파일도 SetGID의 권한을 가진다.
  + 특수 권한의 절대적인 표기 방법

|  |  |  |  |
| --- | --- | --- | --- |
|  | **코드** | **절댓값** | **설명** |
| **SetUID** | s | 4000 | 프로세스 실행당시 UID로 설정 |
| **SetGID** | s | 2000 | 프로세스 실행당시 GID로 설정 |
| **Sticky bit** | t | 1000 | 실행 후에도 메모리를 점유하도록 설정 |

* + SetUID 아래는 예시이고 절댓값을 바꾸어 주면 다른 특수 권한도 실행 가능

chmod 4644 SYN => 실행 파일(-rw-r--r--)이 아니기 때문에 -rwSr--r--(s가 대문자)로 표시된다.

chmod 4744 SYN => 실행 파일(-rwx-r--r--)이기 때문에 -rwsr--r--(s가 소문자)로 표시된다.

* Sticky bit
  + 일반적으로 공용 디렉터리를 사용할 때 sticky bit를 사용한다.
  + Sticky bit가 설정되어 있는 디렉터리 안의 내용은 해당 파일의 소유자나 root만이 변경이 가능하여 공용 디렉터리라도 권한의 제약을 두어 다른 사용자들의 파일을 보호하기 위한 목적으로 만든 것이다.
  + 사용자 권한을 지정하기 힘든 프로그램들이 일시적(/tmp)으로 특정 디렉터리에 파일을 생성하고 삭제하도록 이용된다.
  + 특정 응용 프로그램이 다른 응용 프로그램에서 생성한 파일을 삭제하지 못하는 권한을 설정한다.
  + 설정된 디렉터리에는 누구든 접근하고(공용 디렉터리) 파일을 생성할 수 있다.
  + 생성된 sticky bit 파일 삭제 시에는 소유자(파일 생성자)와 관리자만 지울 수 있다. 다른 생성자는 자신의 소유가 아닌 파일을 삭제할 수 없다.
    - Sticky bit가 적용된 디렉터리 내의 파일을 생성하는 것은 누구나 가능하지만 삭제는 생성자 본인과 관리자만 가능하다.
    - 일시적으로 sticky bit로 설정되는 디렉터리는 /tmp 안에 생성된다.

**4. 디스크 쿼터(Disk Quota)**

* 파일 시스템마다 사용자나 그룹이 생성할 수 있는 파일의 용량 및 개수를 제한하는 것이다. 보통 블록 단위의 용량 제한과 inode의 개수를 제한한다.
* 사용자나 그룹이 가질 수 있는 inode의 수, 사용자나 그룹에게 할당된 디스크 블록 수를 제한한다.
* 쿼터는 사용자별, 파일 시스템별로 동작된다.
* 그룹단위로도 용량을 제한할 수 있으며 웹호스팅 서비스를 하는 경우에 유용하다.
* 디스크 쿼터 지정
  + 1단계: 파일 /ect/fstab에 디스크 관련 설정

|  |  |  |
| --- | --- | --- |
| **옵션** | **적용 대상** | **설명** |
| **quota** | fsfold, vfsv0 | 사용자 할당량 사용 |
| **gquota** | xfs | 그룹 할당량 사용 |
| **usrquota** | 모든 유형 | 사용자 할당량 사용 |
| **grpquota** | 모든 유형 | 그룹 할당량 사용 |
| **usrjquota=파일명** | vfsv0 | 저널 사용자 할당량 사용  jqfmt옵션의 스팩 및 할당량 데이터베이스 파일 이름이 필요  일반적으로 사용되는 파일명은 aquota.user |
| **grpjquota=파일명** | vfsv0 | 저널 그룹 할당량 사용  jqfmt옵션의 스팩 및 할당량 데이터베이스 파일 이름이 필요  일반적으로 사용되는 파일명은 aquota.group |
| **jqfmt=format** | vfsv0 | Userjquota 또는 grpjquota가 지정될 때 사용된 할당량 형식  현재는 vfsv0가 유일하게 지원되는 형식 |

* + 2단계: 재마운팅(remounting) 실행 후 확인
  + 3단계: 마운트 된 쿼터를 끄고 생성된 쿼터 파일 삭제
  + 4단계: 쿼터 데이터베이스 생성
  + 5단계: 사용자별 쿼터 지정

Ex) Filesystem blocks soft hard inodes soft hard

|  |  |
| --- | --- |
| **필드** | **설명** |
| **Filesystem** | 사용자별 쿼터를 할당하는 파일 시스템 |
| **blocks** | 현재 사용자가 사용하는 디스크 블록  기본 단위는 KB |
| **soft** | 소프트 사용한도  사용자가 사용할 수 있는 최대 용량  한 파티션에서 사용자가 사용할 수 있는 최대 용량  유예기간 내에 사용자는 사용 용량 초과에 대해 경고를 받음  지정용량이 hard 값보다 적을 때 지정한 유예기간 동안은 초과 가능 |
| **hard** | 하드 사용한도  유예기간이 설정되어 있을 때만 동작  디스크 사용에 있어 절대적인 사용 제한  hard 용량 초과 불가 |
| **inodes** | 현재 사용자가 사용하는 inode(파일과 디렉터리) 개수 |
| **soft** | 사용자에게 지정된 파일과 디렉터리 생성 개수 |

+ **grace period**

* + - 사용자의 사용량이 soft limit을 초과할 때부터 적용되는 시작 제한이다.
    - 시간은 sec, min, hour, day, week, month 단위이다.
    - “edquota -t” 명령을 실행하면 유예 기간을 보거나 수정할 수 있다.
  + 6단계: 쿼터 현재 상황 점검

|  |  |
| --- | --- |
| **옵션** | **설명** |
| **used** | 현재 사용량 |
| **soft** | Soft limit |
| **hard** | Hard limit |
| **grace** | Soft limit에 지정된 용량 초과 시 남은 유예기간 표시 |

* 디스크 쿼터 관련 명령어
  + 명령어 quotaoff/on: 쿼터 서비스를 비활성화/활성화 한다.

|  |  |
| --- | --- |
| **옵션** | **설명** |
| **-a** | 파티션 정보 출력 |
| **-u** | 사용자 쿼터 비활성화/활성화 |
| **-g** | 그룹 쿼터 비활성화/활성화 |
| **-v** | 메시지 출력 |
| **-p** | 쿼터 정보 출력(활성화 비활성화와 상관없이) |

* + 명령어 quotacheck: 파일 시스템의 디스크 사용 상태를 검색한다. quota 기록 파일인 ‘quota.user, quota.group’ 또는 ‘aquota.user, aquota.group’ 파일들을 최근 상태로 갱신하기 위해 사용된다.

|  |  |
| --- | --- |
| **옵션** | **설명** |
| **-a** | 모든 파일 시스템을 체크(all) |
| **-u** | 사용자 쿼터 관련 체크(user) |
| **-g** | 크룹 쿼터 관련 체크(group) |
| **-m** | 재마운트 생략(no-remount) |
| **-n** | 첫번째 검색된 것을 사용(use-first) |
| **-p** | 처리 결과를 출력(print-state) |
| **-v** | 파일 시스템의 상태를 보여줌(verse) |

* + 명령어 edquota: 편집기를 이용하여 사용자나 그룹에 디스크 사용량을 할당하는 명령어이다.
    - 형식: edquota [옵션] [계정명 또는 그룹명]

|  |  |
| --- | --- |
| **옵션** | **설명** |
| **-u** | 사용자 디스크 할당량 설정 |
| **-g** | 그룹 디스크 할당량 설정 |
| **-t** | 디스크 할당량 유예기간 설정 |
| **-p** | 디스크 사용량 설정을 다른 사용자와 동일하게 설정 |

* + 명령어 setquota: 편집기 기반이 아닌 명령행에서 직접 사용자나 그룹에 디스크 사용량을 할당하는 명령어이다.
    - 형식: setquota [옵션] [계정명 또는 그룹명] [block soft limit] [block hard limit] [inode soft limit] [inode hard limit] [파티션명]

|  |  |
| --- | --- |
| **옵션** | **설명** |
| **-u** | 사용자 디스크 할당량 설정 |
| **-g** | 그룹 디스크 할당량 설정 |
| **-a** | 해당 시스템의 모든 설정 |
| **-t** | 유예기간을 초(sec) 단위로 설정 |