



# 파일 권한 관리

## Linux 기본 사항

# 학습 내용

## 강의 핵심 내용

학습 내용:

- 파일 권한을 확인 및 변경합니다.
- 파일 권한에 대한 상징 표현과 절대 표현을 비교합니다.



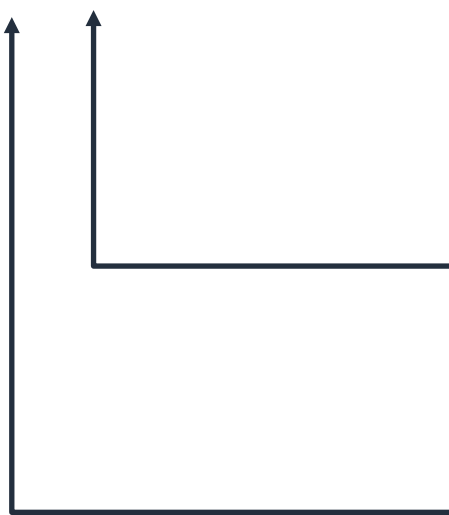


# 파일 권한 확인 및 변경

# Linux 권한 유형

`-rwxr-xr-x`

`-rwx`



**읽기(r):** 사용자가 파일을 열고 읽을 수 있는 권한입니다.

**쓰기(w):** 사용자가 파일 내용을 수정할 수 있는 권한입니다.

**실행(x):** 사용자가 프로그램을 실행할 수 있는 권한입니다.

**파일 유형:** 디렉터리 안에 있는 일반 파일 유형입니다.

# 권한 모드

```
]# chmod g+w file_1
```

상징 모드의 예

```
]# chmod 764 file_2
```

절대 모드의 예

상징 모드

```
[root@server00 Documents]# chmod g+w file1  
[root@server00 Documents]# chmod 764 file2
```

절대 모드

# ls -l 명령을 사용한 권한 보기

```
]# ls -l
```

ls 명령은 파일과 디렉터리를 나열하는 데 사용됩니다. -l 옵션은 파일이나 디렉터리, 크기, 수정한 날짜와 시간, 파일, 폴더 이름, 파일 소유자와 그 권한을 표시합니다.

권한

```
[root@server00 Documents]# ls -l
total 0
drwxr-xr-x. 2 root root 6 Feb 27 23:03 DirA
drwxr-xr-x. 2 root root 6 Feb 27 23:03 DirB
-rw-r--r--. 1 root root 0 Feb 27 23:03 file1
-rw-r--r--. 1 root root 0 Feb 27 23:03 file2
-rw-r--r--. 1 root root 0 Feb 27 23:03 file3
[root@server00 Documents]#
```

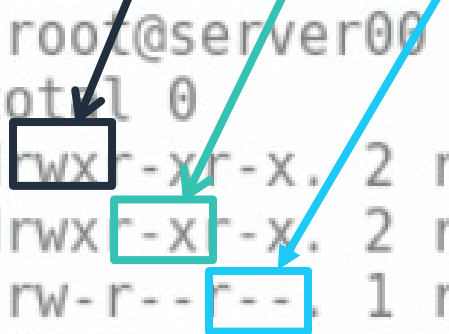
# 차이점 이해

사용자 권한

그룹 권한

기타 권한

```
[root@server00 Documents]# ls -l
total 0
drwxr-xr-x. 2 root root 6 Feb 27 23:03 DirA
drwxr-xr-x. 2 root root 6 Feb 27 23:03 DirB
-rw-r--r--. 1 root root 0 Feb 27 23:03 file1
-rw-r--r--. 1 root root 0 Feb 27 23:03 file2
-rw-r--r--. 1 root root 0 Feb 27 23:03 file3
[root@server00 Documents]#
```



# 사용자 또는 소유자 아이덴티티

소유자가 읽고, 쓰고,  
실행할 수 있습니다.

소유자

-rwx r-x r--

2 c\_salazar reStart\_stu

111 Jul 12 02:51

소유자 권한

파일 소유자는 사용자 아이덴티티 또는 이름에 적용하는 권한을 제어합니다.



# 그룹 아이덴티티

그룹이 읽고,  
실행할 수 있습니다.

그룹

-rwx r-x r--

2 c\_salazar reStart\_stu

111 Jul 12 02:51

그룹 권한

그룹 구성원에게는 파일 또는 디렉터리에 대한 그룹 권한이 부여됩니다.

# 기타 아이덴티티

다른 사용자가 읽을 수  
있습니다.

```
]# -rwx r-x r--      2 c_salazar reStart_stu      111 Jul 12 02:51
```

기타 권한

# ls -l 명령으로 전체 실행 파일 출력

소유자가 읽고, 쓰고,  
실행할 수 있습니다.

다른 사람이 읽을  
수 있습니다.

그룹이 읽고,  
실행할 수 있습니다.

소유자

그룹

```
]# -rwx r-x r--      2 c_salazar reStart_stu      111 Jul 12 02:51
```

소유자 권한

기타 권한

그룹 권한

# 기본 권한

스탠더드 사용자(루트 아님)가 userA@ 또는 username@을 사용하여 파일 또는 디렉터리를 만드는 경우

```
~]$ sudo command
```

루트 사용자가 root@를 사용하여 파일 또는 디렉터리를 만드는 경우

```
]# command
```

# chown 명령

```
[root@hostname ~]# chown [options] user[:group] file(s)
```

**chown new-owner:new-group file1**

↑        ↑        ↑        ↑  
명령    사용자    그룹    파일

**chown new-owner file1**

↑        ↑        ↑  
명령    사용자    파일

**chown :new-group file1**

↑        ↑        ↑  
명령    그룹    파일

```
[root@ip-10-0-4-100 projects]# chown jstiles file2
[root@ip-10-0-4-100 projects]# chown arosalez file3
[root@ip-10-0-4-100 projects]# chown :sales file1
[root@ip-10-0-4-100 projects]# █
```

# 파일 권한의 상징 표현과 절대 표현

# chmod 명령

```
chmod [permissions] file1.txt
```

# 상징 모드에서의 chmod 명령

아이덴티티	권한	연산자
u(사용자 또는 소유자)	r(읽기)	+ 권한 부여
g(그룹)	w(쓰기)	- 권한 삭제
o(기타)	x(실행)	= 권한을 삭제하고 새 권한을 설정

```
]$ chmod u+x process.sh  
]$ chmod g=x process.sh  
]$ chmod g-rw Roseter.csv  
]$ chmod o-r process.sh
```

u+x - 사용자에게 실행 권한이 주어짐

g=x - 그룹 실행 권한이 삭제됨

g-rw - 그룹 읽기/쓰기 권한이 삭제됨

```
-rwx--x--- 1 labsuser labsuser 0 Mar 29 07:48 process.sh  
-rw----r-- 1 labsuser labsuser 0 Mar 29 07:47 Roseter.csv
```



# 절대 모드에서의 chmod 명령

권한	값
읽기	4
쓰기	2
실행	1
모든 권한	7

```
[root@server00 Documents]# chmod 764 file1
[root@server00 Documents]# chmod 740 file2
[root@server00 Documents]# chmod 777 file3
[root@server00 Documents]# ls -l
total 0
drwxr-xr-x. 2 root root 6 Feb 27 23:03 DirA
drwxr-xr-x. 2 root root 6 Feb 27 23:03 DirB
-rwxrw-r--. 1 root root 0 Feb 27 23:03 file1
-rwxr-----. 1 root root 0 Feb 27 23:03 file2
-rwxrwxrwx. 1 root root 0 Feb 27 23:03 file3
[root@server00 Documents]#
```

절대 모드에서는 파일 권한을 나타내는 8진수를 사용하여 파일 권한을 변경할 수 있습니다.

```
]# chmod 400 file_1
```

다음과 같이 출력됩니다.

```
]# - r-----. 2 c_salazar reStart_stu 111 Jul 12 02:51 file_1
```

# 데모: 파일 권한의 식별 및 구성



이 데모에서는 파일을 만들고 기본 권한을 검사합니다.

터미널 창을 엽니다.

1. touch 명령을 사용하여 새 파일을 만듭니다.

```
[root@hostname ~]# touch file_1
```

2. ls -l 명령을 실행하고 다음 질문에 답합니다.

- 파일은 누가 소유합니까?
- 파일은 어떤 그룹이 소유합니까?

```
[root@hostname ~]# ls -l
```

3. chmod 400을 사용하여 새 파일을 읽기 전용으로 만듭니다.

4. ls -l를 실행하여 권한 변경을 확인합니다.

# 파일 권한 관리에 대한 모범 실무



다음은 Linux에서 권한을 관리하는 경우의 모범 실무입니다.

# 확인 질문



파일과 디렉터리에 적절한 권한을 지정하지 않으면 어떤 위험이 있습니까?



절대 모드, 상징 모드 중에 어떤 것을 선호하십니까? 그 이유는 무엇입니까?

# 요점



- 절대 모드 또는 상징 모드에서 `chmod` 명령을 사용하여 Linux에 있는 파일에 권한을 지정합니다.
- `ls -l`는 권한을 보는 데 사용됩니다.
- `chown` 명령은 소유권을 변경하는 데 사용됩니다.

# 감사합니다.

© 2021 Amazon Web Services, Inc. 또는 자회사. All rights reserved. 본 내용은 Amazon Web Services, Inc.의 사전 서면 허가 없이 전체 또는 일부를 복제하거나 재배포할 수 없습니다. 상업적인 복제, 임대 또는 판매는 금지됩니다. 수정해야 할 사항, 피드백 또는 기타 질문이 있다면 <https://support.aws.amazon.com/#/contacts/aws-training> 에서 문의해 주십시오. 모든 상표는 해당 소유자의 자산입니다.

