

# 실습 - 사용자 및 그룹

## 목표

본 실습에서는 다음을 수행한다.

- 기본 암호를 사용하여 새 사용자 생성
- 그룹 생성 및 적절한 사용자 할당
- 다른 사용자로 로그인

## 소요 시간

본 실습을 완료하는 데는 약 **45 분**이 소요된다.

## AWS 서비스 제한 사항

이 실습 환경에서 AWS 서비스 및 서비스 액션에 대한 액세스는 실습 지침을 완료하는 데 필요한 작업으로 제한될 수 있다. 다른 서비스에 액세스하거나 이 실습에서 설명하는 것 이외의 액션을 수행하려고 하면 오류가 발생할 수 있다.

## 태스크 1: SSH 를 사용하여 Linux EC2 인스턴스에 연결

## 태스크 2: 사용자 생성

이 섹션에서는 다음 테이블을 기반으로 사용자를 생성한다.

이름	성	사용자 ID	직무	시작 암호
Alejandro	Rosalez	arosalez	Sales Manager	P@ssword1234!

이름	성	사용자 ID	직무	시작 암호
Efua	Owusu	eowusu	Shipping	P@ssword1234!
Jane	Doe	jdoe	Shipping	P@ssword1234!
Li	Juan	ljuan	HR Manager	P@ssword1234!
Mary	Major	mmajor	Finance Manager	P@ssword1234!
Mateo	Jackson	mjackson	CEO	P@ssword1234!
Nikki	Wolf	nwolf	Sales Representative	P@ssword1234!
Paulo	Santos	psantos	Shipping	P@ssword1234!
Sofia	Martinez	smartinez	HR Specialist	P@ssword1234!
Saanvi	Sarkar	ssarkar	Finance Specialist	P@ssword1234!

이러한 사용자가 기본 보안 인증을 사용하여 로그인할 수 있도록 사용자 ID의 철자가 올바른지 확인한다.

1. **pwd** 입력하고 ENTER 키를 눌러 현재 사용자의 홈 폴더에 있는지 확인한다

```
ubuntu@ip-172-31-3-46:~$ pwd
/home/ubuntu
ubuntu@ip-172-31-3-46:~$ █
```

2. 위의 목록에서 첫 번째 사용자인 **Alejandro Rosalez**를 추가하려면 `sudo adduser arosalez`를 입력하고 Enter 키를 누른다. 이렇게 하면 사용자 **arosalez**가 생성된다.
3. 암호는 2번 입력해야 한다. `P@ssword1234!`를 암호로 사용해도 된다.

주 암호를 입력할 때 화면에 아무 것도 표시되지 않으면 암호를 입력하고 Enter 키를 누른다.

```

ubuntu@ip-172-31-3-46:~$ sudo adduser arosalez
Adding user `arosalez' ...
Adding new group `arosalez' (1001) ...
Adding new user `arosalez' (1001) with group `arosalez' ...
Creating home directory `/home/arosalez' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for arosalez
Enter the new value, or press ENTER for the default
    Full Name []: Alejandro Rosalez
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n]
ubuntu@ip-172-31-3-46:~$ █

```

4. 사용자가 생성되었음을 확인하려면 `sudo cat /etc/passwd | cut -d: -f1` 를 입력하고 Enter 키를 눌러 `/etc/passwd` 파일의 내용을 살펴본다.

```

ubuntu@ip-172-31-3-46:~$ sudo cat /etc/passwd | cut -d: -f1
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
backup
list
irc
gnats
nobody
systemd-network
systemd-resolve
messagebus
systemd-timesync
syslog
_appt
tss
uidd
tcpdump
sshd
pollinate
landscape
fwupd-refresh
ec2-instance-connect
_chrony
ubuntu
lxd
arosalez
ubuntu@ip-172-31-3-46:~$

```

## 주

이 명령은 생성된 사용자를 시각화하는 데 사용되며 현재로서는 기억할 필요가 없다. **cat** 은 가장 널리 사용되는 명령 중 하나이다. 이 명령의 용도 중 하나는 파일을 표시하는 것이다. `cat /etc/passwd` 를 입력하여 파일의 전체 내용을 표시할 수 있다. 단, 이 옵션은 많은 정보를 표시하므로 가독성이 떨어질 수 있다. 지금은 명령의 두 번째 부분을 크게 신경 쓰지 않는다. **cat, cut, |** 명령에 대해서는 이 과정의 뒷부분에서 자세히 알아보겠다. 또한 사용자 추가할 때 `useradd` 명령어와 `adduser` 의 명령어가 서로 다를 수 있다.

5. `sudo useradd <User ID>` 및 `sudo passwd <User ID>` 명령을 사용하여 테이블의 나머지 사용자를 추가한다. `<User ID>`를 이 태스크의 시작 부분에 있는 테이블의 각 **User ID** 로 바꾸십시오.

```
ubuntu@ip-172-31-3-46:~$ sudo useradd eowusu
ubuntu@ip-172-31-3-46:~$ sudo passwd eowusu
New password:
Retype new password:
passwd: password updated successfully
ubuntu@ip-172-31-3-46:~$
```

6. 사용자가 생성되었음을 확인하려면 `sudo cat /etc/passwd | cut -d: -f1` 를 입력하고 Enter 키를 누른다.

```
ubuntu@ip-172-31-3-46:~$ sudo cat /etc/passwd | cut -d: -f1
root
daemon
bin
sys
sync
```

```
ubuntu
lxd
arosalez
eowusu
jdoe
ljuan
mmajor
mjackson
nwolf
psantos
smartinez
ssarkar
ubuntu@ip-172-31-3-46:~$
```

## 태스크 3: 그룹 생성

이 섹션에서는 사용자 그룹을 생성하고 그룹에 사용자를 추가한다.

- Sales
- HR
- Finance
- Personnel
- CEO
- Shipping
- Managers

이러한 그룹을 생성한 후 태스크 2의 테이블에 제공된 정보를 기반으로 적절한 그룹에 사용자를 추가한다.

주 루트 사용자가 아닌 경우 **sudo**를 사용하여 이 연습을 완료해야 할 수 있다.

주의. 관리자는 직원이지만 모든 직원이 관리자는 아니다. 일부 사용자는 여러 그룹에 속할 수 있다.

7. 사용자의 현재 위치가 홈 폴더라는 것을 확인하려면 `pwd`를 입력하고 Enter 키를 누른다.
8. **Sales** 그룹을 생성하려면 `sudo groupadd Sales`를 입력하고 Enter 키를 누른다.
9. 그룹이 추가되었음을 확인하려면 `cat /etc/group`을 입력하고 Enter 키를 누른다.

```
ubuntu@ip-172-31-3-46:~$ sudo groupadd Sales
ubuntu@ip-172-31-3-46:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
```

```
psantos:x:1008:
smartinez:x:1009:
ssarkar:x:1010:
Sales:x:1011:
ubuntu@ip-172-31-3-46:~$ █
```

주 `/etc/group` 파일에는 모든 그룹이 포함된다. 사용자가 생성될 때마다 그룹도 생성되기 때문에 이전에 생성한 사용자는 이미 소속된 그룹이 있는 것을 알 수 있다. 표시된 번호가 다른 번호가 있을 수 있다. 첫 번째 콜론 뒤에 숨겨진 다른 정보를 신경 쓰지 않아도 된다. `/etc/group` 형식에 대해서는 이 과정의 뒷부분에서 자세히 배울 것이다.

10. `sudo groupadd <Group>` 명령을 사용하여 나머지 그룹을 추가한다. `<Group>`을 **HR**, **Finance**, **Shipping**, **Managers**, **CEO**로 바꿔 이러한 그룹을 생성한다.
11. 모든 그룹이 추가되었음을 확인하려면 `cat /etc/group`을 입력하고 Enter 키를 누른다.

```

ssarkar:x:1010:
Sales:x:1011:
HR:x:1012:
Finance:x:1013:
Shipping:x:1014:
Managers:x:1015:
CEO:x:1016:
ubuntu@ip-172-31-3-46:~$

```

12. 사용자 **arosalez** 를 **Sales** 그룹에 추가하려면 터미널에 `sudo usermod -a -G Sales arosalez` 에 입력하고 Enter 키를 누른다.
13. 사용자가 추가되었음을 확인하려면 `cat /etc/group` 을 입력하고 Enter 키를 누른다.

```

ubuntu@ip-172-31-3-46:~$ sudo usermod -a -G Sales arosalez
ubuntu@ip-172-31-3-46:~$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
ssarkar:x:1010:
Sales:x:1011:arosalez
HR:x:1012:
Finance:x:1013:
Shipping:x:1014:
Managers:x:1015:
CEO:x:1016:

```

14. `sudo usermod -a -G <Group Name> <User ID>` 명령을 사용하여 나머지 사용자를 적절한 그룹에 추가한다. 다음 테이블의 정보를 사용하며 *<Group Name>*을 **Group Name** 으로 바꾸고, *<User ID>*를 **User ID** 열의 각 사용자 ID 로 변경한다.

그룹 이름	사용자 ID	그룹 이름	사용자 ID	그룹 이름	사용자 ID
Sales	arosalez, nwolf	HR	ljuan, smartinez	Finance	mmajor, ssarkar
Shipping	eowusu, jdoe, psantos	Managers	ljuan, mmajor	CEO	mjackson

15. 모든 그룹에 **ubuntu** 를 추가한다.

```

ubuntu@ip-172-31-3-46:~$ sudo usermod -a -G Sales ubuntu
ubuntu@ip-172-31-3-46:~$ sudo usermod -a -G HR ubuntu
ubuntu@ip-172-31-3-46:~$ sudo usermod -a -G Finance ubuntu
ubuntu@ip-172-31-3-46:~$ sudo usermod -a -G Shipping ubuntu
ubuntu@ip-172-31-3-46:~$ sudo usermod -a -G Managers ubuntu
ubuntu@ip-172-31-3-46:~$ sudo usermod -a -G CEO ubuntu
ubuntu@ip-172-31-3-46:~$

```

16. 그룹 멤버십을 확인하려면 터미널에 `sudo cat /etc/group` 을 입력하고 Enter 키를 누른다.

```
Sales:x:1011:arosalez,nwolf,ubuntu
HR:x:1012:ljuan,smartinez,ubuntu
Finance:x:1013:mmajor,ssarkar,ubuntu
Shipping:x:1014:eowusu,jdoe,psantos,ubuntu
Managers:x:1015:ljuan,mmajor,ubuntu
CEO:x:1016:mjackson,ubuntu
ubuntu@ip-172-31-3-46:~$
```

## 과제 4: 새로운 사용자로 로그인

이제 시스템에 일부 사용자가 생성되었으므로 새로운 사용자로 로그인할 수 있다. 또한 **sudoer** 가 무엇이고 어떻게 활성화하는지, 그리고 **sudo** 를 사용하여 실행된 명령이 **/var/log/secure** 파일에 기록되는 방법을 확인할 수 있다.

주

루트 사용자가 아닌 경우 **sudo** 를 사용하여 이 연습을 완료해야 할 수 있다.

17. **su arosalez** 를 입력한다.

18. 암호로는 **P@ssword1234!**를 입력하고 Enter 키를 누른다. 현재 **arosalez** 로 로그인되어 있다.

```
ubuntu@ip-172-31-3-46:~$ su arosalez
Password:
arosalez@ip-172-31-3-46:/home/ubuntu$
```

끝에 있는 **ubuntu** 는 사용자 위치가 **ubuntu** 홈 디렉터리인 **/home/ubuntu** 임을 나타낸다.

19. **pwd** 를 입력하고 Enter 키를 눌러 현재 위치가 **/home/ubuntu** 디렉터리라는 것을 확인한다.

20. **touch myFile.txt** 를 입력하고 Enter 키를 누른다.

```
arosalez@ip-172-31-3-46:/home/ubuntu$ touch myFile.txt
touch: cannot touch 'myFile.txt': Permission denied
arosalez@ip-172-31-3-46:/home/ubuntu$
```

사용자 **arosalez** 에게 **ubuntu** 홈 폴더에 파일을 쓸 수 있는 권한이 없기 때문에 이 메시지가 표시된다.



21. 이제 **sudo** 명령을 사용하여 관리자로 시도한다. `sudo touch myFile.txt` 를 입력하고 Enter 키를 누른다.
22. 암호 **P@ssword1234!**를 입력하고 Enter 키를 누른다.

```
arosalez@ip-172-31-3-46:/home/ubuntu$ sudo touch myFile.txt
[sudo] password for arosalez:
arosalez is not in the sudoers file. This incident will be reported.
arosalez@ip-172-31-3-46:/home/ubuntu$
```

사용자 **arosalez** 가 sudoer 파일의 목록에 없기 때문에 이 메시지가 표시된다. Sudoer 는 루트 권리가 필요한 명령을 실행할 수 있는 특별한 권리가 있는 사용자이다. 소수의 사용자에게만 이 권한이 부여되어야 한다.

23. `exit` 를 입력하고 Enter 키를 눌러 이전 사용자 **ubuntu** 로 전환한다.

```
arosalez@ip-172-31-3-46:/home/ubuntu$ exit
exit
ubuntu@ip-172-31-3-46:~$
```

24. 이제 `/var/log/auth.log` 파일의 내용이 시각화된다. `sudo cat /var/log/auth.log` 를 입력하고 Enter 키를 눌러 보안 파일의 내용을 표시한다. 아래쪽 화살표를 사용하여 파일의 맨 아래로 스크롤한다.

```
Dec 19 07:30:32 ip-172-31-3-46 sudo: arosalez : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/touch myFile.txt
Dec 19 07:31:45 ip-172-31-3-46 su: pam_unix(su:session): session closed for user arosalez
```

`sudo` 및 허용되지 않은 액션이 `/var/log/auth.log` 파일에 기록된 방법을 확인할 수 있다.