



사용자 및 그룹

Linux 기본 사항

학습 내용

강의 핵심 내용

학습 내용:

- 사용자 계정을 관리합니다.
- 그룹 계정을 관리합니다.
- `su` 명령과 `sudo` 명령으로 권한을 승격합니다.
- Amazon Web Services(AWS)에서 사용하는 인증 서비스인 AWS Identity and Access Management(IAM)를 설명합니다.






사용자 관리

사용자 계정

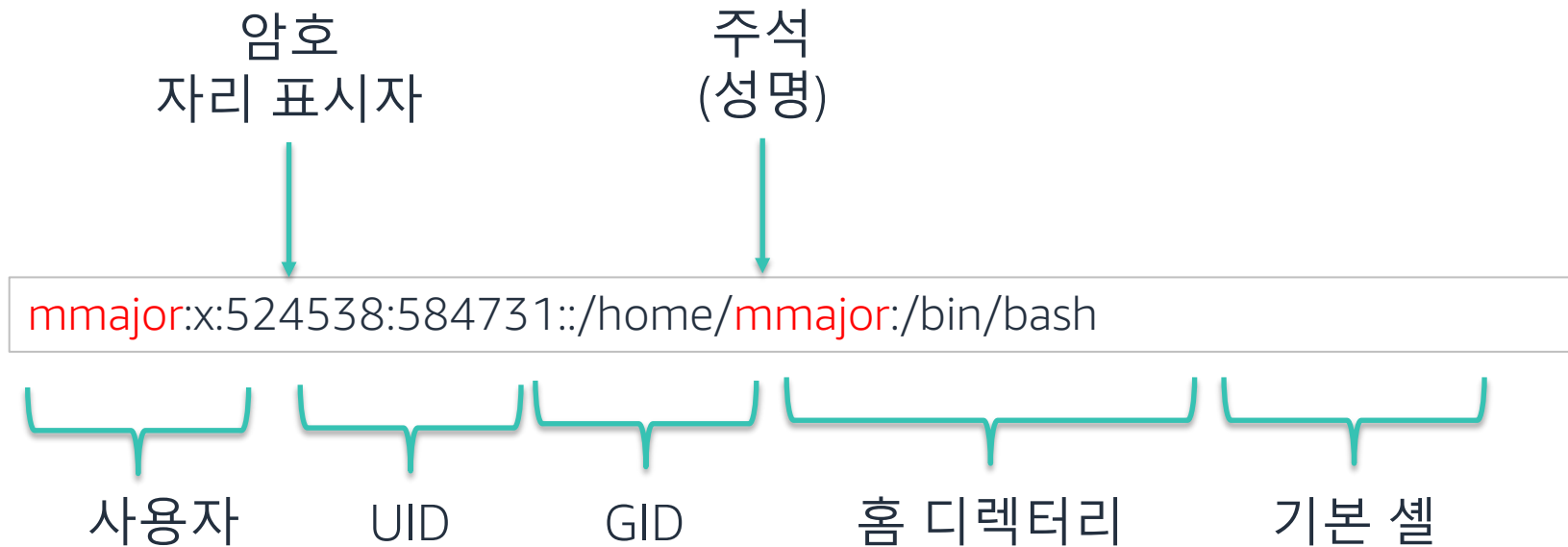
- 사용자 계정은 시스템 사용자를 나타냅니다.
- 사용자 정보는 로컬에 저장하거나 네트워크를 통해 액세스할 수 있는 다른 서버에 저장할 수 있습니다.
- 정보가 로컬에 저장되면 Linux는 이 정보를 `/etc/passwd` 파일에 저장합니다.
- 계정당 사용자 한 명을 할당하는 것이 가장 좋습니다.
- 계정을 공유하지 마십시오.

```
[root@ip-10-0-4-100 ~]# tail /etc/passwd
libstoragemgmt:x:999:997:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
ec2-instance-connect:x:998:996:./home/ec2-instance-connect:/sbin/nologin
postfix:x:89:89:./var/spool/postfix:/sbin/nologin
chrony:x:997:995:./var/lib/chrony:/sbin/nologin
tcpdump:x:72:72:./:/sbin/nologin
ec2-user:x:1000:1000:EC2 Default User:/home/ec2-user:/bin/bash
arosalez:x:1001:1001:./home/arosalez:/bin/bash
[root@ip-10-0-4-100 ~]#
```



/etc/passwd 파일

Linux는 계정을 /etc/passwd 파일에 저장합니다.



기본 사용자 계정

- Linux와 서비스를 설치하는 동안 기본 시스템 계정이 만들어집니다.
- 예를 들면, 설치 중에 루트 사용자 계정이 만들어져 시스템을 관리할 수 있습니다.

```
[root@ip-10-0-4-100 ~]# head /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
```

useradd 명령

- 사용자 계정 만들기
- /home에 사용자의 홈 디렉터리 만들기
- 계정 기본값 정의

```
[root@ip-10-0-4-100 ~]# useradd mmajor
[root@ip-10-0-4-100 ~]# id mmajor
uid=1002(mmajor) gid=1002(mmajor) groups=1002(mmajor)
[root@ip-10-0-4-100 ~]# grep mmajor /etc/passwd
mmajor:x:1002:1002::/home/mmajor:/bin/bash
[root@ip-10-0-4-100 ~]#
```

useradd 명령 옵션

- 옵션을 이용하면 생성 시 사용자 계정을 사용자 지정할 수 있습니다.
- 주석 필드는 사용자 성명을 저장하는 데 사용되는 경우가 많습니다.

| 옵션 | 설명 | 예 |
|----|-----------|---|
| -c | 주석 | <code>useradd -c "new employee" jdoe</code> |
| -e | 계정 만료 | <code>useradd -e 2025-01-01 jdoe</code> |
| -d | 홈 디렉터리 경로 | <code>useradd -d /users/jdoe jdoe</code> |

usermod 명령

이 명령은 기존 사용자 계정의 일부 또는 전부를 수정하거나 변경하는 데 사용됩니다.

| 옵션 | 설명 | 예 |
|----|-------|---|
| -c | 주석 | <code>usermod -c "Mary Major" mmajor</code> |
| -e | 계정 만료 | <code>usermod -e 2025-01-01 mmajor</code> |

```
[root@ip-10-0-4-100 ~]# grep mmajor /etc/passwd
mmajor:x:1002:1002::/home/mmajor:/bin/bash
[root@ip-10-0-4-100 ~]# usermod -c "Mary Major" mmajor
[root@ip-10-0-4-100 ~]# grep mmajor /etc/passwd
mmajor:x:1002:1002:Mary Major:/home/mmajor:/bin/bash
```

userdel 명령

- 사용자 계정 삭제
- -r 옵션을 사용하여 사용자 홈 디렉터리도 삭제

```
[root@ip-172-31-27-186 ~]# useradd jdoe
[root@ip-172-31-27-186 ~]# id jdoe
uid=1002(jdoe) gid=1002(jdoe) groups=1002(jdoe)
[root@ip-172-31-27-186 ~]# userdel -r jdoe
[root@ip-172-31-27-186 ~]# id jdoe
id: jdoe: no such user
[root@ip-172-31-27-186 ~]#
```

passwd 명령

- 사용자 암호는 passwd 명령으로 설정합니다.
- 암호를 두 번 입력해야 합니다.
- 사용자는 자신의 암호를 재설정할 수 있으며, 루트 사용자는 모든 사용자 암호를 재설정할 수 있습니다.
- 암호를 설정할 때에는 화면에 문자가 표시되지 않습니다.

```
[root@ip-10-0-4-100 ~]# passwd mmajor
Changing password for user mmajor.
[New password:
[Retype new password:
passwd: all authentication tokens updated successfully.
[root@ip-10-0-4-100 ~]#
```



그룹 관리

그룹이란?

- 그룹은 계정 집합입니다.
- 그룹은 보안 요구 사항이 비슷한 사용자 계정을 연결하는 편리한 방법입니다.
- 예를 들면, 사용자 네 명에게 개별적으로 권한을 부여하는 것보다 사용자가 네 명인 그룹 1개에 권한을 부여하는 게 더 쉽습니다.
- 그룹 저장 위치는 `/etc/group` 파일입니다.

| 그룹 | 사용자 |
|----------|--------------------------------|
| ec2-user | mmajor, jdoe, ljuan, moliveira |
| devs | jdoe, wxiulan |

/etc/group 파일

그룹 저장 위치

```
systemd-journal:x:190:ec2-user
```

그룹

그룹암호

그룹 ID

그룹 구성원

groupadd, groupmod, groupdel 명령

| 옵션 | 설명 | 예 |
|----------|----------|---|
| groupadd | 새 그룹 만들기 | groupadd <i>group</i> |
| groupmod | 기존 그룹 수정 | groupmod -n <i>new_group</i> <i>old_group</i> |
| groupdel | 기존 그룹 삭제 | groupdel <i>group</i> |

```
[root@ip-172-31-27-186 ~]# groupadd marketing
[root@ip-172-31-27-186 ~]# tail -n 3 /etc/group
mmajor:x:1001:
devs:x:1004:mmajor
marketing:x:1005:
```

groupadd 명령

```
[root@ip-172-31-27-186 ~]# groupdel marketing
[root@ip-172-31-27-186 ~]# tail -n 3 /etc/group
ec2-user:x:1000:
mmajor:x:1001:
devs:x:1004:mmajor
```

groupdel 명령

그룹에 사용자 추가

- 그룹에 사용자를 추가하는 것은 그룹 수정이 아니라 사용자 수정입니다.
- 그룹에 사용자를 추가하려면 다음을 사용하면 됩니다.
 - usermod 명령
 - gpasswd 명령

```
[root@ip-172-31-27-186 ~]# usermod -aG hr,marketing mmajor
[root@ip-172-31-27-186 ~]# gpasswd -a jdoe marketing
Adding user jdoe to group marketing
[root@ip-172-31-27-186 ~]# tail -n 5 /etc/group
mmajor:x:1001:
devs:x:1004:mmajor
jdoe:x:1002:
marketing:x:1005:mmajor,jdoe
hr:x:1006:mmajor
[root@ip-172-31-27-186 ~]#
```


gpasword 명령

- /etc/group 파일 관리에 사용됨
- 사용 방법: `gpaswd [option] GROUP`

| 옵션 | 설명 |
|--|--------------|
| -a, --add | 그룹에 사용자 추가 |
| -d, --delete | 그룹에서 사용자 제거 |
| -M, --members USER1,USER2,... | 그룹 구성원 목록 설정 |
| -A, --administrators ADMIN1,ADMIN2,... | 그룹 관리자 목록 설정 |



사용자 권한

사용자 권한 수준



루트 사용자

- 모든 파일에 액세스
- 모든 파일 수정
- 제어 서비스
- 모든 계정 관리
- 하드웨어 관리
- Linux 커널 관리
- 소프트웨어 관리



스탠더드 사용자

- 권한이 주어진다면 모든 파일에 액세스
- 사용자가 소유한 모든 파일 제어
- 시스템 관리에 대한 제한된 액세스

root 사용 시 주의 사항

- 보안 모범 실무: 관리자 권한으로 시스템에 로그인하지 마십시오.
- 스탠더드 사용자로 로그인한 후 필요한 경우에만 권한을 승격합니다.
- 루트 사용자는 강력한 Linux 계정이므로, 실수로 인해 시스템이 작동하지 않을 수 있습니다.
- 루트 사용자 명령 프롬프트는 #으로 끝납니다.
- 스탠더드 사용자 명령 프롬프트는 \$로 끝납니다.

```
[root@server00 ~]# exit  
logout  
[userA@server00 ~]$
```

su 명령

- 스탠더드 사용자로 로그인한 후 권한을 승격하여 관리 태스크를 수행합니다.
- 루트 컨텍스트 종료에 주의합니다.

| 명령 | 설명 |
|-----------|--------------------|
| su root | 현재 사용자 환경에서 루트로 전환 |
| su - root | 루트 환경에서 루트로 전환 |

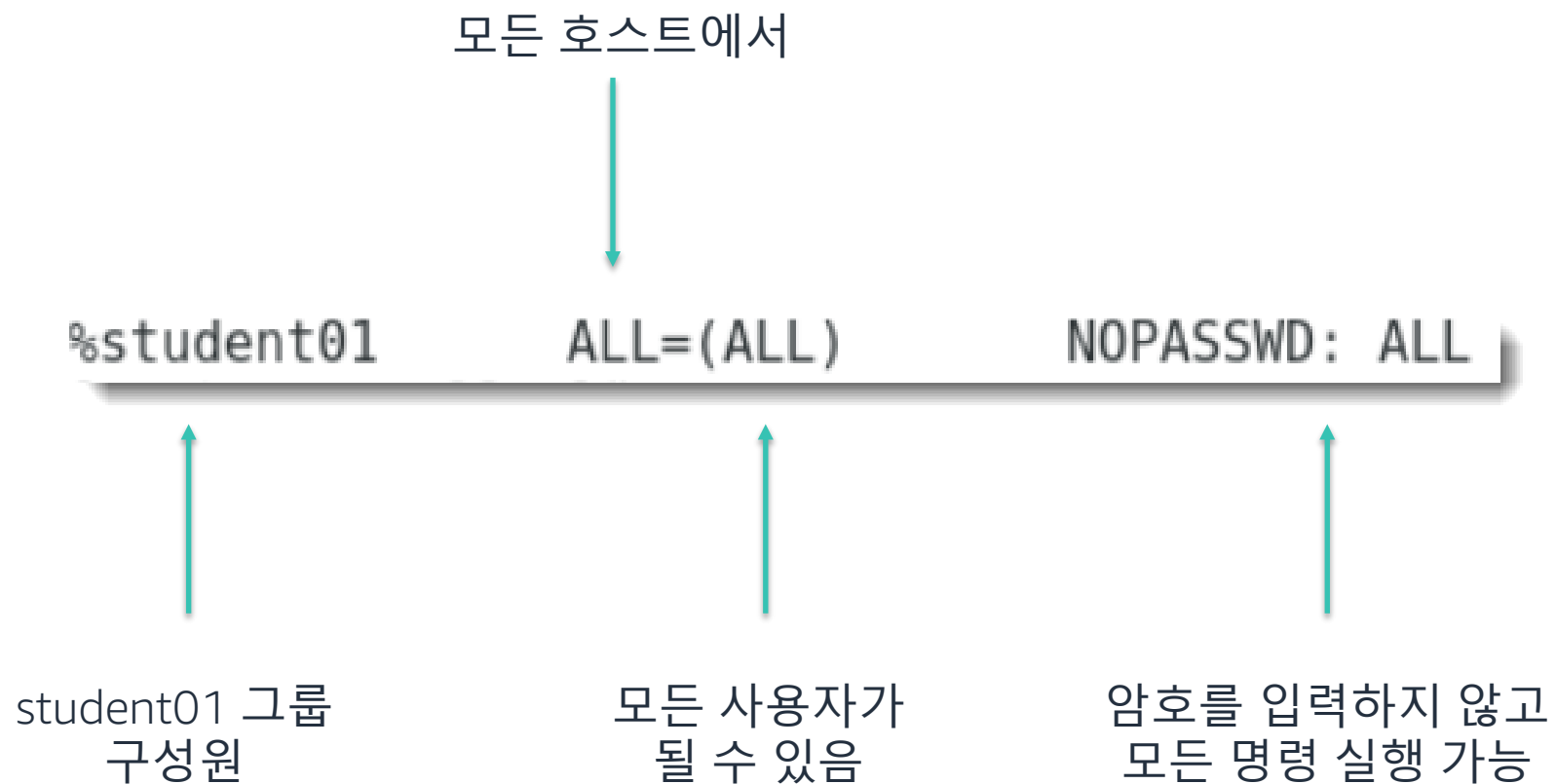
```
[userA@server00 ~]$ su root
Password:
[root@server00 userA]# exit
exit
[userA@server00 ~]$ su - root
Password:
Last login: Thu Feb 28 01:02:16 GMT 2019 on pts/0
[root@server00 ~]#
```

/etc/sudoers 파일

- 특정 명령을 /etc/sudoers에 추가하여 특정 사용자에게 특정 명령을 위임합니다.
- 구문: `users hosts=(user:group) commands`
- 예:
 - 사용자 그룹 구성원이 로컬 호스트를 종료하도록 허용합니다.
 - `%users localhost=/usr/sbin/shutdown -r now`
 - 개발자 그룹 구성원이 암호를 요청하지 않고 모든 호스트에서 모든 액션을 수행하도록 허용합니다.
 - `%devs ALL=(ALL) NOPASSWD: ALL`
- 특정 명령을 /etc/sudoers 파일에 추가하여 특정 사용자에게 특정 명령을 위임합니다.

/etc/sudoers 파일 - 계속

일반 형식: # WHO WHERE = (AS WHOM) WHAT



sudo 사용

student01 계정은 `sudo`를 통해 사용자를 생성할 수 있는 권한을 위임받았습니다.

```
[student01@server00 ~]$ sudo useradd user20  
[sudo] password for student01:  
[student01@server00 ~]$
```



sudo 명령

-lU 옵션을 사용하여 위임된 sudo 권한을 살펴봅니다.

```
[student01@server00 ~]$ sudo -lU student01
Matching Defaults entries for student01 on server00:
    !visiblepw, always_set_home, match_group_by_gid, env_reset,
    env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
    env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE",
    env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE",
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User student01 may run the following commands on server00:
    (ALL) NOPASSWD: ALL
[student01@server00 ~]$
```

sudo 로그

- sudo 권한 사용은 /var/log/messages에 로그됩니다.
- sudo 권한으로 실행되는 명령은 /var/log/secure에 로그됩니다.

```
[root@server00 ~]# tail /var/log/messages  
Feb 28 01:02:16 server00 su: (to root) userA on pts/0
```

su 명령과 sudo 명령의 비교

- su 명령은 전체 관리 권한을 활성화합니다.
 - 모든 관리 권한이 필요할 때 사용됨
 - 사용자에게 루트 암호를 묻는 메시지 표시
- sudo 명령은 위임된 권한만 활성화합니다.
 - 특정 스탠더드 사용자에게 특정 관리 태스크를 위임하는 데 사용됨
 - 사용자에게 자신의 암호를 묻는 메시지 표시

확인 질문

사용자 계정을 추가하는 데 사용하는 명령은 무엇입니까?

사용자 암호를 재설정하는 데 사용하는 명령은 무엇입니까?

사용자를 그룹으로 구성하면 관리자에게 어떤 도움이 됩니까?

사용자 환경에서 사용자에게 전체 관리 권한을 부여하는 데 사용하는 명령은 무엇입니까?



IAM

AWS Identity and Access Management(IAM)

- IAM은 사용자와 리소스 액세스를 관리하는 데 사용되는 AWS 서비스입니다.
- 사용자, 그룹, 역할을 만들 수 있고, 정책을 적용하여 리소스에 대한 액세스를 제어할 수 있습니다.
- 다음을 통해 IAM에 액세스할 수 있습니다.
 - 브라우저를 통한 웹 인터페이스인 AWS 관리 콘솔
 - Linux 셸 또는 Windows 명령줄을 사용하여 액세스할 수 있는 명령줄 인터페이스인 AWS Command Line Interface(AWS CLI)
 - Java, Python, JavaScript 등 다양한 언어로 사용 가능한 AWS 소프트웨어 개발 키트(SDK)



AWS Identity and
Access
Management(IAM)



AWS 관리
콘솔

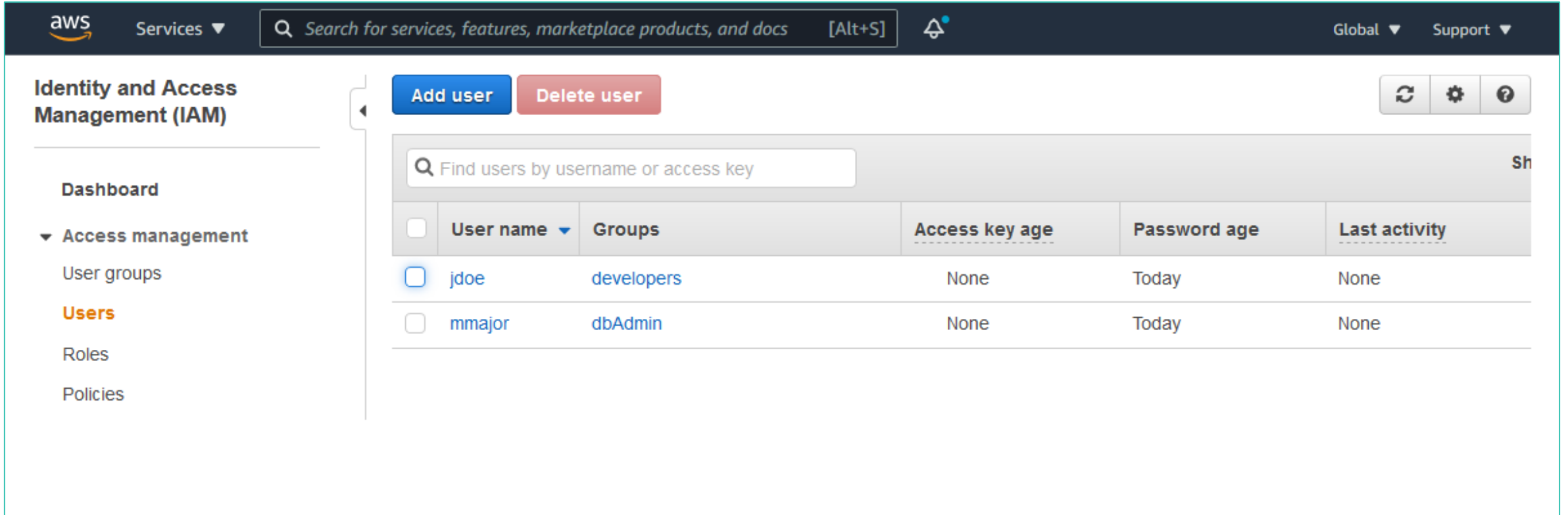


AWS Command Line
Interface(AWS CLI)



AWS 도구
및 SDK

AWS 관리 콘솔의 스냅샷



The screenshot displays the AWS Identity and Access Management (IAM) console. The top navigation bar includes the AWS logo, a search bar, and links for Global and Support. The left sidebar shows the navigation menu with 'Users' highlighted. The main content area shows a table of users with columns for selection, username, groups, access key age, password age, and last activity. Two users are listed: 'jdoe' and 'mmajor'.

| | User name | Groups | Access key age | Password age | Last activity |
|--------------------------|-----------|------------|----------------|--------------|---------------|
| <input type="checkbox"/> | jdoe | developers | None | Today | None |
| <input type="checkbox"/> | mmajor | dbAdmin | None | Today | None |

요점



- Linux **사용자 계정**은 시스템 사용자를 나타냅니다.
- 여러 사용자 계정을 Linux **그룹**으로 그룹화하여 용이하게 보안 성능을 관리할 수 있습니다.
- **루트** 사용자는 시스템의 모든 항목에 액세스하고 수정할 수 있는 권한을 보유합니다.
- **su** 명령을 사용해 명령을 실행할 다른 사용자로 전환할 수 있습니다.
- **sudo** 명령을 사용해 일회성 루트 권한으로 명령을 실행할 수 있습니다.
- IAM은 사용자와 리소스 액세스를 관리하는 데 사용되는 AWS 서비스입니다.

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.

