7장

Linux 사용자 및 그룹 관리

전체 내용

사용자 계정 관리

그룹 계정 관리

관리 권한
위임하기

1 – 사용자 계정 관리

- 사용자 계정 관련 파일 알아보기
- 사용자 계정 생성, 수정, 삭제하기
- 사용자 정보 관리 명령
- 사용자 단위로 디스크 할당량 설정

1 – 사용자 계정 관련 파일 알아보기

- 사용자 계정과 관련된 파일
  - /etc/passwd: 사용자 계정 정보가 저장된 기본 파일
  - /etc/shadow: 사용자 계정의 암호를 저장해 놓은 파일
  - /etc/login.defs: 사용자 계정의 설정과 관련된 기본 값을 정의한 파일
  - /etc/group: 그룹에 대한 정보가 저장된 파일
  - /etc/gshadow: 그룹 암호가 저장된 파일

1 – 사용자 계정 관련 파일 알아보기

- 사용자 계정과 관련된 파일
  - /etc/passwd 파일 세부 설명
    - 사용자 계정은 /etc/passwd, 사용자 암호는 /etc/shadow에 저장한다
    - 사용자 계정을 추가하면 /etc/passwd에 기록이 되고, 인증을 처리할 때 /etc/passwd를 보고 해결한다
      - **tail /etc/passwd**
        adminuser:x:1000:1000:adminuser,,,:/home/adminuser:/bin/bash
        로그인ID :x:UID :GID :설명 :홈디렉터리 :로그인 쉘
    - ls –l /etc/passwd를 하면 누구나 read할 접근 권한이 있다
      - -**r**w-**r**--**r**-- 1 root root 2168 6월 5 09:22 /etc/passwd

1 – 사용자 계정 관련 파일 알아보기

- 사용자 계정과 관련된 파일
  - /etc/passwd 세부 설명
    - 로그인 ID
      - 최대 32자까지 지원 / 중복되는 이름 사용 못함
    - X: 암호 저장하는 곳이었는데 보안상 이유로 암호는 /etc/shadow에 저장
    - UID
      - 사용자 계정을 내부 시스템에서는 번호로 관리
      - 로그인 ID가 다르더라도 UID가 같으면 동일한 사용자이다 (jesuswithme의 UID가 0이면 root 계정 역할)
      - 일반 사용자 계정: 1000부터 할당
      - 시스템 사용자 계정: 0~999, 65534
      - **head /etc/passwd**를 하면 0~9까지 할당된 시스템 사용자 계정 확인 가능하고 root 계정은 UID가 0번이다

1 – 사용자 계정 관련 파일 알아보기

- 사용자 계정과 관련된 파일
  - /etc/passwd 세부 설명
    - GID
      - 그룹 계정에 부여된 고유한 번호로서 사용자의 기본 그룹이고, 사용자를 생성할 때 만들어진다
      - 사용자 계정 생성할 때 소속 그룹을 특별히 지정하지 않으면 로그인ID와 동일한 이름으로 그룹 이름을 생성하여 기본 그룹으로 소속시킨다
      - 리눅스 사용자는 무조건 하나 이상의 그룹에 소속되어 있어야 한다
      - 리눅스 시스템에 등록된 그룹을 모두 확인하려면 **cat /etc/group**으로 알 수 있다
    - 설명
      - 사용자의 본명이나 부서명, 연락처 등이 기록된다
      - **adduser peace**로 사용자 계정을 생성하면 이러한 정보를 쉽게 입력할 수 있다
        tail /etc/passwd | grep peace
        peace:x:1004:1004:Pyeong Hwa Lee,402,010-3088-1234,070-8654-1234,Students:/home peace:/bin/bash

1 – 사용자 계정 관련 파일 알아보기

- 사용자 계정과 관련된 파일
  - /etc/passwd 세부 설명
    - 홈 디렉터리
      - 해당 사용자만 접근할 수 있는 장소이고, 사용자가 로그인하면 자동으로 접근하는 위치이다
      - 사용자는 보통 이곳에 디렉터리와 파일을 만들어서 저장한다
      - 어느 위치에서는 자신의 홈 디렉터리로 이동하려면 **cd ~**또는 **cd**를 입력하면 된다
      - 로그인 사용자가 adminuser라고 한다면 일반적으로 홈디렉터리 위치는 /home/adminuser이다
      - 개별 홈페이지를 배부할 때 일반적으로 이 위치를 홈페이지 root directory로 할당해준다
    - 로그인 쉘
      - 사용자가 기본적으로 사용하는 Shell이다.
      - 보통 Bash(Bourne-again shell)을 기본으로 사용하고 있다

1 – 사용자 계정 관련 파일 알아보기

- 사용자 계정과 관련된 파일
  - /etc/shadow 파일 세부 설명
    - 보안 때문에 암호를 이 파일에 별도로 관리한다
    - /etc/passwd를 누구나 읽을 수 있지만 /etc/shadow는 root만 읽을 수 있다
      - **ls -l /etc/shadow**
        -rw-r----- 1 root shadow 1613 6월 5 09:21 /etc/shadow
      - **cat /etc/shadow**
        cat: /etc/shadow: Permission denied
    - peace:6hrj0diwv$GsCDlPAN6ww2kgiC7ePBIPhROE0c7dqyuW1xJC.31IVMFHSdPGxe85DYl2suP1X5FERbqPlOjzzjle35z9oO00:16591:0:99999:7:::
      - **로그인 ID:암호:최종변경일:MIN:MAX:WARNING:INACTIVE:EXPIRE:FLAG**
      - 최종 변경일의 기준은 1970년 1월1일이다
      - MIN: 3이면 암호를 변경한 후 3일 동안은 암호를 변경할 수 없다. 0은 언제든지 변경 가능
      - MAX: 30이면 30일이 지나면 무조건 암호를 변경해야 한다
      - WARNING: 7이면 암호 만료 7일 전에 암호 바꾸라는 메시지를 보낸다
      - INACTIVE: 3이면 암호가 만료된 이후에도 3일 동안은 로그인 가능하고 3일 이내에 꼭 암호를 변경해야 한다. 변경하지 않으면 계정이 잠겨서 사용 못한다
      - EXPIRE: 사용자 계정이 만료되는 날짜로서 이 후에는 이 계정을 사용 못함

1 – 사용자 계정 관련 파일 알아보기

- 사용자 계정과 관련된 파일
  - /etc/login.defs 파일 세부 설명
    - 사용자 계정의 설정과 관련된 기본 값을 정의한 파일이다
    - **more /etc/login.defs**를 실행하여 기본 설정 내용을 보고, 필요하면 수정할 수 있다. 그 다음부터는 이 설정에 따라 사용자 계정이 생성된다

1 – 사용자 계정 관련 파일 알아보기

- 사용자 계정과 관련된 파일
  - /etc/group 파일 세부 설명
    - 시스템이 사용하는 모든 그룹 정보가 저장되어 있다
    - 사용자 계정은 하나 이상의 그룹에 소속되어 있으며, /etc/passwd의 GID 항목에 지정된 그룹이 사용자가 소속된 기본 그룹이다.
      - tail /etc/passwd
        jesuswithme:x:1003:1003::/home/jesuswithme:
      - Jesuswithme의 기본 그룹의 ID는 1003이다.
      - 1003이라는 GID를 갖는 그룹을 찾으려면
        cat /etc/group | grep 1003
        jesuswithme:x:1003:
      - 또는 jesuswithme의 기본 그룹 및 소속된 2차 그룹을 확인하려면
        id jesuswithme
        uid=1003(jesuswithme) gid=1003(jesuswithme) groups=1003(jesuswithme)

1 – 사용자 계정 관련 파일 알아보기

- 사용자 계정과 관련된 파일
  - /etc/group 파일 세부 설명
    - 사용자가 소속된 2차 그룹은 /etc/group에서 확인한다
      - tail /etc/group
        sambashare:x:125:adminuser
        그룹이름:암호:GID:그룹구성원
      - 그룹 이름
      - 암호: 그룹에 부여된 암호. 그룹은 /etc/gshadow에서 별도로 관리한다. 그룹 암호는 **newgrp** 명령으로 자신이 속해있지 않는 그룹으로 전환 때 필요하다
      - GID: 그룹을 식별하는 번호
      - 그룹 구성원: 이 그룹에 소속된 모든 사람을 보여준다. 사용자 계정은 comma로 구분. 이 사용자(adminuser)들의 2차 그룹이 바로 이 그룹(sambashare)이 된다

1 – 사용자 계정 관련 파일 알아보기

- 사용자 계정과 관련된 파일
  - /etc/gshadow 파일 세부 설명
    - 그룹의 암호가 저장된 파일이다
    - cat /etc/gshadow
      - **adm:*::syslog,adminuser**
        그룹이름:암호:관리자:그룹 구성원
      - 관리자: 그룹의 암호나 구성원을 변경할 수 있는 사용자 계정
      - 그룹 구성원: 그룹에 소속된 구성원이다

2 – 사용자 계정 생성, 수정, 삭제하기

- 사용자 계정 생성하기: **useradd**
  - 사용자 계정 생성하는 명령어
    - whereis useradd
    - ls /usr/sbin
    - 거의 모든 명령어가 /usr/sbin에 있으니 혹시 명령어들이 기억나지 않으면 여기서 찾아본다

2 – 사용자 계정 생성, 수정, 삭제하기

- 사용자 계정 생성하기: **useradd**
  - 옵션 없이 사용자 계정 생성하기
    - <Ubuntu>
      useradd user2
      passwd user2
      ls /home
      adminuser jesuswithme peace yslee (user2에 대한 홈디렉터리가 없다)
    - <CentOS>
      useradd user2
      passwd user2
      ls /home
      adminuser jesuswithme lost+found user2 (user2에 대한 홈디렉터리가 있다)

2 – 사용자 계정 생성, 수정, 삭제하기

- 사용자 계정 생성하기: **useradd**
  - 사용자 계정 생성시 기본적으로 적용되는 기본 값 확인: **-D 옵션**
    - <Ubuntu>
      useradd –D
      GROUP=100
      HOME=/home
      INACTIVE=-1
      EXPIRE=
      SHELL=/bin/sh
      SKEL=/etc/skel
      CREATE_MAIL_SPOOL=no
    - <CentOS>
      useradd –D
      GROUP=100
      HOME=/home
      INACTIVE=-1
      EXPIRE=
      SHELL=/bin/bash
      SKEL=/etc/skel
      CREATE_MAIL_SPOOL=yes

2 – 사용자 계정 생성, 수정, 삭제하기

- 사용자 계정 생성하기: **useradd**
  - 사용자 계정 생성시 기본적으로 적용되는 기본 값 확인: **-D 옵션**
    - -D 옵션으로 만들어진 이 값은 /etc/default/useradd 파일에 저장되어 있다
    - 이 내용을 수정할 때는 파일을 직접 변경하면 된다
  - /etc/skel 디렉터리 사용 목적
    - 사용자 계정을 생성할 때 Home Directory를 지정할 수 있다. 이 때 **Home Directory에 공통으로 들어 갈 파일을 /etc/skel에 넣어 두면 자동으로 복사된다**
    - /etc/skel 위치에 있는 파일 확인해 보면
      ls -a /etc/skel
      . .. .bash_logout .bashrc .profile examples.desktop
    - /etc/skel에 message.txt 파일을 복사한 후 홈 디렉터리를 갖는 사용자 계정을 생성해 본다
    - **touch /etc/skel/message.txt**
      useradd -m -d /home/localuser3 localuser3
      passwd localuser3
      ls -la /home/localuser3
      -rw-r--r-- 1 localuser3 localuser3 0 6월 5 20:59 message.txt

2 – 사용자 계정 생성, 수정, 삭제하기

- 사용자 계정 생성하기: **useradd**
  - 여러 개의 옵션을 사용하여 사용자 계정 생성
    - **useradd user3 -m -d /home/user3 -u 2000 -g 1000 -G 3**
      passwd user3
    - **cat /etc/passwd | grep user3**
      user3:x:2000:1000::/home/user3:
    - **cat /etc/group | grep user3**
      sys:x:3:user3

2 – 사용자 계정 생성, 수정, 삭제하기

- 사용자 계정 수정하기: **usermod**
  - 기존에 존재하는 사용자 계정의 UID,GID, 홈디렉터리, 기본 쉘, 로그인 ID, 암호 관련 정보를 수정한다

  - 현재 시스템이 사용하고 있는 쉘을 확인하기
    - **cat /etc/shells**
    - **chsh –l** (##CentOS만)

2 – 사용자 계정 생성, 수정, 삭제하기

- 사용자 계정 수정하기: **usermod**
  - UID 변경하기: **-u 옵션**
    - cat /etc/passwd | grep user3
      user3:x:504:504::/home/user3:/bin/bash
      usermod -u 1003 user3
      cat /etc/passwd | grep user3
      user3:x:1003:504::/home/user3:/bin/bash
  - UID 변경 및 중복하기: **-u –o 옵션**
    - User3을 User2와 동일한 계정으로 변경하는 것
    - **id user2**
      uid=502(user2) gid=502(user2) groups=502(user2)
    - **id user3**
      uid=1003(user3) gid=504(user3) groups=504(user3)
    - **usermod -u 502 -o user3**
      cat /etc/passwd | grep 502
      user2:x:502:502::/home/user2:/bin/bash
      user3:x:502:504::/home/user3:/bin/bash

2 – 사용자 계정 생성, 수정, 삭제하기

- 사용자 계정 수정하기: **usermod**
  - 홈 디렉터리 변경하기: **-d 옵션**
    - **mkdir /home/user33**
      usermod -d /home/user33 user3
      cat /etc/passwd | grep user3
      user3:x:502:504::/home/user33:/bin/bash
  - 로그인 ID 변경하기: **-l 옵션**
    - 로그인 ID를 변경할 때는 Home Directory도 변경하는 것이 좋다
    - **useradd user4**
      passwd user4
      mkdir -p /home/user4
      usermod -d /home/user4 -l user44 user4
      cat /etc/passwd | grep user44
      user44:x:504:505::/home/user4:/bin/bash

2 – 사용자 계정 생성, 수정, 삭제하기

- 사용자 계정 수정하기: **usermod**
  - 사용자 계정의 Password Aging 확인하기: **chage –l** 로그인ID
    - **chage -l user3**
      Last password change : Jun 05, 2015
      Password expires : never
      Password inactive : never
      Account expires : never
      Minimum number of days between password change : 0
      Maximum number of days between password change : 99999
      Number of days of warning before password expires : 7
  - 암호 기간(Password Aging) 변경하기: **chage 옵션 로그인ID**
    - chage -m 2 -M 100 -W 5 -I 10 -E 2015-06-30 user3
      chage -l user3
      Last password change : Jun 05, 2015
      Password expires : Sep 13, 2015
      Password inactive : Sep 23, 2015
      Account expires : Jun 30, 2015
      Minimum number of days between password change : 2
      Maximum number of days between password change : 100
      Number of days of warning before password expires : 5

2 – 사용자 계정 생성, 수정, 삭제하기

- 사용자 계정 삭제하기: **userdel**
  - 사용자 계정을 삭제할 때는 홈 디렉터리와 함께 삭제할 것인지 결정한다
  - -r 옵션을 사용하지 않으면 사용자 계정만 삭제된다

  - 사용자 계정만 삭제하기
    - **userdel user3**
  - 사용자 계정과 홈 디렉터리를 함께 삭제하기: -r 옵션
    - **cat /etc/passwd | grep user44**
      user44:x:504:505::/home/user4:/bin/bash
      userdel -r user44
      ls -la /home/user4
      ls: cannot access /home/user4: 그런 파일이나 디렉터리가 없습니다

2 – 사용자 계정 생성, 수정, 삭제하기

- 사용자 계정 삭제하기: **userdel**
  - 현재 접속하고 있는 사용자 계정 삭제하기: **-f 옵션**
    - Console-1에서 User2로 192.168.219.125에 접속
      hostname
      linux200
      ssh user2@192.168.219.125
      hostname
      centos.webtime.local
    - Console-2에서 현재 로그온한 User2 계정과 홈디렉터리를 삭제
      userdel -r user2
      userdel: user user2 is currently used by process 3174
      userdel -rf user2
      userdel: user user2 is currently used by process 3174
      userdel -f user2
      userdel: 'user2' 사용자가 없습니다
      cat /etc/passwd (##user2 계정이 없다)
      ls –la /home (##/home/user2라는 디렉터리가 없다)

2 – 사용자 계정 생성, 수정, 삭제하기

- 사용자 계정 삭제하기: **userdel**
  - 홈 디렉터리 뿐 아니라 사용자가 소유한 파일도 모두 삭제하기
    - User1 사용자의 UID가 503인 경우
      id user1 (##user1의 UID 확인)
      userdel –rf user1 (##접속중인 user1의 계정과 홈디렉터리까지 삭제)
      find / -user 503 –exec rm –rf {} \;
      (##UID 503이 소유주인 모든 파일 및 디렉터리를 찾아서 삭제하기)

3 – 사용자 정보 관리

- UID(RUID)와 EUID의 관계
  - UID: 로그인 한 사용자의 ID
  - 명령을 실행한 ID: EUID

  - UID 확인하는 명령어(접속할 때 사용한 로그인 ID)
    - **who am I** (=who –m)
  - EUID 확인하는 명령어(명령어를 실행하고 있는 ID / su를 했을 때 ID)
    - **whoami**
    - **id**

  ** who am i와 whoami는 다르다는 것에 유의한다

3 – 사용자 정보 관리

- 사용자 로그인 정보 확인하기: **who, w, last**
  - 사용자 이름, 사용자가 접속한 단말기 번호, 로그인한 시간, IP 주소
    who
    who -H
  - 로그인한 사용자의 수와 계정 이름 확인
    who -q
  - 컴퓨터가 최근에 부팅한 시간
    who -b
  - 어떤 run level로 부팅했는지 확인하기(runlevel 5는 윈도로 부팅)
    who -r

3 – 사용자 정보 관리

- 사용자 로그인 정보 확인하기: **who, w, last**
  - 로그인 사용자 정보 외에 사용자가 현재 무엇을 하고 있는지 실행중인 작업을 알려준다

    w
    w 사용자

- 사용자 로그인 정보 확인하기: **who, w, last**
  - 사용자 이름과 로그인 시간, 로그아웃한 시간, 터미널 번호나 IP 주소, 시스템이 종료한 시간, 다시 시작한 시간, root 사용자가 로그인한 시간

    last

3 – 사용자 정보 관리

- 특정한 사용자가 어느 그룹에 소속되었는지 확인하기: **groups**
  - 현재 로그인 한 사용자가 소속된 그룹 확인
    groups
  - 특정한 사용자가 소속된 그룹 확인
    groups adminuser

3 – 사용자 정보 관리

- passwd 명령 활용하기
  - 자신의 암호를 변경한다: passwd
  - 관리 권한이 있는 사용자는 다른 사용자의 암호를 생성한다: passwd 사용자
  - 다른 사용자의 암호를 잠궈서 로그인을 못하게 한다: **-l 옵션(lock)**
    - [root@**centos** adminuser]# **passwd -l user1**
      user1 사용자의 비밀 번호 잠금
      passwd: 성공
      user1:**!!**$6$0Bf4/QKd$Kroa798wdpzI0T285s/GRBs3PsrmO3loYFhig3Ft0yARQSHlc5ahoPDFZ0VSARoXfyLdpZY5FPcuW3FUE4HMx.:16591:0:99999:7:::
    - adminuser@**linux200**:~$ **ssh user1@192.168.219.125**
      user1@192.168.219.125's password:
      Permission denied, please try again.
    - [root@centos adminuser]# cat /etc/shadow | grep user1
  - 잠긴 사용자의 암호를 잠금 해제한다: **-u 옵션(unlock)**
    - [root@**centos** adminuser]# **passwd -u user1**
    - adminuser@**linux200**:~$ ssh user1@192.168.219.125
      user1@192.168.219.125's password:
      Last login: Sat Jun 6 08:37:09 2015 from 192.168.219.104

3 – 사용자 정보 관리

- passwd 명령 활용하기
  - 암호를 삭제한다: **-d 옵션**
    - **passwd -d user2**
      cat /etc/shadow | grep user2
      user2::16592:0:99999:7::: (##user2 다음에 ::으로 처리되어 암호가 없다)
  - 사용자 계정에 암호가 없으면 로컬에서 로그온 하거나 sudo 작업을 할 때 암호를 요구하지 않는다
  - 하지만 원격에서 ssh 접속을 할 때는 암호가 없는 사용자는 로그인을 할 수 없다는데 유의한다

3 – 사용자 정보 관리

- 파일 및 디렉터리의 소유자와 소유그룹 변경: **chown, chgrp**
  - 파일이나 디렉터리를 누군가가 생성하면 생성한 사용자가 그 파일이나 디렉터리의 소유자 및 소유 그룹이 된다
    - -rw-r--r--. 1 **user1** adminuser 158 2015-06-06 10:08 hosts
      drwxrwxr-x. 2 **adminuser** group1 4096 2015-06-06 10:09 temp
      hosts 파일의 소유자는 user1, temp 디렉터리의 소유자는 adminuser
      hosts 파일의 소유그룹은 adminuser1, temp 디렉터리의 소유그룹은 group1
  - **chown**: 파일(hosts)과 디렉터리(temp/)의 **소유자**와 소유그룹을 변경한다
  - **chgrp**: 파일과 디렉터리의 **소유 그룹만**을 변경한다
  - root 계정만 chown, chgrp를 사용할 수 있으며, 사용할 때 하위 디렉터리까지 변경할 때는 –R 옵션 사용

3 – 사용자 정보 관리

- 파일 및 디렉터리의 소유자와 소유그룹 변경: **chown, chgrp**
  - **파일**에 대한 **소유자만** 변경
    - [root@centos adminuser]# **chown user2 hosts**
      [root@centos adminuser]# **ls -l hosts**
      -rw-r--r--. 1 user2 adminuser 158 2015-06-06 10:08 hosts
  - **파일**에 대한 **소유자와 소유 그룹을 동시**에 변경
    - [root@centos adminuser]# **chown user1:group1 hosts**
      [root@centos adminuser]# **ls -l hosts**
      -rw-r--r--. 1 user1 group1 158 2015-06-06 10:08 hosts
  - **디렉터리** 및 그 하위 디렉터리와 파일들에 대한 **소유자와 소유 그룹을 동시**에 변경 (chown 명령 사용)
    - [root@centos adminuser]# **ls -l temp/services** (##현재 상태 모습)
      -rw-r--r--. 1 **adminuser adminuser** 641020 2015-06-06 10:09 temp/services
    - [root@centos adminuser]# **chown -R user2:group2 temp** (##강추)
      [root@centos adminuser]# **ls -l temp/services**
      -rw-r--r--. 1 user2 group2 641020 2015-06-06 10:09 **temp/services**
    - [root@centos adminuser]# **ls –l**
      drwxrwxr-x. 2 user2 group2 4096 2015-06-06 10:09 **temp**

3 – 사용자 정보 관리

- 파일 및 디렉터리의 소유자와 소유그룹 변경: **chown, chgrp**
  - **디렉터리**의 **소유 그룹만** 변경 (chgrp 사용)
    - [root@centos adminuser]# **ls –l** (##현재 상태 모습)
      drwxrwxr-x. 2 user2 **group2** 4096 2015-06-06 10:09 **temp**
    - [root@centos adminuser]# **chgrp adminuser temp/**
      [root@centos adminuser]# **ls –l**
      drwxrwxr-x. 2 user2 adminuser 4096 2015-06-06 10:09 temp
  - **디렉터리** 및 그 하위 디렉터리와 파일들에 대한 **소유 그룹만** 변경 (chgrp **-R** 사용)
    - [root@centos adminuser]# **ls -l temp/services** (##현재 상태 모습)
      -rw-r--r--. 1 user2 **group2** 641020 2015-06-06 10:09 **temp/services**
    - [root@centos adminuser]# **chgrp -R root temp**
      [root@centos adminuser]# **ls –l**
      drwxrwxr-x. 2 user2 root 4096 2015-06-06 10:09 temp
    - [root@centos adminuser]# **ls -l temp/services**
      -rw-r--r--. 1 user2 root 641020 2015-06-06 10:09 temp/services

3 – 사용자 정보 관리

- 파일 및 디렉터리의 소유자와 소유그룹 변경: **chown, chgrp**
  - /home/adminuser 하위 디렉터리와 파일들에 대한 **소유자와 소유그룹을 동시**에 adminuser로 변경 (chown –R 명령 사용)
    - 특정한 사용자의 홈디렉터리의 파일들을 소유자 및 소유그룹을 초기 설정으로 환원하는 것이다
    - [root@centos adminuser]# **chown -R adminuser:adminuser /home/adminuser**
      [root@centos adminuser]# **ls –l**
      -rw-r--r--. 1 **adminuser adminuser** 158 2015-06-06 10:08 hosts
      drwxrwxr-x. 2 **adminuser adminuser** 4096 2015-06-06 10:09 temp
    - [root@centos adminuser]# **ls -l temp/**
      -rw-r--r--. 1 **adminuser adminuser** 641020 2015-06-06 10:09 services
  - 이렇게 작업이 끝나면 /home/adminuser에는 adminuser가 접속하여 자기가 만든 파일에 대한 소유권이 생겨서 원하는데로 작업할 수 있게 된다

2 – 그룹 계정 관리

- 새로운 그룹 생성하기
- 그룹 정보 수정하기
- 그룹 삭제하기
- 그룹 암호 설정하고 사용하기

1 – 새로운 그룹 생성하기

- 그룹을 사용하는 이유
  - 영업부서 직원 30명이 사용할 디렉터리가 3개(SalesDir2, SalesDir2, SalesDir3)가 있고, 기술부서 20명이 사용할 디렉터리가 2개(EngDir1, EngDir2)가 있다
  - 각 디렉터리 마다 Permission을 부여해야만 사용자가 접근할 수 있다
  - 각 디렉터리마다 30명씩, 20명씩 할당해주는 것은 힘든 일이고 지루한 일이고 신경이 많이 쓰이는 작업이다
  - 만약 영업부서에 새로운 직원이 들어 오면 또 3개 디렉터리에 접근할 수 있도록 작업을 해야 하는 번거로움이 있다
  - 이럴 때 Group을 사용하여 Permission을 할당하고, 사용자들을 Group에 포함시켜두면 편리하다
  - 만약 기술부서 직원이 영업부서로 부서 전환이 되더라도 해당 기술부서 직원 계정을 기술부서에서 영업부서 그룹으로 이동만 시켜주면 쉽게 끝난다

1 – 새로운 그룹 생성하기

- 아무 옵션 없이 그룹 생성하기: **groupadd 그룹명**
  - 옵션 없이 생성하면 GID는 가장 마지막 번호 다음 번호를 할당한다
    - **groupadd testgroup1**
      cat /etc/group | grep testgroup1
      testgroup1:x:511:
    - **groupadd testgroup2**
      cat /etc/group | grep testgroup2
      testgroup1:x:512:
- 시스템 그룹 생성하기: **groupadd –r 그룹명**
  - 0~499번의 GID를 할당하며, 지금까지 할당되지 않은 번호 중에서 가장 높은 번호를 자동으로 할당한다
    - **groupadd -r systemgroup1**
      groupadd -r systemgroup2
      cat /etc/group | grep systemgroup*
      systemgroup1:x:493:
      systemgroup2:x:492:

1 – 새로운 그룹 생성하기

- GID를 지정하여 그룹 생성하기: **groupadd –g 번호 그룹명**
  - Testgroup1000, testgroup1001 생성하기
    - **groupadd -g 1000 testgroup1000**
      groupadd -g 1000 testgroup1001
    - **cat /etc/group | grep testgroup***
      testgroup1:x:511:
      testgroup2:x:512:
      testgroup1000:x:1000:
      testgroup1001:x:1001:

2 – 그룹 정보 수정하기

- 기존의 그룹에 대한 정보를 수정: **groupmod 옵션 그룹명**
  - GID 바꾸기: **-g 옵션**
    - **groupmod -g 1002 testgroup1**
      groupmod -g 1003 testgroup2
      cat /etc/group | grep testgroup*
      testgroup1:x:1002:
      testgroup2:x:1003:
  - 그룹 이름 변경하기: groupmod **–n 새로운이름 기존이름**
    - **groupmod -n group3 testgroup1**
      groupmod –n group4 testgroup2
      cat /etc/group | grep group*
      group1:x:509:
      group2:x:510:
      group3:x:1002:
      group4:x:1003:

2 – 그룹 정보 수정하기

- 그룹 삭제하기: **groupdel 그룹명**
  - Testgroup1000, testgroup1001 삭제하기
    - **groupdel testgroup1000**
      groupdel testgroup1001
      cat /etc/group | grep testgroup*

2 – 그룹 정보 수정하기

- 그룹 암호 설정하고 사용하기: **gpasswd 옵션 그룹명**
  - 그룹의 암호를 삭제하고 **그룹에 구성원을 추가하거나 삭제한다**

  - 그룹(group1)에 구성원(user1)을 추가하기: **-a 옵션**
    - **id user1**
      uid=506(user1) gid=507(user1) groups=507(user1)
    - **gpasswd -a user1 group1**
      Adding user user1 to group group1
    - **id user1**
      uid=506(user1) gid=507(user1) groups=507(user1),**509(group1)**

2 – 그룹 정보 수정하기

- 그룹 암호 설정하고 사용하기: **gpasswd 옵션 그룹명**
  - 그룹(group1)의 구성원(user1)을 삭제하기: **-d 옵션**
    - Group1에 포함된 사용자 확인하기
      cat /etc/group | grep group1
      group1:x:509:user1,user2
    - 사용자 user1이 소속된 그룹 이름 확인하기
      groups user1
      user1 : user1 group1 group2
    - Group1에 소속된 user1을 제거하기
      gpasswd -d user1 group1
      Removing user user1 from group group1
    - **cat /etc/group | grep group1**
      group1:x:509:user2
    - **groups user1**
      user1 : user1 group2
  - 그룹(group1)의 암호 재설정하기: **gpasswd 그룹명**
    - Group1의 현재 암호 설정 여부 확인하기
      cat /etc/gshadow
    - Group1의 암호 설정하기
      gpasswd group1

2 – 그룹 정보 수정하기

- **기본그룹** 변경하기: **newgrp 그룹명**
  - 사용자는 1차(기본) 그룹과 2차 그룹에 가입된다
  - 사용자는 자신이 소속될 1차(기본) 그룹을 **스스로 변경한다**
    - **Root 계정이** newgrp 명령을 내려서 다른 사용자 계정의 소속 그룹을 **변경하는 것이 아니다**
  - 관리자(root)가 일반 사용자의 1차 그룹을 변경할 때는 암호가 필요 없다
    - **usermod -g salesgroup imsiuser**
  - 사용자의 **2차 그룹에도 포함되지 않는 그룹 이름을** 기본 그룹으로 설정할 때 **그룹 암호가 사용된다**
    - **su user1**
      id
      uid=506(user1) gid=507(user1) groups=507(user1),506(jesuswithme),510(group2)
    - **newgrp group2**
      id
      uid=506(user1) gid=510(group2) groups=510(group2),506(jesuswithme),507(user1)
    - **newgrp group1** (##2차 그룹에 없는 그룹이 group1이다)
      암호:
      id

2 – 그룹 정보 수정하기

- 그룹 암호 삭제하기: **gpasswd -r 그룹명**
  - 그룹에 대한 암호 설정
    - **gpasswd group1**
      cat /etc/gshadow | grep group1
      group1:6yH1cvqDy7G//7$4pn5FX5vbJyXZvhHF8sbhmsCbKP48ulIHy4osW4DUOLUONxHtPGuwCkFo.8NhQ1Ti11AqyxaL558AV6ojXXVA0::user2
  - 그룹 암호 제거하기
    - **gpasswd -r group1**
      cat /etc/gshadow | grep group1
      group1:::user2

3 – 관리 권한 위임하기

- 관리 권한 위임 개요
- 관리 권한이 있는 사람만 sudo 명령 실행
- /etc/sudoers 파일 수정하기

3 – 관리 권한 위임하기

- 관리 권한 위임 개요
  - Root 계정이 다른 사용자 및 그룹 구성원들에게 관리 권한을 위임해 주고자 할 때 **/etc/sudoers** 파일을 수정하면 된다
  - 관리 권한을 위임 받은 사용자는 해당 관리 작업을 할 때만 반드시 **[sudo 명령어]**으로 사용하여 권한을 상승시켜 작업을 할 수 있게 된다
  - sudo는 substitute user do 또는 super user do 를 말한다
  - **sudo**와 같은 개념이 윈도우에는 **UAC(User Account Control)** 기능이다
  - 관리 작업 권한을 위임 받지 못한 일반 사용자 계정은 sudo를 사용할 수 없다
  - sudo를 사용할 때는 반드시 root 계정이 아닌 사용자 계정의 암호를 입력
  - sudo 명령어를 사용하여 암호를 입력하면 5분 동안은 암호가 cache가 되기 때문에 추가적인 sudo 명령어를 사용할 때 암호를 다시 입력할 필요가 없다.
  - 만약 보안 수준을 높이기 위해서 password cache를 아예 없애고 싶으면, 즉, sudo 명령어를 입력할 때 마다 암호를 입력하게 하려면 sudo -k를 입력하면 된다
  - 로그인 계정을 변경하여 다른 계정으로 작업할 때 **su** 명령어를 사용한다
  - **su**와 동일한 것이 윈도우의 **runas** 명령어이다

3 – 관리 권한 위임하기

- 관리 권한이 있는 사람만 sudo 명령 실행
  - Ubuntu에서 설치할 때 생성한 계정인 adminuser로 로그인하여 사용자 계정을 생성할 수 있다
  - 그 이유는 Account Type이 Administrator이기 때문에 관리 권한을 수행할 수 있다.(sudo 사용 가능)
  - 하지만 CentOS에서는 설치할 때는 Root 계정에 대한 암호만 입력하였고, 설치 끝난 후에 추가적으로 adminuser를 생성하였다
  - 이 계정은 관리 권한이 없다. 그래서 기본적으로 sudo를 사용할 수 없다
  - CentOS에서 사용하는 adminuser에서 관리 권한을 위임하여 sudo를 사용하려면 /etc/sudoers 파일을 편집해야 한다
  - Ubutun에서도 CentOS에서도 Root를 제외한 다른 사용자가 관리 작업을 하려면 반드시 관리 권한이 위임되어 있어야 한다

3 – 관리 권한 위임하기

- /etc/sudoers 파일 수정하기
  - /etc/sudoers 파일에서 사용자 및 그룹 표현하는 방법
    - 로컬 사용자: **사용자이름**
      로컬 그룹: **%그룹이름**
      AD 도메인 사용자: **PEACEFUL\\사용자이름**
      AD 도메인 그룹: **%PEACEFUL\\그룹이름**
  - 특정한 사용자 및 그룹들에게 root 권한(모든 권한)을 위임하기
    - **root ALL=(ALL) ALL**
      admin1 ALL=(ALL) ALL
      %admins ALL=(ALL) ALL
      %PEACEFUL\\linuxadmins ALL=(ALL) ALL
      PEACEFUL\\linuxuser1 ALL=(ALL) ALL
  - User1에게 useradd, usermod 명령 권한 위임하기
    - **user1 ALL=/usr/sbin/useradd, /usr/sbin/usermod**
  - 파일 이름만 입력하지 않고 반드시 파일의 Full Path를 입력해야 한다
  - 위임 받은 권한을 실행할 때는 **sudo useradd imsiuser**로 입력한다

3 – 관리 권한 위임하기

- /etc/sudoers 파일 수정하기
  - User2에게는 gedit, User3에게는 fdisk 권한 위임하기
    - **user2 ALL=/usr/bin/gedit**
    - **user3 ALL=/sbin/fdisk**

    - su user2를 하여 **sudo gedit**를 실행해본다 (성공)
    - **sudo fdisk –l**을 실행해본다 (실패)
    - Su user3를 하여 **sudo fdisk –l**을 실행해 본다 (성공)

3 – 관리 권한 위임하기

- /etc/sudoers 파일 수정하기
  - Alias 및 Wildcard 를 이용하여 그룹에 관리 위임하기
    - useradd, passwd 명령어 사용, userdel 명령어 사용 못하도록 설정
      Cmnd_Alias USERADMIN=/usr/bin/passwd,/usr/sbin/user*, !/usr/sbin/userdel
      %adminusers ALL=USERADMIN
    - 암호 설정 가능, 사용자 계정 생성 및 삭제 등등의 모든 사용자 관리 가능(/etc/sbin/에 있는 모든 명령어 사용; useradd, userdel), /usr/bin/에 있는 gedit, nano 명령어 사용 가능
      Cmnd_Alias MANAGESYSTEM=/usr/sbin/*,/usr/bin/*
      %manageusers ALL=MANAGESYSTEM
    - Adminusers, manageusers 그룹을 생성한 후 사용자 계정을 추가해야 한다
      - **useradd –m –d /home/admin1 admin1**
        passwd admin1
        useradd –m –d /home/admin2 admin2
        passwd admin2
      - **groupadd adminusers**
      - **gpasswd –a admin1 adminusers**
        gpasswd –a admin2 adminusers