2013년 01회
132. 다음 중에서 UNIX 운영체제에 관한 설명으로 옳지 않은 것은?
① 유닉스 운영체제는 커널(Kernel), 셸(Shell), 디렉터리(파일 시스템)으로 구성된다.
② 파일 시스템은 환경설정파일을 담고 있는 /etc 디렉터리가 있고, 특수 파일 및 장치에 대한 것은 /dev에 있다.
③ 셸에는 C shell, Bourne shell, Korn shell 등이 있다.
④ OLE(Object Linking Embedded)를 사용한다.

| 정답 | 4 |
|---|---|

■ OLE(object linking and embedding)
- 윈도우에서, 데이터와 데이터를 연결하는 방법을 말한다. 연결된 데이터는 수정될 때 함께 수정되어 저장된다.

**unix기본 사용법 user/group/other p,564**

2018년 12회
133. 다음 중 UNIX 파일 시스템의 무결성 보장을 위해 점검해야 할 사항이 아닌 것은?
① 파일의 소유자, 소유그룹 등의 변경 여부 점검
② 파일의 크기 변경 점검
③ 시스템의 이중화여부를 확인한다.
④ 파일의 symbolic link의 수 점검

| 정답 | 3 |
|---|---|

무결성 보장이란 정보가 의도하지 않은 방법으로 변경되거나 파괴되지 않도록 보장하는 것을 말한다.

2018년 12회
134. 다음 중 무결성을 점검하는 방법과 거리가 먼 것은?
① 소유자 그룹 권한을 확인한다.
② 파일의 크기를 확인한다.
③ 서비스의 흐름, 교환, 저장 등이 끊임없이 제공될 수 있는지를 확인한다.
④ 파일의 심볼릭 링크 수를 확인한다.

| 정답 | 3 |
|---|---|

2013년 01회

135. UNIX 파일시스템 설명으로 옳지 않은 것은?

① 파일의 권한은 소유자, 그룹, 일반 사용자로 구성되어 있다.

② 파일의 변경 또는 삭제는 소유자만 가능하다.

③ 유닉스 파일 시스템은 NFS(Network File System)를 통해서 파일을 공유할 수 있다.

④ 파일 시스템은 디렉터리와 파일로 구성되며, 계층화 된 트리구조를 가진다.

| 정답 | 2 |
|---|---|

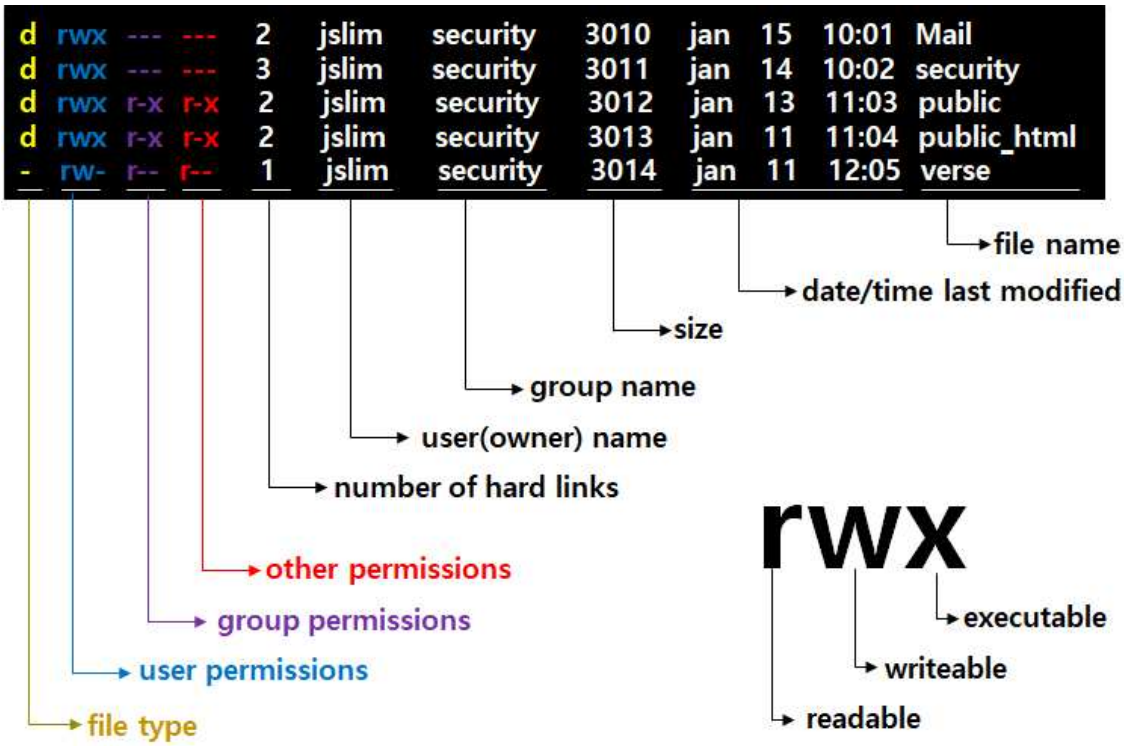


그림 24 디렉터리 정보 출력 예

136. 다음의 명령어를 실행한 파일의 접근 권한으로 옳은 것은?

```
chmod 751 test.c
```

① -rwxr-x - -x　　② -rwxrw- --x
③ -rwxr-x ---　　④ -rw-r-- ---

정답 1

137. Unix 운영체제에서 파일에 대한 권한을 모두 허용(-rwxrwxrwx)하는 모드 (명령어)는 무엇인가?

① chmod 777　　② chmod a-rwx
③ chmod 666　　④ chmod ug+rw

정답 1

2016년 07회

138. UNIX 시스템에서 다음의 chmod 명령어 실행 후의 파일 test1의 허가비트(8진법 표현)는?

```
$ ls -l test1
-rw-r--r-- 1 root user 2320 Jan 1 12:00 test1
$ chmod o-r test1
$ chmod g-r test1
```

① 644　② 244
③ 600　④ 640

정답 3

test1의 퍼미션은 user(4+2+0), group(4+0+0), other(4+0+0) 으로 644 이다. 그리고 chmod 로 o(other)와 g(group)의 r(읽기) 권한을 - (삭제) 하였으므로 퍼미션은 600 이된다.

2018년 12회

139. 다음 중 Unix 시스템에서 secure.txt 파일의 소유자에게는 읽기와 실행권한을 부여하고 다른 사용자에게는 읽기 권한을 제거하라는 권한 변경 명령으로 알맞은 것은?

① #chmod 306 secure.txt
② #chmod 504 secure.txt
③ #chmod otrx, a-r secure.txt
④ #chmod u=rx, o-r secure.txt

| 정답 | 4 |
|---|---|

+ : 지정된 모드들은 지정된 클래스들에 더한다
- : 지정된 클래스들로부터 지정된 모드들은 지운다
= : 지정된 클래스들을 위해서 지정된 모드들이 정확한 모드들로 만들어지게 된다.

2018년 12회

140. 다음 중 소유자에게 읽기 쓰기 권한을 부여하고, 일반사용자에게 읽기 권한을 제거하는 리눅스 명령은?

① chmod 604
② chmod 504
③ chmod o+rw a-r
④ chmod u=rw o-r

| 정답 | 4 |
|---|---|

2014년 03회

141. 다음은 리눅스 파일권한에 대한 설명이다. 올바르지 못한 것은?

① ls –al명령어로 권한을 자세히 볼 수 있다.
② chmod명령어는 파일, 디렉토리명을 수정할 수 있다.
③ 맨앞에 문자가'-'이면 파일, 'd'이면 디렉토리, 'l'이면 링크이다.
④ chown 명령어는 파일소유자, 파일소유그룹을 수정 할 수 있다.

| 정답 | 2 |
|---|---|

# 유닉스(솔라리스) 명령어 및 로그 파일

## UNIX 명령어

| 명령어 | 설명 |
|---|---|
| **rlogin** | 로컬 호스트와 remote 호스트를 연결하는 명령어 |
| **ftp** | 파일을 공유하기 위한 명령어 |
| **uname** | 현재 시스템의 정보를 출력하는 명령어 |
| **finger** | **특정 컴퓨터의 사용자 정보를 볼 수 있는 유닉스 명령어** |
| who | 누가, 언제 로그인해 사용하고 있는지 정보 확인 (utmp 로그 내용 확인) |
| chdir | 작업 디렉터리를 변경한다. |
| chgroup | 그룹의 속성을 변경한다. |
| chroot | path가 지정한 곳으로 루트 디렉터리를 바꾼다. |
| **chmod** | **파일과 디렉터리에 접근권한을 변경한다.** 해당 파일의 소유자나 슈퍼유저만 실행가능하다. |
| **chown** | **파일과 디렉터리에 소유자 및 소유 그룹을 변경한다. 오직 슈퍼유저(root)만 실행**이 가능하다. 예) chown [소유자 계정] [file name] |
| chgrp | 파일 및 디렉토리의 소유그룹 변경하는 명령어이다. |
| umask | 파일 및 디렉토리 생성 시 부여되는 기본 권한 변경하는 명령어이다. |
| **last** | **last 명령어는 로그인과 로그아웃 기록을 보여주는 명령어로, /var/adm/wtmpx 파일의 내용을 분석해서 출력한다.** |
| lastcomm | lastcomm 명령은 /var/adm/pacct 의 내용을 참조하여 이전에 실행된 명령들에 대한 정보를 표시한다. |
| lastb | lastb 명령은 /var/log/btmp 로그 파일을 기본값으로 보여주는데 이 부분을 제외하고는 last 명령어와 동일하다. |
| **at** | **수행 시간 지정 명령어** |
| **cat** | 파일을 작성하거나 파일의 내용을 출력하는 명령어 |
| **cron** | 일정 시간마다 시스템에서 자동으로 특정 작업을 실행시키는 데몬 |
| **ps(Process Status)** | **시스템에서 상주하는 프로세스(PID) 정보를 알려준다.**<br>시스템에서 수행 중인 명령어의 TTY 정보를 알려준다.<br>시스템에서 수행 중인 프로세스의 사용자 정보를 알려준다.<br>시스템에서 로딩된 셸 정보를 알려준다. |
| ps -ef \| grep java<br>(java: 프로세스이름) | e 옵션은 모든 프로세스를 표시하는 것이고<br>f 옵션은 프로세스의 정보를 더 많이 보여주도록 하는 옵션이다.<br>ef 옵션은 많은 프로세스가 한 번에 표시되기 때문에 grep 명령어로 원하는 키워드를 가려서 사용한다.<br>즉 ps -ef \| grep java 명령어는 프로세스 이름 중에서 java라는 문자열을 포함하는 프로 |

| | |
|---|---|
| | 세스 정보를 알려준다. |
| SetUID | 일반 유저가 자신의 패스워드를 변경할 수 있도록 SetUID가 설정된 파일은 실행 되는 동안에 잠깐 관리자 권한을 빌려오고, 작업을 마친후엔 다시 권한을 돌려주게 된다. |
| grep | 파일에서 특정 단어나 문자열을 포함하는 행을 찾아 출력한다. |
| whereis | whereis 명령어는 실행 파일의 위치와 함께 소스, 설정 파일, 매뉴얼 페이지를 검색하여 출력한다. |
| which | which 명령은 $PATH 내의 실행 파일의 위치를 알려준다. |
| lsof | lsof는 liSt open files(열려있는 파일 나열)을 뜻하는 명령으로, 수많은 유닉스 계열 운영체제에서 열려있는 모든 파일과, 그 파일들을 열고 있는 프로세스들의 목록을 출력한다. |
| mount | 파일 시스템을 마운트 한다. (장치를 사용하기 위해 루트 디렉터리의 시스템의 하위 디렉터리로 붙이는 작업을 마운트라고 한다.) |
| umount | 파일 시스템을 언마운트 한다. |
| pwd | pwd 명령어는 현재 작업 중인 디렉터리의 절대 경로를 출력한다(Print Working Directory). |
| more | 파일을 화면 단위로 출력한다. |
| ln | 파일 링크를 만든다(명령어는 파일을 실제 경로가 아니라 사용하기 편리한 다른 경로로 접근할 수 있도록 지정한다). |

표 181 UNIX 명령어

* solaris(솔라리스)는 SUN(현재는 Oracle) 사에서 solaris(솔라리스)라는 운영체제를 만들어서 SUN사에서 출시한 서버나 워크스테이션에 기본적으로 장착되는 운영체제이다.

## UNIX 로그파일

| 로그파일 | 설명 |
|---|---|
| history | 각 계정별로 실행한 명령어에 대한 기록을 저장한 파일 |
| **sulog** | **su 명령어 사용 내역을 기록**(su : switch user 사용자 전환) |
| syslog | system에서 발생하는 log 정보로 서비스의 동작과 에러를 확인할 수 있다. |
| **xferlog** | **FTP 파일 전송 내역 기록**<br>Thu Feb 2 16:41:30 2017 1 192.168.10.1 2870 /tmp/12-ftp.bmp b<br>접근날짜와 시간 접속IP 파일SIZE 전송한 파일 Binary(파일종류)<br>o r wish ftp 0 * c 2870 0<br>outgoing real 로그인한id 서비스방법 인증방법 전송상태 성공 |
| **loginlog** | **loginlog는 로그인 실패를 했을 경우에 로그인 실패 정보를 기록한다.**<br>(리눅스에서 5번 이상 로그인 실패 시 로그인 실패정보 기록하는 로그는 **btmp**이다.) |
| lastlog | 최근 로그인 시각(마지막 로그인 시각)을 기록(Linux) |
| **utmp** | **현재 사용자의 정보를 기록,**<br>로그인, 로그아웃 등 현재 시스템 사용자의 계정 정보 |
| **wtmp** | **성공한 로그인, 리부팅한 정보 등을 기록(계정들의 로그인 및 로그아웃에 대한 정보)하는 로그파일이다.** wtmp파일을 분석할 때는 last –w –F –f wtmp >> wtmp.txt |
| btmp | 실패한 로그인 정보를 담고 있는 로그 파일(Linux) |
| pacct | 시스템에 로그인한 모든 사용자가 수행한 프로그램에 대한 정보를 기록 |
| **acct/pacct** | **로그인한 후부터 로그아웃할 때까지 입력한 명령과 시간, 작동된 tty 등에 대한 정보를 기록** |
| secure | telnet, ftp, pop, smpt, ssh 접속에 대한 로그인 인증내역을 기록한다.<br>/var/log/secure 로그는 인터넷 슈퍼데몬인 inetd 데몬에 의해서 생성되고 기록되는 로그 파일이다. |

표 182 UNIX 로그파일

**UNIX 명령어 p,567**

2019년 14회

142. 리눅스 시스템에서 rlogin를 통합 접근을 허용하는 호스트를 설정하는 파일은?

① /etc/hosts.equiv
② /etc/allow
③ /etc/hosts.allow
④ /etc/rlogin.allow

| 정답 | 1 |
|---|---|

rlogin: 로컬 호스트와 remote 호스트를 연결하는 명령어

2015년 06회

143. rlogin 시에 아이디와 패스워드 없이 시스템에 인증할 수 있다. 다음 중 관련된 파일은?

① /etc/hosts.deny ② /etc/hosts.equiv
③ /etc/hosts.allow ④ /etc/host.login

| 정답 | 2 |
|---|---|

■ 패스워드 없이 원격 시스템에 접근하는 방법을 설정할 수 있는 파일
- /etc/hosts.equiv (루트를 제외한 모두)
- $HOME/.rhosts (루트를 포함한 특정 계정)

2015년 05회

144. 다음에서 설명하는 리눅스 명령어는?

| 리눅스 운영체제에서 원격 서버에 접속하기 위한 명령어로, 접속하고자 하는 호스트를 /etc/hosts.equiv 파일에 사전에 등록해 두어야 한다. |
|---|

① telnet
② login
③ rlogin
④ talkd

| 정답 | 3 |
|---|---|

rlogin 명령은 TCP/IP 컴퓨터 네트워크를 경유하여[1] TCP 포트 513를 통해 통신 사용자가 네트워크를 통해 다른 호스트에 로그인할 수 있도록 유닉스와 같은 컴퓨터 운영 체제를위한 소프트웨어 유틸리티이다.

2015년 06회

145. 다음 중 'lastb'라는 명령을 통하여 로그를 살펴볼 수 있는 로그 파일명은?

① utmp ② btmp

③ dmGsg ④ secure

| 정답 | 2 |
|---|---|

- lastb 명령은 /var/log/btmp 로그 파일을 기본값으로 보여주는데 이 부분을 제외하고는 last 명령어와 동일하다.
- btmp는 실패한 로그인 정보를 담고 있는 로그 파일이다.

2013년 02회

146. 다음 로그 중에서 'lastb' 명령을 사용하여 확인해야 할 것은 무엇인가?

① wtmp ② utmp

③ btmp ④ last

| 정답 | 3 |
|---|---|

2019년 14회

147. 다음 중 리눅스 시스템에서 좀비 프로세스를 찾기 위해 사용할 수 있는 명령어로 옳은 것 2가지를 선택하시오.

① ps -ef | grep defunct

② top -b -n 1 | grep defunct

③ ps -ef | grep zombie

④ top -b -n 1 | grep zombie

| 정답 | 3, 4 |
|---|---|

좀비 찾기 : ps -ef | grep defunct 좀비 수 확인 : top -b -n 1 | grep zombie

2019년 14회
148. 유닉스/리눅스 환경에서 로그인 실패 기록을 저장하는 로그파일은?
① xferlog
② wtmp
③ btmp
④ syslog

| 정답 | 3 |
|---|---|

btmp: 실패한 로그인 정보를 담고 있는 로그 파일이다.

2019년 14회
149. 리눅스 환경에서 의심으로운 접근기록이 확인되어 로그인 실패 기록을 살펴보려고 한다. 어떤 로그 파일을 참조하는 것이 가장 적절한가?3
① pacct ② wtmp
③ btmp ④ utmp

| 정답 | 3 |
|---|---|

2018년 12회
150. 리눅스/유닉스 시스템에서 로그를 확인하는 명령어나 로그파일과 가장 거리가 먼 것은?
① wtmp ② history
③ pacct ④ find

| 정답 | 4 |
|---|---|

find는 일부 사용자 지정 기준에 따라 파일을 찾고 사용자 정의 행위를 각 매칭되는 파일에 적용하여 파일 시스템의 하나 이상의 디렉터리 트리를 검색하는 명령 줄 유틸리티이다.

2018년 11회
151. 분석 시 사용될 수 있는 명령어에 대하여 잘못 나열한 것은?
① secure - 사용자 원격접속 정보 - text file - grep
② utmp - 현재 로그인 사용자 정보 - binary file - who
③ pacct - 사용자별 명령 실행 정보 - text file - history
④ wtmp - 최근 로그인 및 접속 호스트 정보 - binary file- last

| 정답 | 3 |
|---|---|

pacct : 로그인한 후부터 로그아웃할 때까지 입력한 명령과 시간, 작동된 tty 등에 대한 정보를 기록한 로그파일

2017년 10회
152. 사용자 로그인과 로그아웃 정보를 누적하여 저장하는 파일은?
① utmp ② wtmp
③ lastlog ④ xferlog

정답 2

- **wtmp 로그파일은** 성공한 로그인, 리부팅한 정보 등을 기록(계정들의 로그인 및 로그아웃에 대한 정보)하는 로그파일이다.
- wtmp파일을 분석할 때는 last –w –F –f wtmp >> wtmp.txt

2017년 10회
153. 로그에 관한 설명으로 옳지 않은 것은?
① wtmp : 사용자들이 로그인, 로그아웃한 정보를 가지고 있다.
② utmp : 시스템에 현재 로그인한 사용자들에 대한 상태정보를 수집한다.
③ pacct : 사용자가 로그인한 후부터 로그아웃하기 까지의 입력한 명령과 시간, 작동된 tty 등에 대한 정보를 수집한다.
④ btmp : syslog 데몬에서 일괄적으로 생성된 로그 정보를 수집한다.

정답 4

btmp: 실패한 로그인 정보를 담고 있는 로그 파일이다.

2016년 08회
154. 다음 중 가장 바르지 않은 것은?
① wtmp: 사용자들이 로그인, 로그아웃한 정보를 가지고 있다.
② pacct: 사용자가 로그인한 후부터 로그아웃할 때까지의 입력한 명령과 시간, 작동된 tty 등에 대한 정보를 가지고 있다.
③ utmp: 시스템에 현재 로그인한 사용자들에 대한 상태 정보를 가지고 있다.
④ btmp: 사용자별로 가장 마지막에 로그인한 시간과 접속 IP, tty 등에 대한 정보를 가지고 있다.

정답 4

2014년 04회
155. 다음 보기에 해당하는 로그 파일은 무엇인가?

| |
|---|
| - 시스템 로그인에 실패할 경우 이 파일에 저장된다.<br>- lastb 명령어를 통해 확인이 가능하다. |

① wtmp ② btmp
③ utmp ④ pact

정답 2