Żródło :**http://users.uj.edu.pl/~ufkapano/linux/cz1wstep/konta.html**

**Konta użytkowników**

**INFORMACJE**

Podręcznik systemowy *man*: useradd, userdel, passwd, chown, chgrp, usermod, group, groupadd, groupdel, newgrp, groupmod.

**PLIKI**

/etc/skel

/etc/passwd (spis kont użytkowników)

/etc/group (grupy istniejące w systemie)

/etc/shadow (istnieje, jeżeli używamy "shadow passwords")

/etc/shells (powłoki dostępne w systemie)

/etc/login.defs (ustawienia domyślne dla kont)

**OPIS**

Każdy użytkownik, który loguje się w Linuksie jest identyfikowany w oparciu o konto użytkownika. Konto użytkownika kontroluje dostęp do systemu, definiując nazwę użytkownika i hasło, które uwierzytelnia użytkownika podczas procesu logowania się. Do kontroli przywilejów zalogowanego użytkownika wykorzystywane są identyfikator użytkownika (UID) i identyfikator grupy (GID), odpowiadające kontu użytkownika. Wartości te, zdefiniowane podczas tworzenia konta użytkownika, kontrolują bezpieczeństwo systemu plików i identyfikują, który użytkownik kontroluje dany proces.

Podstawowy proces dodawania konta użytkownika jest taki sam we wszystkich systemach linuksowych. Dodanie konta użytkownika wymaga następujacej procedury:

* edycji pliku */etc/passwd*, aby zdefiniować nazwę użytkownika, UID, GID, katalog domowy i powłokę logowania dla danego użytkownika
* ustawienia hasła dla użytkownika za pomocą polecenia *passwd*
* utworzenia katalogu domowego za pomocą polecenia *mkdir*
* skopiowania domyślnych plików inicjalizujących z katalogu */etc/skel* do katalogu domowego użytkownika
* zmiany właściciela katalogu domowego i znajdujących się w nim plików, tak aby użytkownik miał pełny dostęp do swoich plików; przykładowe polecenie to
* chown -R andrzej:users /home/andrzej

Istnieje polecenie *useradd*, które automatycznie wykonuje powyższe czynności. Bardziej nowoczesne polecenie to *adduser*, którego zachowanie można kontrolować przez opcje linii poleceń i plik konfiguracyjny [Linux Debian].

Wszyscy użytkownicy w systemie Linux mają odpowiedni wpis w pliku */etc/passwd*. Wpisy w tym pliku mają format:

użytkownik:hasło:UID:GID:tekst:katalog:shell

Są tu wpisy dla kont prawdziwych użytkowników oraz wpisy dla kont specjalnych utworzonych dla programów, które muszą kontrolować procesy lub które tworzą bądź usuwają pliki.

UID jest niepowtarzalnym identyfikatorem użytkownika. UID jest liczbą z zakresu od 0 do 32767 (nie zawsze!). Liczby poniżej 100 są zarezerwowane dla specjalnych kont systemowych. Red Hat Linux rezerwuje liczby od 0 do 499, a wolne są od 500 do 60000. Debian użytkownikom nadaje liczby od 1000 w górę.

Pole GID jest wykorzystywane do identyfikacji grupy podstawowej użytkownika. Wartości GID z zakresu od 0 do 499 są zwykle zarezerwowane dla kont systemowych (czasem rezerwuje się wartości od 0 do 99). Grupy dla zwykłych użytkowników leżą w przedziale od 500 do 60000 (Red Hat Linux).

Istniejące grupy zapisane są w pliku */etc/group*. Wpisy w tym pliku maja format:

nazwa\_grupy:hasło:GID:lista\_użytkowników

Grupa główna użytkownika jest przypisana w pliku */etc/passwd*. Lista w pliku */etc/group* jest używana do przypisania użytkownika do dodatkowych grup.

Nazwy dozwolonych powłok dla użytkowników są zapisane w pliku */etc/shells*. Jeżeli dodamy nową powłokę do systemu, dodajemy jej nazwę do pliku */etc/shells*. Typowa zawartość pliku */etc/shells*:

/bin/bash (Bourne Again Shell)

/bin/sh (Bourn Shell - link do /bin/bash)

/bin/tcsh (Tenex C Shell)

/bin/csh (C Shell - link do /bin/tcsh)

/bin/ash (A Shell)

/bin/bsh (B Shell - link do /bin/ash)

/usr/bin/pine (moj dopisek dla kont specjalnych)

Polecenie *umask* ustawia domyślne prawa dostępu do tworzonych plików i katalogów (ustawia się które prawa zabrać). Występuje ono np. w pliku */etc/profile* i jest wykonywane podczas otwierania sesji. Zwykle mamy takie prawa dostępu:

plik 644 (umask 133)

katalog 755 (umask 022)

Red Hat - narzędzie do konfiguracji typu uwierzytelniania to *authconfig* (dostępny wprost lub przez *setup*).

**ZAKŁADANIE KONTA**

Można zrobić to ręcznie w trybie tekstowym lub wykorzystać jakieś narzędzie graficzne, np. *linuxconf* (Users accounts | Normal | User accounts). Ręczne zakładanie konta dla zwykłego użytkownika *user1* z grupy *users*:

[root]# useradd -g users user1

[root]# passwd user1 (dwa razy wpisujemy hasło)

(tak można zmienić zapomniane hasło)

[root]# chfn user1 (informacje dla polecenia finger)

[root]# useradd -s /usr/bin/pine user2 (wybór login shell)

[root]# useradd -u uid user3 (wybór UID)

W Debianie warto korzystać z nowoczesnego polecenia *adduser*, które ma własny plik konfiguracyjny */etc/adduser.conf*.

**USUWANIE KONTA**

Można wykorzystać *linuxconf* lub zrobić to ręcznie:

[root]# userdel user1

Trzeba jeszcze recznie usunac katalog */home/user1* i pliki tego użytkownika w systemie. Usuwany użytkownik nie może być zalogowany i nie może mieć działających procesów.

[root]# userdel -r user1 (usunie katalog domowy)

W Debianie warto korzystać z nowoczesnego polecenia *deluser*, które ma własny plik konfiguracyjny */etc/deluser.conf*.

**ZMIANA WŁAŚCICIELA LUB GRUPY DLA PLIKU**

[root]# chown user2 plik1

[root]# chown user2:grupa2 plik1 (zmiana wlasciciela i grupy)

[root]# chown :grupa2 plik1 (zmiana tylko grupy, jak chgrp)

[root]# chown -R user2:grupa2 kat1

(rekurencyjna zmiana właściciela i grupy w podkatalogach)

$ chgrp grupa2 plik1 (przypisanie pliku do grupy)

**ZMIANA GRUPY DLA UŻYTKOWNIKA**

[root]# groupadd -g gid grupa1 (utworzenie nowej grupy z GID=gid)

[root]# groupdel grupa1

(usunięcie grupy; pliki trzeba ręcznie poprawiać)

[root]# groupmod -g gid grupa1

(zmiana GID dla grupy; pliki trzeba recznie poprawiać)

[root]# groupmod -n grupa2 grupa1 (zmiana nazwy z grupa1 na grupa2)

[root]# usermod -G grupa2 user1 (przypisanie czlowieka do grupy)

$ newgrp grupa2 (log in to a new group)

$ newgrp (powrot do login group)