



Învățați LINUX

Un angajat nou, Un user nou

Fie că este vorba de un angajat, client nou, accesul la unul din sisteme sau aplicații se face prin identificarea userului cu parola. În acest articol ne focalizăm atenția asupra creării unui nou user.

DE DRAGOȘ ACOSTĂCHIOAIE

Un *utilizator* reprezintă o entitate care poate executa programe sau deține fișiere. Accesul la resursele sistemului se realizează prin intermediul utilizatorilor înregistrați, în funcție de drepturile atribuite acestora.

Din punctul de vedere al sistemului de operare UNIX, un utilizator (numit și câteodată și cont de utilizator, *user* sau *user account*) nu este neapărat o persoană.

Utilizatorii pot fi ori persoane reale, ori utilizatori logici. Aceștia din urmă sunt rezervați pentru anumite aplicații care efectuează activități specifice (cum ar fi utilizatorul *apache* utilizat de serverul *httpd*). De asemenea, poate exista un cont utilizator partajat de mai multe persoane dintr-un grup de lucru. În majoritatea cazurilor, însă, un utilizator înseamnă o anumită persoană care poate "intra" (*log in*) în sistem, executa programe și utiliza sistemul.

Fiecare cont are un *nume de utilizator* (*username*) care îl identifică. De asemenea, fiecare utilizator are asociat câte un *identificator* (*User ID* sau *UID*), care este folosit intern de către sistem.

Utilizatorii pot fi grupați în *grupuri*. Acestea sunt practic colecții de utilizatori și pot conține unul sau mai mulți utilizatori. Fiecare grup are asociat un *identificator de grup* (*Group ID* sau *GID*), folosit intern de sistem.

Folosiți împreună, identificatorul de utilizator respectiv identificatorul de grup determină drepturile de acces la fișiere și la alte resurse ale sistemului. Acești doi identificatori sunt atribuiți în mod automat la momentul creării utilizatorului, însă pot fi modificați și ulterior.

Fișierul care memorează informațiile despre utilizatori în UNIX este */etc/passwd*, iar cel despre grupuri este */etc/group*. Parolele utilizatorilor sunt memorate criptat, într-un fișier protejat, și anume */etc/shadow*.

Fișierul */etc/passwd* are următoarea structură:

```
nume : parola : UID : GID : ↵
informatii : director : shell
```

unde:

- **nume** - este numele utilizatorului
- **parola** - reprezintă parola criptată a utilizatorului, dacă nu se folosește sistemul *shadow*, sau caracterul "x", dacă este utilizat acest sistem. Dacă acest câmp este "*", nu este permisă intrarea utilizatorului în sistem. Dacă acest câmp este vid, nu va fi solicitată nici o parolă pentru autentificarea utilizatorului
- **UID** - reprezintă identificatorul utilizatorului, având în mod normal valoare unică
- **GID** - este identificatorul grupului principal din care face parte utilizatorul
- **informații** - conține în mod normal numele utilizatorului. Acest câmp este numit și *câmpul GECOS*. În acest câmp pot fi memorate și informații suplimentare privind biroul în care lucrează utilizatorul, numărul de telefon etc., aceste informații fiind separate prin virgulă
- **director** - reprezintă directorul *home* al utilizatorului, de obicei */home/nume*. Fiecare utilizator deține câte un asemenea director separat, folosit pentru a depozita fișierele proprii

- **shell** - este interpretorul de comenzi folosit de utilizator. Interpretorul va fi lansat imediat după autentificarea utilizatorului în sistem. Este în general */bin/bash*, dar poate fi și */bin/csh*, */bin/tcsh* etc. În anumite cazuri, poate fi constituit de o aplicație, singura pe care o poate folosi utilizatorul

Un fragment dintr-un fișier */etc/passwd* poate arăta astfel (observăm numele a doi utilizatori reali, *dragos* și *ovidiu*, și cele ale unor utilizatori sistem):

```
mysql:x:27:27:MySQL:↵
Server:/var/lib/mysql:/bin/bash
apache:x:48:48:↵
Apache:/var/www:/sbin/nologin
dragos:x:500:500:↵
Dragos Acostachioaie:↵
/home/dragos:/bin/bash
ovidiu:x:501:501:↵
Ovidiu Ene:/home/ovidiu:/bin/bash
```

Fișierul */etc/group* are următoarea structură:

```
nume : x : GID : [ lista_utilizatori ]
```

unde:

- **nume** - este numele grupului
- **GID** - reprezintă identificatorul de grup
- **lista_utilizatori** - desemnează lista de utilizatori care fac parte din acest grup. Elementele listei sunt separate prin virgulă

Fișierul */etc/group* poate arăta ca mai jos:

```
mysql:x:27:
apache:x:48:
dragos:x:500:
```

Tabelul 1

Comanda	Acțiunea
<code>useradd</code> nume	adăugarea de utilizatori
<code>userdel</code> nume	ștergerea de utilizatori
<code>usermod</code> nume	modificarea parametrilor asociați utilizatorilor
<code>chfn</code> nume	modificarea informațiilor (GECOS) despre utilizatori
<code>groupadd</code> grup	adăugarea de grupuri
<code>groupdel</code> grup	ștergerea de grupuri
<code>gpasswd -a</code> nume grup	adăugarea de utilizatori la un grup

```
ovidiu:x:501:
autori:x:600:dragos,busaco
```

Există un utilizator privilegiat, cu statut de supervisor al sistemului, denumit *root*, având identificatorul de utilizator egal cu zero. Acest utilizator are drepturi totale asupra sistemului, în sensul că poate, de exemplu, controla execuția proceselor, manipula orice fișier sau schimba diverse atribute asociate utilizatorilor.

În mod normal, acest cont de utilizator trebuie folosit doar atunci când se execută anumite operațiuni administrative, cum ar fi instalarea de programe, modificarea fișierelor de configurare ale sistemului sau adăugarea de noi utilizatori.

Atât contul *root*, cât și o serie de conturi de utilizatori logici, sunt creați în mod automat la momentul instalării sistemului. Se recomandă crearea unuia sau mai multor utilizatori obișnuiți pentru utilizarea obișnuită a calculatorului, deoarece o comandă greșită lansată ca *root* poate cauza deteriorarea sistemului sau chiar pierderea datelor și aplicațiilor stocate.

În vederea asigurării securității sistemului, este obligatoriu ca toți utilizatorii să aibă parolă. Este de dorit ca parolele să aibă minim 6 caractere și să nu fie constituite din cuvinte ușor de ghicit, cum ar fi cuvinte de dicționar sau elemente importante pentru utilizatorul în cauză (numele prietenilor, data nașterii etc.). Principiul de bază

pentru alegerea parolelor este ca acestea să fie ușor de memorat, dar greu de ghicit. De asemenea, utilizatorii trebuie să își schimbe parolele în mod regulat.

Procesele din UNIX au două identități la un moment dat. Prima identitate este *identificatorul de utilizator real*, adică cea dată de numele de cont de la conectarea utilizatorului. Uneori, pentru execuția anumitor programe sau comenzi, utilizatorii trebuie să primească provizoriu identitatea trebuie să primească identitatea altui utilizator; acesta este *identificatorul de utilizator efectiv*, valabil doar pe durata execuției respectivului program. Acest transfer de identitate este acceptat de proprietarul programului, prin setarea bitului *Set UID (SUID)* din drepturile de acces ale fișierului executabil.

Comanda *su* (Substitute User) permite schimbarea identității unui utilizator. Dacă noul nume de cont furnizat este protejat prin parolă, utilizatorul trebuie să o furnizeze; dacă utilizatorul real este *root*, nu este necesară furnizarea parolei.

Administrarea utilizatorilor se poate face cu ajutorul aplicațiilor grafice specifice distribuției instalate (e.g. *config-users* în Fedora/Red Hat, *userdrake* în Mandrake), precum în figura 1, fie cu ajutorul progra-

melor tradiționale vezi Tabelul 1

Modificarea parolei utilizatorului curent se va face cu ajutorul programului *userpasswd* sau *passwd*. Este solicitată parola actuală și de două ori parola nouă (a doua oară pentru confirmare):

- Alte comenzi referitoare la utilizatori:
- **whoami** - furnizează numele utilizatorului efectiv curent
 - **who** - afișează lista sesiunilor deschise ale utilizatorilor
 - **w** - comandă înrudită cu *who*, afișează sesiunile deschise și, pentru fiecare sesiune în parte, ultima comandă executată
 - **id** - oferă informații privitoare la identitatea reală a unui utilizator:
 - **finger [nume]** - afișează utilizatorii conectați curent la sistem. Dacă este specificat un nume de utilizator, vor fi afișate diferite informații despre respectivul utilizator, cum ar fi numele acestuia și ultima intrare în sistem
 - **last [nume]** - afișează ultimele intrări ale utilizatorilor în sistem, în ordine descrescătoare a datei. Dacă este specificat un nume de utilizator, jurnalul afișat se va referi la intrări ale utilizatorului respectiv. ■

AUTORUL

Dragos Acostăchioaie este programator de sistem și aplicații Linux, administrator de rețea, putând fi contactat la adresa dragos@adt.ro

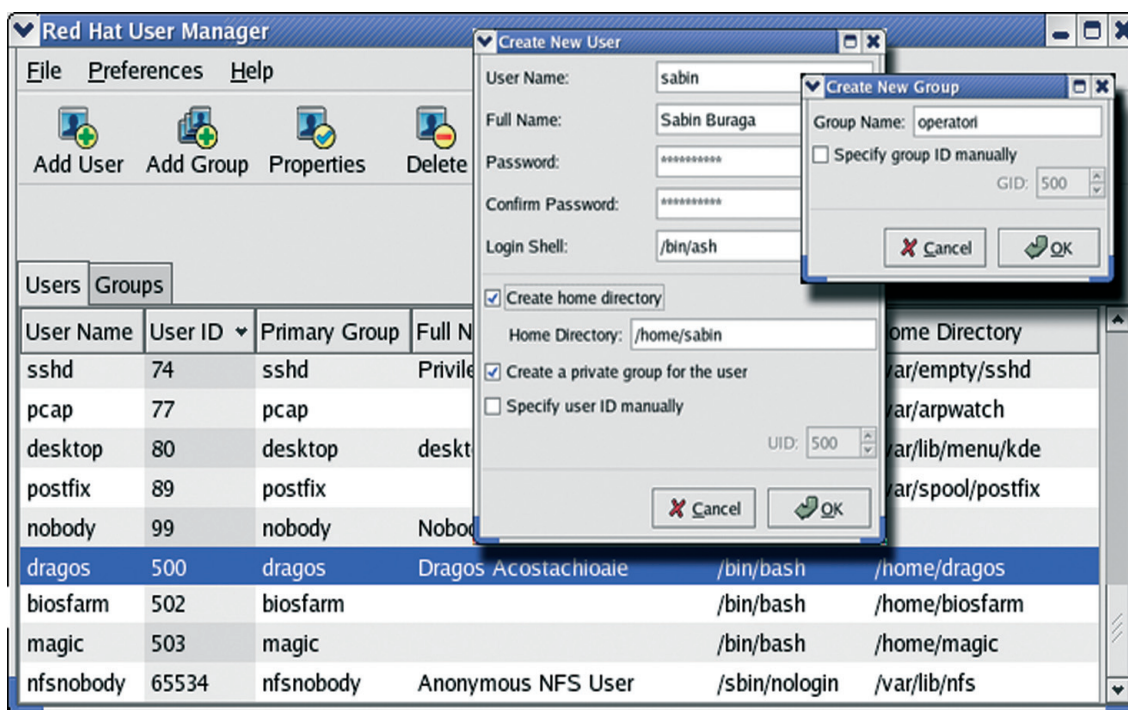


Figura 1: Administrarea utilizatorilor cu ajutorul Red Hat User Manager